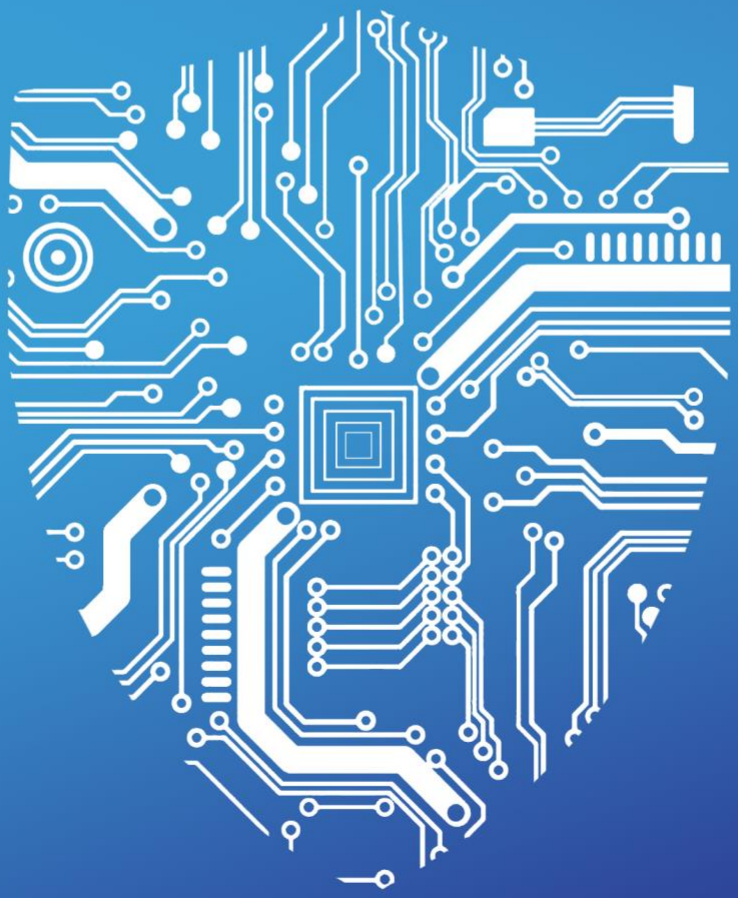
2019 TAG CYBER SECURITY ANNUAL

VOLUME 2

INTERVIEWS WITH CYBER LUMINARIES



Dr. Edward G. Amoroso

TAG cyber

Lead Author – Ed Amoroso
Researchers – Matt Amoroso, Felix Andersen, Liam Baglivo, Ana Bolsoni, Shawn Hopkins, Miles McDonald, Ankit Parekh, Pratik Patel, Stan Quintana, Tim Steinberg
Media – Matt Amoroso, Laura Fanelli, Miles McDonald
Detailed Copy Editing – Shawn Hopkins
Finance – M&T Bank
Design – Alicia Amoroso, Miles McDonald, Rich Powell
Administration – navitend
Facilities – WeWork, NYC

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2019 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

September 17, 2018

To the Reader:

Conducting and transcribing a detailed interview with an expert is harder than it looks. This is the third year we've published our questions and the corresponding answers received from various cyber security luminaries for this *TAG Cyber Security Annual, Volume 2*. While we would admit considerable remaining distance between our work and Cronkite's, we do think we are getting better. In fact, we are confident you will find this series of interviews to be the most crisp and interesting content in our three volumes – probably because our interviewees did all the work.

Our primary goal in each interview was to showcase the expert views of the *person* being interviewed. This might sound obvious, but it is often complicated by marketing and public relations teams who certainly earn their monthly paychecks. On occasion, we would submit questions and receive back cut-and-pasted responses perfectly phrased from a brochure: "Our industry-leading security solution provides superior protection of your critical assets on both premise and in the cloud." We tried to push back whenever we received anything vacuous like this.

For the most part, however, our experts – forty-five in total – were selected because their voice was simply worth hearing. Too many enterprise security teams avoid vendors like the plague, and this is a lose-lose situation. Enterprise teams lose out because they are deprived the amazing perspectives available from the cyber technology community; and the vendors lose out because they drive customers away by being too pushy about why their product would have solved the problems of Target, Sony, OPM, and Home Depot, not to mention stock fluctuations and global warming. Our interviews cut through all of that.

We recommend that you use these interviews in your day-to-day source selection or vendors and partners. If you are considering a purchase in some area of cyber security protection, then check to see if a principal from that firm is included here (or in our two previous volumes published in 2016 and 2017). Take a moment and read their words, because it will help provide for you with a sense of their purpose, belief, and intent. It's been our experience at TAG Cyber that understanding what a company and its principals *believe* is often the most important factor in determining whether their products will fit your needs.

By the way, if you are a vendor and haven't been included here – but believe this is an injustice the size of our galaxy, then please feel free to drop us an email at eamoroso@tag-cyber.com. We will do our best to set up time to review your solution offering. We cannot promise that we will make it together to second base, but we promise to try to listen to your message, and to try to understand what you and your team are about. Our experience dictates that this is the optimal means for any industry analysts to advance the community.

Wishing you nothing but the best in your cyber security work this year, enjoy this volume – and we hope it helps you save time, effort, and money.

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Fulton Street Station on Broadway

2019 TAG Cyber Distinguished Vendors

Each year, we cover roughly 2000 vendors in the cyber security industry and write a one-pager for Volume 3 of this Annual. From that large group, we down-select about 200 or so to deep-dive their technology and usually to generate an article, blog, or technical article. We do this work gratis – and enjoy every bad-business-model-because-it's-free minute of the work. Every day, we try to assist the industry – and that includes you – with this work. You should follow Edward Amoroso on LinkedIn or @hashtag_cyber on Twitter to gain access to this stream of content. In addition, however, we down-select the list to about 40 or so cyber security vendors that we believe are truly worth spending serious time with during our year. These vendors become our *TAG Cyber Distinguished Vendors*, and we channel their technology message to you through a series of articles, webinars, white papers, technical reports, eBooks, videos, interviews, and on and on. This report would not be possible without their technical, in-kind, time, travel, research, meeting, and financial assistance to TAG Cyber throughout the year. The list of 2019 Distinguished Vendor sponsors is provided below and I hope you'll take a moment to review the list. These are fine companies:

Table of Contents

Offering DMARC-Based Solutions for Email

An Interview With
Ravi Khatod
CEO
Agari

WHEN EARLY email security standards emerged such as DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework), the community took notice of the weaknesses inherent in the email protocol. As these standards were wrapped into the more modern DMARC (Domain Message Authentication Reporting and Conformance), it became clear that enterprise teams needed to improve the authentication properties of their email usage.

One of the leading cyber security companies in this important initiative has been *Agari*. The company has been at the absolute forefront in the drive toward improved cyber security for messaging with a platform that is both mature and easily integrated into an enterprise. We recently sat down with the company's CEO Ravi Khatod, to learn more about this important area of enterprise email security.

EA: What is the authentication issue with typical enterprise email?
RK: Without authentication, it is impossible to establish a trusted identity. Unfortunately, a lot of enterprise email is sent without authentication, which puts it at risk for spoofing and fraud. Malicious third parties can easily hijack a brand by sending emails on their behalf, which can damage the reputation of a company or any other organization by negatively impacting their customers. Phishing attacks are among the most common and effective forms of cybercrime today, even by the most advanced adversary, which is why so many organizations depend on Agari for protection.

EA: How does DMARC address this weakness?
RK: Agari has been working closely with the industry for half a decade to develop DMARC, which is an open standard that authenticates the sender of a message to its receiver. Because it is an open standard, DMARC is supported by every major email service provider, which means unauthenticated messages can be quarantined or completely blocked from being delivered to the users' inbox. And it's one of the most effective ways to protect the trust people have in your brand.

EA: Tell us about your platform and how it works.
RK: The Agari Email Trust platform is currently used by Facebook, Microsoft, Google, six of the top ten banks and hundreds of government domains to protect their inbound and outbound email messages from identity deception attacks, such as phishing and business email compromise. Agari protects more than two trillion emails per year, and we use this data to inform more than 300 million machine learning models, which we call Agari Identity Intelligence – and we update these models every day. Our AI-based solution leverages this enormous data set to build models of trusted communication. It is impossible to build models of malicious behavior because you cannot predict what technique or tactic cybercriminals will try next. So instead, we model this enormous set of known, trusted communications to teach our machine learning models what "trustworthy" communication looks and acts like. That lets us identify deviations from the good, detect the bad, and stay one step ahead of criminals.

EA: What sort of telemetry will security teams have access to once they buy into DMARC?
RK: DMARC is a free and open standard, which can be deployed easily within minutes, so the only buy-in is the desire to improve email security. Once deployed, DMARC enables organizations to gain a complete view of their email ecosystem, including third-party senders, email volume and forensic data on attacks impersonating their domains.

EA: Have you seen real risk reduction in enterprise since you've been delivering platform solutions these past years?
RK: Absolutely. We're changing the game and turning the tables on cybercriminals with this model. Cybersecurity has traditionally been a game of cat and mouse. Criminals develop new techniques, security experts develop new defenses, criminals develop new techniques, and so on. Despite decades of technical innovation and billions of dollars invested, security experts have always been fighting a defensive battle. But by switching the focus of our AI to model the good, and by moving away from the traditional perimeter-based enterprise defenses into more cloud-based solutions, we're seeing a widespread modernization of security that's making a real difference. The zero-trust model is predicated on identity, authorization and authentication. Artificial intelligence solutions are enabling organizations to make smarter business decisions. The pendulum is swinging in favor of organizations that are embracing these new trends.

Outmaneuvering Cyber Adversaries with Deception

An Interview With
Tushar Kothari
CEO
Attivo Networks

THROUGHOUT MILLENIA, defenders have used the power of deception to deal with advanced adversaries. The tradition of traps, lures, and misinformation traces its roots to early warfare, where battle commanders knew that any uncertainty on the part of the adversary would create both tactical and strategic advantages. Deception in cyber security, is a natural evolution to modern protections for the enterprise and in strategies for outwitting today's adversary.

A pioneering organization in the establishment of deception as a best practice for enterprise cyber security is *Attivo Networks*. Their platform includes embedded trap functionality to support live forensics, advanced attack detection, and state of the art incident response. We recently caught up with the company's CEO Tushar Kothari, to ask him to share his views on how deception is being used, and how it will evolve.

EA: How long now have companies been deploying deception as a part of their defensive strategy?

TK: The earliest form of cyber deception technology, known as honeypots, was introduced around 20 years ago as a tool for researching what forms of attacks were targeting an organization. Honeypots only saw limited adoption in enterprise environments because they were designed for watching attacks and not specifically as a tool for detecting or analyzing threats. The complexity and lack of scalability of these early solutions was a barrier to broad adoption. That changed in 2014 when Attivo introduced a commercial grade deception technology that offered detection of threats that are inside the network. The focus on detection vs. research dramatically changed the value of threat deception, along with the removal of operational and scalability limitations. Since Attivo started shipping product, the company has grown into triple digits of customers and has seen substantial deployment expansions. I would say that 2017 was one of the first years that we began seeing deception began as a line item in security budgeting, and I am really pleased with the significant number of companies we are working with to establish 2019 budgets. Deception is well on its way to becoming a standard detection security control for organizations across all major industries and for organizations both large and small.

EA: How does deceptive functionality typically work in an enterprise?

TK: With today's threat deception technology, customers can choose to deploy endpoint, network, application, and data deceptions. A comprehensive set of deceptions is critical to effectively detect and respond to all types attack types across various attack surfaces comprised of legacy to advanced environments such as server-less cloud or IoT. Attivo customers will typically start with deceptive credentials and lures at the endpoint to catch attempts of credential theft or ransomware attacks. They will then place decoys around critical assets that would be targeted by an adversary. From here, organizations will expand into clouds, user networks, remote locations, and into specialized deception environments such as ICS-SCADA, IOT, POS, network and telecom infrastructure or possibly into very specific application decoys like SWIFT financial systems or web services servers. Our more advanced customers will then venture into data and database deceptions to gather attacker counterintelligence and geolocation services that can help with attacker attribution. The Attivo ThreatDefend is extremely flexible with an out of the box set up working for many smaller customers and extremely sophisticated deceptions for our financial or government customers. It's interesting that regardless of size, it is push-button simple to generate, deploy, and maintain deceptions. This year, Attivo introduced machine self-learning that quickly learns the network to automatically generate and deploy deception campaigns. Attivo automated attack analysis and native integrations will also dramatically simplify incident response. For perspective, a customer can have Attivo deception deployed in under an hour and maintain the environment with typically less than 5% of an FTE's time. Attivo deception can also be a core factor in creating an active defense for its customers. In addition to early detection, the platform includes its own attack analysis engine, extensive forensic reporting, and over 30 native integrations which automates and accelerates incident response. Collectively, this delivers early detection and response for organizations of all sizes, giving them the upper hand against attackers.

EA: Are honey pots part of the deceptive equation?

TK: Honeypots have their place as single hosts that can provide research on types of attacks targeting an organization. It's interesting but not near the value of a high-fidelity in-network detection system. Because we get so many questions regarding the differences, let me take a moment to outline what they are. First, Deception platforms are much more than just a honeypot in that they can detect not only reconnaissance, but also in-network lateral movement, credential theft, man-in-the-middle, and Active Directory attacks. In addition to covering a broader set of attack methods, deception plays a critical role in detecting attacks on legacy through to modern day infrastructure. A low interaction, emulated decoy won't have the authenticity to be believable to an attacker. A key to achieving an attractive decoy for attackers is through over 50 real operating systems, services, and applications. This, and the option to use the same golden image software as production devices, make these decoys appear as a mirror image to the real assets. Second, the ThreatDefend platform is extremely scalable as it can deploy across any environment, including enterprise user networks, clouds, data centers, Remote Office/Branch Office, and specialized environment. The ThreatDirect forwarder technology can also be deployed to easily present deception in geographically distributed environments. Legacy scalability limitations are completely removed along with operational

limitations. As I mentioned earlier, one of the downfalls of honeypots was their complexity to manage. Machine learning has completely changed the set up and operational management of deception. Complexity should no longer be viewed as a barrier to entry.

EA: How can companies who operate mostly in the cloud make use of deception?
TK: The cloud has expanded an organization's capabilities, but also its attack surface. Currently, there is complexity in shared security models and lower levels of visibility in the cloud that can lead to detection gaps that attackers can exploit. Many cloud detection models are challenged in that they simply don't scale to meet the needs of a high-volume computing environment. This becomes even more challenging when containers and serverless computing is introduced. Deception plays a critical role in effectively close cloud detection gaps. Not all deception offerings can support the cloud. However, Attivo has invested significant engineering resources so that the ThreatDefend platform supports not only AWS, Google, Azure, and Oracle environments but also includes support for decoy containers, deception credentials in production Lambda functions, decoy IAM Access Keys/Tokens, SSH keys, S3 buckets, Route53 DNS entries, deception Lambda functions, and CloudWatch monitoring. Attivo is customer-proven with deceptions deployed in production cloud environments and has many additional features recently added to expand deception to serverless computing and containers.

EA: Any predictions on where deception technology is headed in the coming years?
TK: This is the first technology that truly turns the tables on attackers and puts the power back in the hands of the defenders, so they can leverage their home-field advantage. Based upon customer traction and technology evolution, deception will become a ubiquitous new layer in the security stack and a de facto security control that empowers organizations to efficiently detect and respond to attackers early in the attack lifecycle.

Active Visibility and Mitigation of OT Security

An Interview With
Toby Weir-Jones
Senior Director of Product
Bayshore Networks

THE PROTECTION of industrial control system (ICS) infrastructure involves direct interaction with so-called operational technology (OT) networks, systems, and software. This is different than one finds with traditional IT, if only because the underlying standards, protocols, norms, and technical methods are quite different – not only with IT, but across the spectrum of OT systems, including factories, plants, vehicles, processing centers, and the like.

One of the earliest technology companies to begin developing cyber security solutions for ICS and OT infrastructure is *Bayshore Networks*. The company has developed an appliance that resides in the OT network and collects data for cyber security analysis and active risk mitigation. We recently connected with Toby Weir-Jones of Bayshore to learn more about OT visibility and active mitigation from cyber threats.

EA: Do you still have to convince OT companies that they need to focus on cyber security?
TWJ: Most operations technology (OT)-oriented companies now recognize that they need to pay close attention to cyber security issues, but the challenge is they're not sure exactly where to start. They're being bombarded by complicated product messages without a lot of clear thought leadership on best practices. We've adjusted our focus towards a core set of critical OT security activities which should be monitored in every OT environment, along with recommendations on what mitigation steps can be performed without disrupting operations or safety.

EA: Where should an OT security professional focus their efforts?
TWJ: They need to understand not only what's "out there" on their networks, but also what they can do, safely and constructively, to improve their OT security within the safety and maintenance parameters that production environments demand. Improvements in configuration, or network segmentation, or policy can often be done without requiring downtime on the floor, and Bayshore is the only ICS security tool which can provide real-time

mitigation to protect OT devices at the payload level. This allows safer operation, with less downtime, all while improving your security posture.

EA: Tell us how your solution works and how it can be used for visibility and mitigation?
TWJ: Bayshore's solution includes a wire-speed data collection device which can sit on a network tap or span port, or can be installed inline to provide active mitigation functions. It analyzes a range of ICS network protocols down to the payload level and categorizes all the activity it sees based on both our own recommended critical OT security activity filters and any customer-defined policies. All such information rolls up to a centralized management console where you see a record of your assets and OT network activity and, most importantly, recommendations about policy improvements and priority decisions which you need to review. While many vendors offer solid visibility tools, Bayshore's combination of visibility along with safe and smart real-time mitigation is unique in the industry, and works for both the most insightful end-users and on behalf of large service providers who are working to deliver against SLAs for their global customers.

EA: What trends are you seeing in OT security, other than perhaps greater awareness?
TWJ: The customers have been flooded with visibility pitches for the past few years, and they are realizing that awareness is only the very first part of an effective OT security solution. Ultimately, they need to know what to do next, and how much of that can be done on their behalf by their tool or their service provider. OT threat mitigation is all about preserving production safety and continuity unless you absolutely can't, and then providing the best detail and recommendations so everyone has a transparent and objective understanding of why the OT team needs organizational support for major risks. The vendors who will succeed in this evolving space are already positioned to enable these 'shades of gray' and satisfy the demands of not only the OT security team, but the corporate IT security team as well.

EA: Any new features or capabilities that your team is currently working on?
TWJ: Absolutely. Bayshore's strategy is to bring its payload-level policy controls to the entire OT environment. This includes the network inside the plant, the transition layer to other corporate or external networks, and the remote access gateway required for trusted ingress. As a result, we have updated our OTSRA™ secure remote access product to incorporate granular policy controls as a baseline function for all user connections to all endpoints, and we are planning to bring a soft data diode in early 2019 with the same policy controls available, at a much lower cost than the existing hardware-based designs. It's an exciting time to invest in the Bayshore platform and we are confident our solutions will readily distinguish themselves from the visibility and asset management providers on the market today.

Packet-Based Authentication and Security

An Interview With
John Hayes
CTO
BlackRidge Technology

FOR MANY years, enterprise security teams have had to react to adversaries' ability to conduct network scanning and reconnaissance, and attacks on an organization's IT environment. The implicit trust required by the Internet Protocol (IP) generally allows packets from any IP address to progress inbound and put an organization at risk. If access management policies could be better enforced on inbound IP addresses, greater security can be ensured.

A company at the forefront of ensuring better network packet-based authentication and security is *BlackRidge Technology*. The company has developed technology that creatively enhances the TCP/IP suite to provide authentication of the packet sender's identity and enforcement of enterprise policy before connections are established. We recently caught up with John Hayes, CTO of the company, to learn how such protocol security methods work.

EA: Can you explain the basic concept behind the BlackRidge Transport Access Control method?
***JH*:** We use authenticated identity to authenticate TCP sessions before allowing them to be established. Each TCP session is individually authenticated with a cryptographic token inserted into the first packet (TCP-SYN) of a TCP session. Our software approach enables deployment in enterprise, cloud, SDN and IIoT infrastructure.

EA: What threats specifically are addressed by your technology?
JH: With today's security threats, any information used in the security decision process must be authenticated before it is used. Using unauthenticated information in this decision process provides an attack surface for the adversary. Applying this concept to network traffic, most network security approaches use a combination of network addresses and content to make decisions. Addresses cannot be authenticated. Content, when available, is not always authenticatible. I say, "when available," with respect to content because as more and more content is being encrypted, it is not available for decision making, unless the encryption keys are shared with the network security device. Not all customers are willing to do that. BlackRidge uses authenticated identity for its decision process that is available at the network layer, independent from the content, whether encrypted or not. Getting back to relying on

authenticated information when making security decisions, another thing to consider is how the authentication is performed. If the authentication requires interaction- a series of communications between the requesting party and the authenticating party- then the authentication mechanism itself can be used for mapping and discovery. This is how PKI certificates, TLS and IKEv2 operate. BlackRidge uses non-interactive authentication, blocking scanning and discovery from unauthorized sources in addition to managing access to BlackRidge protected resources.

EA: What aren't existing IP-based tools sufficient for authentication and security?
JH: Existing IP-based tools use a combination of rules, heuristics and statistical metrics for decision making. These tools use information which cannot be authenticated, and which often needs continuous updating. The limitation of these tools is that they suffer from both false positives and false negatives, limiting both their deployability and effectiveness. A false positive, by the way, is a false alarm, an indication of a security event when no event exists. A false negative is an undetected attack. It is the false positives that that preclude the automation of these tools for cyber defense. BlackRidge, with its cryptographically secured identity tokens have an extremely low false positive rate (<0.0001%) enabling deployable cyber defense automation.

EA: How do customers integrate your solution into their security architecture?
JH: BlackRidge products are designed to work as an overlay software solution to block unidentified and unauthorized access and protects resources from discovery from unauthorized network mapping and reconnaissance. By integrating with existing Identity Management systems (IDMS) enables existing identities to be used to authenticate network sessions and automate security policies. We have also integrated our event reporting with several SIEM and analytics systems, providing visibility to events within a customer's existing monitoring and response infrastructure. Operationally, we deploy our BlackRidge TAC software as inline layer 2 (transparent) or layer 3 (addressed) enforcement points. Being able to select layer 2 or layer 3 operation enables us to deploy in both LAN environments and cloud/SDN environments. In this way, we can extend a customer's identity-based security policies from the enterprise to the cloud, enabling an identity secured hybrid solution.

EA: What threat trends are you hearing from customers?
JH: The largest growth of threats we are seeing is coming from the Industrial IoT (IIoT) sector and Operational Technology (OT) converging onto enterprise IT networks. This includes industrial control systems, building management systems, medical equipment and factory automation. Legacy, non-networked devices that have been migrated to networks and new IoT devices have paid little attention to the security of the networks and devices, providing new surfaces for attack. Now we are being asked how to secure both legacy (brownfield) IIoT as well as new deployments. BlackRidge's identity-based technology can be applied "on the wire" to authenticate and secure both legacy (brownfield) IIoT as well as new deployments.

Code Injection for Mobile App Security

An Interview With
John Aisen
CEO
Blue Cedar

MANY DIFFERENT methods exist for mitigating threats to mobility. Most of them have progressed directly from comparable security controls for PCs; this includes basic anti-malware security, scanning, and even behavioral solutions. But the potential for dramatically increased threats to mobile devices, systems, and infrastructure continues to grow, and new approaches are needed in enterprise and consumer contexts.

One approach to mobile app security involves "no-code" integration techniques to introduce security controls without the need for writing or maintaining integration code. This is powerful because it expands the ability for enterprise teams to reduce mobile app risk without having to introduce large projects. We recently asked John Aisen of *Blue Cedar* to explain how security control integration works and how it reduces the security risks associated with mobile apps.

EA: Do enterprise teams recognize the risks of mobility and especially mobile apps?
JA: There is no doubt that enterprise teams have figured out that as business activity continues to shift to mobile devices and apps, corresponding security and compliance concerns are shifting accordingly. I mention compliance simply because it helps to drive good behavior from a security perspective. Both security and compliance complement each other as mobile apps become so important in business.

EA: How does your solution work and what is its differentiator with other security approaches?
JA: What we do involves a unique set of integration services, powered by our Blue Cedar Integration Platform, which allow us to embed SDKs, services and, in the case of Blue Cedar Enforce, native security controls into the mobile application code. This is especially powerful because it does not require any programming by development teams, which would obviously complicate matters, especially for third-party developed apps.

EA: Can the Blue Cedar approach be used for both new and existing apps?
JA: Absolutely. Existing mobile apps benefit from the convenience of no-code security integration without making great demands on the development team. But if a new application

is being developed for mobile, then the Blue Cedar platform provides an excellent means for ensuring the highest levels of protection from malicious exploits.

EA: What sort of features are included in your offering?
JA: Our Enforce product is primarily concerned with enforcement of policy and protection of user privacy through the mobile app usage lifecycle. We use FIPS-compliance cryptography, for example, to integrate encryption support into the mobile app to protect user data. We impose blocks on potentially compromised devices so that mobile apps cannot run on these dangerous platforms. We can also integrate identity, analytics, and even quality-of-service functionality into corporate mobile apps.

EA: Any major industry trends your team is hearing regarding mobility security?
JA: The biggest trend is the acceleration of native mobile app usage for essential business requirements. This is driven by productivity and cost advantages, as well as the growth in demand for corporate data processing on edge devices like mobile, triggered by augmented reality, artificial intelligence and business use cases that demand zero to no latency. But with all these capabilities comes the obligation to offer commensurate security at the edge – and that is where Blue Cedar Enforce comes in.

Securing and Simplifying File Delivery

An Interview With
Karl Falk
CEO
Botdoc

A NAGGING annoyance for so many enterprise teams is that options for secure transfer and delivery of files are not always evident. Teams struggle with the proper means for sending or collecting a sensitive document to/from someone they have no prior arrangement with – and that perhaps have no plans for future arrangement. Sending an application, form, or simple write-up in a secure way has always been a mystery to business people who often must request sensitive documents like a driver's licenses, bank statements, W-9s, or medical ID cards.

The good news is that excellent secure options are now available, and *Botdoc* has been at the forefront in this regard. Their primary use-case makes sending a secure document over the Internet easier and better than sending a fax. We recently connected with Karl Falk, CEO of Botdoc to ask about how his customers were using his secure sending solution to improve the security and ease of transferring files.

EA: What has been the primary challenge to date for securely sending or collecting files in business?
KF: Cybercrime is increasing and has become a nemesis every major company must face now and in the future. In response, companies are implementing more and more security, which is exactly what they should be doing. The problem is that with these new layers of security, business processes can become cumbersome and complex. It's like a child see-saw, with one side being security, and the other side, convenience. Over time, as we add more security, we're driving down convenience factors, or as we decrease security, we increase convenience. CIO and CISO teams are continually in this battle with the operational side of the business. This is the primary challenge today, where the complexity of security gets in the way of ease and simplicity. There are two things I am confident will be true in the future: First, cyber-crime will always be a growing issue that is not going away. And second, the human being will always resonate with whatever is simpler, even if they know it's less secure.

EA: How does your product solve this issue?
KF: Our clients call us the 'secure FedEx' of data. We're in the secure electronic transportation business, where we pick data up and drop it off. Botdoc transports data and documents with

end-to-end encryption. Such use of encryption might not necessarily be unique, except that we're doing it without pins, passwords, logins, accounts, apps, or software to download. Furthermore, upon delivery, the encrypted container and everything inside, evaporates. Companies are now botdocing their customers and clients for secure digital transport.

EA: How does the technology work and how are clients using Botdoc?
KF: Botdoc uses a point-delivery method and secure digital transportation layer that can be bolted onto existing systems to handle incoming and outgoing data transfers. Since each request is unique and disposable, the transaction is uniquely identifiable, so the originating system knows what it's for, and where it needs to go when it comes back. This allows companies to avoid central queues, not to mention the staff to manage those queues. Now, documents can be transported and delivered into the account where they need to go. Companies can collect and send documents and data securely via text or email (in the future these will be other means), by not imposing something foreign, like an app or portal. Today, when most companies want to send or collect something securely, they immediately migrate toward creating or leveraging a portal for their clients to log into. Not only does this introduce more friction and delay in the transaction, it also increases company infrastructure costs significantly, as they must support logins for potentially millions of clients.

EA*: Do you worry about phishing attacks that might try to exploit the file transfer process?*
KF: We do. It's something we've considered in our design. But keep in mind that with the Botdoc technology, the use cases are often "just in time" transactions. Suppose that ACME Brokerage is talking with Bob Smith, for example, and requests a copy of Bob's driver's license and an old 401K statement. What happens is that seconds later, Bob receives a text saying that ACME is requesting documents from you. So, with this "just in time" use case, the risk of phishing is minimal. We are working to developed consumer education to make sure that business people and citizens will learn that if they receive weird, unexpected requests for documents, that they should treat this as they would suspicious Spam.

EA: What features and capabilities should we be expecting in the future?
KF: After considerable usage and feedback from large and small companies, a few design issues have emerged. First, we see that the need for secure digital transport, more than just documents, is real and is an immediate need. We predict that in the next several years, every major company that maintains a system or portal will be rolling a secure digital transportation layer into their architecture roadmap. It's a new niche area that is exposing the challenges of the see-saw scenario we discussed earlier. With this new area of focus, you can expect to see more capabilities from Botdoc that allow activities to happen through a transportation layer versus a login. If a company needs to send something versus sharing it, Botdoc will be handling those transactions and adding new capabilities to make the experience easier.

EA: What is a secure digital transportation layer and why is it important?
KF: A secure digital transportation layer, as a bolt-on to an existing system, has many advantages: First, it allows a company to transport documents and data into and out of its systems, without anyone having to login. Second, this reduces friction for the consumer as well

as infrastructure costs for situations where documents can just be transported. Systems support fewer logins, and thus need less infrastructure to operate. Third, over 80% of all hacks come from compromised login credentials. If you reduce the number of logins, then you reduce the number of hacks. Even as companies move to non-password technologies, there will still be a login to manage. Fourth, a system with a digital transportation layer has a reduced attack surface area with fewer access points. And fifth, by adding a transportation layer, a company is segregating its external surface, the transportation layer, from its internal system. Furthermore, with firewalls that can be put in place between the system of delivery and the transportation layer, the potential for hacks is greatly reduced.

EA: Are there any situations where a digital transportation layer is not good to use?
KF: There's a difference between sharing and sending. Sharing is a collaborative environment, and involves a real-time exchange of data. Although that is necessary, over 95% of the time, all that is needed to happen involves a send or collection. Sending with the Botdoc technology involves removing one party from the sharing equation, and the party left on the system can now remote collect and send documents to the other party without them needing to be on the system doing the sending or collecting. We are challenging companies to assess their current processes and technology, and if they are imposing a sharing technology on a sending situation, then their business will not be as secure, efficient, or effective as it should be, putting too much friction between them and their customers. If they are imposing a sharing requirement on a sending situation, then they need to implement Botdoc as a sending technology to break their see-saw.

Securing Linux for the Data Center and Cloud

An Interview With
John Viega
CEO
Capsule8

A SURPRISING characteristic of modern computing is that Linux has become the dominant operating system. That a Unix-based underlying framework would guide the present and future data center, cloud, and other server-rich environments should not be a huge surprise, given the maturity and effectiveness of that technology. Just about all operating systems, even Windows, are built from that base.

But not all security professionals realize how extensive the open source base has become, and that now requires world-class, commercialized cyber security controls to ensure sufficient compliance support, and attack avoidance. We recently spent time with John Viega of *Capsule8* to learn more how data centers, cloud infrastructure, and other environments can benefit from improved Linux security.

EA: What statistics are available on the use of Linux in the data center and cloud?
JV: The adoption of Linux in Fortune 500 staggering. According to the Linux Foundation, Linux runs 90 percent of the public cloud workload. It's the operating system for more than 95 percent of the top one million domains and more than 75% of cloud-enabled enterprises report using Linux as their primary cloud platform. That's why it was such a huge market for Capsule8 to address. We went out and spoke with CIOs and CSOs at major companies and one of the main issue we heard time and again was that there was no solution focused on protecting Linux production infrastructure.

EA: What is your strategy for introducing improved security to Linux?
JV: Capsule8's main strategy is to provide real-time, zero-day attack detection and response for Linux-based production environments. And while everyone knows how big of an issue zero-day attacks are, no vendor has been able to bring that detection to the scale required for the production environment. In addition, with cloud-native technologies like containers now being widely adopted, traditional security appliances don't have the visibility needed to detect attacks. To address these challenges, we knew our solution had to be easy to deploy, effective, and scalable for all potential Linux production environments. No production environment is the

same and we had to be prepared to protect them all, whether containerized, virtualized, or bare metal. Essentially how it works is that Capsule8 deploys sensors throughout your infrastructure —in the cloud and the data center, on both bare metal and containers. These sensors run outside the kernel, to ensure the performance and stability of the workload. The sensors capture only small amounts of security-critical data, and stream it to nearby analysis instances, which can detect and respond in real time, allowing you to catch zero-days and other unwanted activity as they happen. And when Capsule8 detects an attack it can immediately disrupt that attack before it takes hold with an automated response such as automatically killing attacker connections, restarting workloads, or immediately alerting an investigator.

EA: Can you provide a simple explanation of what a container is and how you secure it?
JV: Containers are an OS-level virtualization method for running multiple isolated Linux workloads on a host using a single Linux kernel. Everything outside the kernel is virtualized, and the applications, runtimes and files in one container can't see other containers on the same machine, but they share an underlying operating system. Containers have not only allowed companies to pack more onto a single machine, they've made it much easier to build portable software that is continuously redeployed. They've become a key technology to enable micro-services and auto-scaling applications, and are now a staple in many continuous integration/continuous delivery (CI/CD) pipelines. When it comes to containers, there is a significant amount of isolation built in by default. One of the most significant issues with securing containers is visibility. When multiple containers live on the same machine and talk to each other, communication doesn't go over the network and can never be seen by an appliance—even a virtual appliance. You still don't have access to what is going on inside. The solution to container security lies within tooling that is container aware. By looking real-time into system, network and intra-container data, you achieve the level of visibility needed to know when something bad is happening inside of a container and can respond to it appropriately, such as shutting down or isolating the affected container.

EA: Why is it so difficult is it to detect attacks in production?
JV: Production has some specific challenges that have prevented past technologies from working well, and why many organizations have much better security for their endpoints than their servers. One of the biggest reasons is because things like performance and reliability generally trump security when it comes to production. Servers tend to deal with large numbers of transactions at once, and so performance overhead is a big issue. The CPU overhead to handle security processing needs to be very low, even when machines are under heavy load. And when it comes to reliability, if a bug in the security solution might cause the application to not function properly (or for the instance to crash), that's a huge issue. As a result, kernel modules are generally frowned upon in most environments, and the second there's a bug in production that can't be replicated outside of it, the security solution takes the blame and is ripped out. And, anyone trying to build a solution for production knows that production ecosystems are evolving extraordinarily quickly. Solutions must be able to deal with new cloud-native technologies to be effective, be container-aware, and so on. It's a huge challenge, and one we're willing to take on.

EA: What are the top few attacks you've been hearing about from customers?
JV: Meltdown and Spectre were big concerns for our customers and prospects, and a wakeup call to the industry. It wasn't just the breadth of processors affected, but how difficult it was to patch or remediate without causing even more damage, performance issues, and so on. And some of the patches hardly provided enough protection to be considered a mitigation at all. It forced companies to start prioritizing detection as part of their security strategy. When it comes to newly disclosed vulnerabilities, or even major high-profile exploits from the past like Heartbleed and Shellshock, real-time detection is what our customers want, and the problem we are trying to solve.

Telemetry-Based Protection of Applications

An Interview With
Sameer Malhotra
CEO
CIX Software

SECURING APPLICATIONS is especially difficult for several reasons. First, the rate of change for application software will always be greater than for underlying platform software, such as operating systems. Second, application software continues to be plagued by weaknesses in software engineering that produce bugs at a high rate. Third, applications vary significantly from one environment to another, and often include specialized legacy code with limited, isolated use.

The team at *CIX Software* understands this challenge and has been developing advanced solutions to help secure application software. The secret sauce for CIX Software involves combining real-time telemetry from each application environment with real-time analytics and response, which provides insight into application operations, as well as immediate response to potential misuse. We recently connected with Sameer Malhotra, CEO of CIX Software to learn more about the application security space and how his BUSHIDO platform works.

EA: Why has it been so challenging for enterprise teams to secure their applications?
SM: Enterprises are unable to effectively secure their applications because they do not understand their application environment, nor do they have visibility to gain that understanding. Mergers, acquisitions and divestitures have resulted in disparate and redundant systems. Tribal knowledge has been lost for legacy applications. In addition, while it is true that flat networks enable business, they also enable sophisticated threat actors, advanced malware, and insider threats.

EA: How does the BUSHIDO platform work?
***SM*:** It starts with real-time visibility from both agent-driven and agentless data. BUSHIDO looks at the process and identity details that drive each network connection, in addition to many other parameters. Network data alone is not enough. Additional context is necessary for complete visibility. This approach brings immediate value by building an intuitive Application Dependency Map with real-time data flows to help meet NYDFS, GDPR, SWIFT CSP and other regulatory requirements. We have partnered with many leading EDR and AV vendors to leverage investments in existing agents in the enterprise to achieve a zero-friction experience.

BUSHIDO uses machine learning to establish a true baseline for expected behavior, and then alerts and responds to anomalies in real-time. Automated responses to suspicious behavior include disconnecting users, killing processes, terminating network connections, and uninstalling software, among others. Finally, BUSHIDO combines active response capabilities with static micro-segmentation to ensure zero-trust security across every application, going far beyond network-level controls.

EA: What specific types of telemetry does BUSHIDO generate and how do teams use this information to advance security goals?

SM: We stream over 115 different parameters in real-time from live application environments. This telemetry can be broadly classified into network, process, identity, software and system metrics. This telemetry is used to create a baseline of behavior to ensure that anomalous activity is identified and prevented. It can also readily be combined with other data from the environment to enable effective security-related decisions and response. In addition, this information is persisted and can be leveraged by different teams; the SOC for real-time response and forensic review, DevOps to push application updates into the associated profile, and by IT Ops to understand system hardening and patch levels.

***EA*: Machine learning systems are notorious for having too many false positives. How does BUSHIDO address this problem?**

SM: BUSHIDO is a whitelist-based application and is therefore inherently less prone to false-positives. If a behavior is observed that is not part of an application profile, it either needs to be addressed, or added into the profile so it will not alert again. We have two methods of creating profiles to quickly get to a "known good" state: Machine Learned Profiling and Application Profile Definition. Machine Learned Profiling is the default methodology of the system. It allows the system to learn the actual day to day behavior of the application across all 115+ parameters and across time. This is stored as the application profile and is used as reference data for detecting anomalous behavior – Network, Process, Identity, etc. Application Profile Definition allows application teams to fully and dynamically define and control the behavior of their application. This is especially useful for agile development teams where application behavior definition can be part of their release/deployment process. Machine Learned Profiling and Application Profile Definition can work in tandem to eliminate the false positives. Alerts become meaningful and relevant. BUSHIDO also correlates alerts to discover related behaviors and actors, as well as to focus on common root causes of security and operational issues.

EA: Do legacy applications cause any unique challenges?

SM: Obviously, legacy applications with proprietary or even out-of-date technologies present significant security challenges. For example, they might be hard to patch if a serious bug is found. BUSHIDO was designed to handle legacy, home-grown and off-the-shelf applications. All applications have network, process and time-based behaviors specific to each implementation that need to be understood. Our powerful agent has broad OS support, including Windows, Linux, AIX, and Solaris. We even recently adapted it to z/Linux mainframe environments. This allows BUSHIDO to provide visibility, profiling, control and micro-segmentation across all environments: bare-metal, virtual, and container from the data center to the cloud.

EA: What are some application security trends you're observing in your customers?
SM: Micro-segmentation continues to grow in the community as something requiring advanced application security support. However, there are significant operational challenges with broadly deploying traditional micro-segmentation into enterprise environments. An application-centric approach is the only way to ensure success. Organizations also need comprehensive visibility first to provide value and prepare for segmentation. They also need to be able to distribute the effort to DevOps, SecOps and Infrastructure teams to each provide their own insights to effectively secure environments. We also see an increased need for real-time visibility and automated response capabilities during application execution to reduce the time-to-mitigation. The ability to truly understand and protect PaaS and container-based applications is dependent on these capabilities and is a major part of what we have built with BUSHIDO.

Workload Security Protection in the Cloud

An Interview With
Carson Sweet
CEO
CloudPassage

AS PERIMETERS have gradually diminished in their effectiveness as an enterprise control, the community has searched for alternatives to protect data and resources. Some have proposed encryption as the primary protector, but this does little to ensure integrity and availability – and has no bearing on useful telemetry for indicator analytics. The cloud micro-segment approach, in contrast, offers many useful benefits for every type of cyber security considerations.

CloudPassage has been one of the clear leaders for many years in protecting cloud workloads via containers in a DevOps environment. We recently caught up with Carson Sweet, CEO of CloudPassage, to ask him to share his experiences and insights into the best available methods for protecting cloud workloads, applications, and systems in the context of the speed with which DevSecOps processes now operate.

EA: What is meant by a micro-segment and is this a practical option for most enterprise cloud workloads?
CS: Every enterprise security team recognizes that a flat perimeter-protected network creates an opportunity for intruders to traverse from one portion of the infrastructure to another. This is how bad actors used entry points such as third-party portals to follow lateral, east-west paths to find unrelated assets such as point-of-sale terminals to steal credentials. Micro-segmentation is a powerful technique designed to address this risk by creating small compartments that do not include implicit trust. This is not only a practical option, but an imperative one. Our CloudPassage solution is designed to secure micro-segments in the context of virtualized data centers, enterprise networks, and network infrastructure.

EA: How does DevOps complicate – or perhaps enhance – the ability of a team to protect its cloud resources?
CS: DevOps enhances security by driving focus on automation. With the speed of exploits becoming too great for any human-time process to address, modern software development lifecycles must be adjusted to move more quickly to prevent exploits. DevOps certainly does speed things up during development – and must hence be properly protected with a great

platform. But with the best support for telemetry collection, continuous compliance, and fast mitigation, DevOps processes will be an improvement over traditional SDLC methods.

EA: Tell us about the Halo platform and how it works.
CS: Halo is a SaaS-based security automation platform that protects cloud and virtualized computing. The platform is automated, and integrates into infrastructure through REST APIs and micro-agents, often via deployments that can be completed in less than an hour. The Halo platform monitors traditional bare-metal servers, cloud workloads, container images and instances, and public IaaS services and resources. These assets are discovered and continually monitored for security exposures and compliance issues. The platform alerts the security team to vulnerabilities that might exist, with great visibility and control across the hybrid enterprise; more importantly, the platform provides multiple integration points to allow developers and operations teams to automate remediation. One Halo customer reduced over 60,000 critical vulnerabilities to under 100 in a matter of months using this automation approach.

EA: What is the greatest challenge for teams with legacy architectures to move to a more modern cloud solution?
CS: The good news is that the shift from legacy enterprise to more hybrid and pure public cloud usage is becoming a reality in just about every sector, in companies and organizations of every size and shape. So, the technical and architectural challenges are clearly being worked out. Obviously, compliance obligations remain as data handling control shifts from internal to external resources, but with Halo, we believe we help to ease these concerns through visibility and automated compliance support.

EA: Have you seen recently any new types of cyber attacks to cloud resources?
CS: The offense continues to innovate, but we continue to see the same general strategies for attacking cloud resources just adjusted to the new architecture. For example, where credential theft was previously around finding passwords for legacy hosted applications in the local data center, now the same techniques – often based on simple phishing – are used to obtain credentials for as-a-service applications hosted in cloud.

Network Security with Emphasis on Software

An Interview with Bruce Gregory *CEO* *Corsa Technology*

NETWORK SECURITY has evolved from simple devices on IP networks beaconing telemetry to a correlation engine, to more advanced platforms that understand the intricacies of software-defined network infrastructure and complex network service delivery environments. Emerging SDN-based switching, routing, and mitigation form a core for a new generation of network protections for a world that will be ever-more dependent on cloud.

Corsa Technology understands this evolution and focuses its efforts on open programmable networks, and how such technology can be protected most effectively with modern cyber security functions. We recently spent time with Bruce Gregory, CEO of Corsa Technology to learn more about how his company is addressing this space with solutions for programmable in-line security on any size network. In conjunction with existing threat detection, SIEM and analysis tools, Corsa dynamically scales up network security functions to manage illegitimate traffic entering or leaving a network.

EA: What are the main network security functions that your team focuses on?
BG: From a high-level perspective, the best way to think of Corsa is as the enabling hardware platform for a software-defined security solution. Corsa acts as a transparent control point in the network that sees the network traffic and can act on that traffic under the direction of multiple sources of analysis, interpretation, and orchestration. We enable a concept called Security Function Virtualization to create dynamic security service chains that are orchestrated to meet customer demands – on the fly. We are talking about a true software-defined security capability that allows customers to deploy their trusted cyber security solutions dynamically and at scale at key points in their network. Think of it as implementing a 4th generation software-defined firewall with Corsa as the high-performance hardware that enables the security functions to run as dynamic service chains on commodity servers.

EA: What is your strategy for using SDN-based controls to improve network protections?
BG: SDN was all about the disaggregation of software and hardware to try and simplify the underlying physical network while enabling future services to be created and managed simply and efficiently. The service provider world created Network Function Virtualization to bring

cloud economics to bear on the service provider market and SDN is the architecture that strongly supports NFV. When we looked at cyber security, we realized that the same concepts could be applied to great advantage. If cyber threats are constantly evolving, then the cyber defenses need to evolve at the same pace. Rather than forcing a customer into a fixed function defense, we felt strongly that enabling a dynamic environment where the right capability could be spun up on demand would bring real value to our customers. We give the customers an ability to create and test environments that consist of diverse analytics and detection capabilities, creating truly software-defined security strategies that can be deployed on high speed network links.

EA: Does your team focus on addressing a single threat?
BG: The real value in the Corsa solution is that it enables multiple threat responses all on the same platform. In the Corsa architecture, we enable everything from the simplest of blacklists to the most complex combination of AI based threat hunting across a network. We don't pre-define what the overall solution looks like, we enable customers to combine their preferred analytics and detection packages into dynamic hunters that can then be scaled out or up using the Corsa platform to programmatically create the dynamic security function chains appropriate to the defense strategy.

EA: Can you explain the key differentiators of your platform versus other commercial offerings?
BG: The reality of network security is that we can't inspect all network traffic all the time for every possible threat. We must move away from today's brute force inspection of all traffic. We look at it as 'The Art of War' where an attack happens one way, and you creatively counter in a non-obvious way. Adjust, flex and bend, but never fail. That requires a dynamic software-defined security capability, and Corsa uniquely provides the foundation on which to build that solution. Corsa uses the dynamic power of SDN service-chaining and granular flow forwarding to create a software-defined security solution that lets users programmatically provision what is needed. IDS, IPS, and deep packet inspection (DPI) are added as required within this dynamic, scalable software-defined security solution. Unlike other offerings that have embedded, pre-defined security features, Corsa intelligently enables the use of abstraction, orchestration, and AI to dynamically classify traffic to whatever type of security inspection or function is required. Security functions can change or be modified on the fly to optimize the overall security posture with the Corsa foundation intact and able to automatically scale and adjust as required.

EA: What are some network security trends you are observing from your customer base?
BG: There are a few significant trends we've noticed – the first is flexibility with explicit control. Customers want orchestration of playbook scenarios – when a threat is detected, they want the overall system to help them run a playbook to deal with it. That playbook is an instantiation of a software-defined response, but it's critical to realize that along the way to full automation, we will spend time with humans guiding or approving the playbook. So, fitting into an orchestrated environment that has a human making the final decision is a necessary step. The system must be ready to move to full automation, but must accommodate the operators' desire to maintain that final authority. Encryption is one of the most challenging issues – most traffic on the

Internet is encrypted and mostly legitimate, yet we know that hackers take advantage of the trusted nature of encrypted traffic to embed threats. Having a capability to direct encrypted traffic differently from unencrypted, or trusted encrypted traffic differently from untrusted encrypted traffic, with the ability to change those classifications on the fly, is highly desirable. Finally, we are seeing a push to disaggregation and open interfaces. Security operators are used to having a diverse set of functions and interfaces in their arsenal. What they don't like is the complexity and cost of that arsenal, particularly for something that delivers less than optimal protection and is comprised of proprietary products. They are looking for an environment that allows them to instantiate the right threat response at the right time. This is hard to do in a production environment, yet it's the only way to create dynamic defense, and that's why Corsa took on the challenge of building one of the keystones of that dynamic defense architecture.

Privileged Access Security for Enterprise

An Interview with Nir Gertner *Chief Strategist CyberArk*

ASK ANY attacker what would be the most attractive area of a target enterprise to gain offensive advantage, and they will inevitably point to the typically weak management of privileged access. Incident after incident in recent years has involved malicious exploitation of weaknesses in this area. Given the broad, powerful access that privileged accounts provide, adversaries have thus learned to focus their attention here.

As a result, advanced solutions for improving the protection of privileged access are now considered essential to enterprise security for organizations of every size and shape. We recently spent some time with Nir Gertner, CyberArk's Chief Security Strategist, to learn how the field of privileged access security is evolving, and how the modern enterprise can benefit from use of a world-class solution for protecting privileges and reducing risk.

EA: Why do you suppose enterprise security teams have struggled with privileged access security traditionally?

NG: Nearly all advanced attacks involve the exploitation of privileged accounts, which provide powerful access to organizations' most sensitive data, applications and infrastructure. It's critical that these accounts are protected - the security of an organization's crown jewels depend on it. While the risks of unprotected privileged access is known, with increasing investments in key areas such as cloud technologies, the privilege-related attack surface is expanding exponentially. Many organizations simply don't know where all their privileged accounts exist – and therefore lack visibility into where they are most vulnerable. This challenge intensifies when you consider that it's no longer just human access that needs to be secured, organizations must also manage, monitor and control privileged access for applications and machine identities. Reactive approaches and traditional security defenses that aim to keep attackers out of the network are simply not enough. Attackers are innovating at an accelerated pace, finding new ways to steal credentials, infiltrate networks and halt business operations, so a "set it and forget it" method for enterprise security is sure to fail. A long term, programmatic approach is required. This explains why CyberArk encourages our customers to "think like an attacker." CyberArk strongly recommends the use of Red Team services to simulate attacks and

identify areas of weakness in IT infrastructure that could be exploited by an attacker, then help organizations prioritize and implement a proactive security program.

EA: Tell me about your company's Privileged Access Security Hygiene Program?
NG: One of the most effective, preventative steps an organization can take to bolster its security program is to secure privileged accounts, credentials and secrets. That's why we've developed the CyberArk Privileged Access Security Hygiene Program – a programmatic, risk-based approach for helping organizations prioritize privileged access security to improve their overall security posture. The program is based on the extensive experience of CyberArk's security services team in responding to significant data breaches. It is designed to maximize risk reduction in the most effective, efficient way possible. Real world insights are built into customized, step-by-step goals and an actionable process for eliminating irreversible network takeover attacks, limiting lateral movement, protecting third-party application credentials, defending DevOps secrets and more. Implementing this type of holistic program, built to evolve over time as an organization matures its approach to privileged access security, will help organizations achieve greater risk reduction in less time, and help satisfy security and regulatory objectives with fewer internal resources.

EA: How does your solution approach this challenge of managing privileged access?
NG: The CyberArk Privileged Access Security Solution is the industry's most comprehensive solution for protecting against the exploitation of privileged accounts, credentials and secrets anywhere – including on the endpoint and across on-premises, hybrid cloud and DevOps environments. It eliminates advanced cyber threats by identifying existing privileged credentials across networks, making sure those credentials are locked down and secure, and leveraging advanced analytics and continuous monitoring to detect and isolate anomalous behavior to stop attacks early on—before they cause irreparable damage. Built on a shared technology platform, the CyberArk Privileged Access Security Solution is designed with a "security first" approach to integrate into any IT environment, and delivers enterprise-class security, scalability and high availability in a single integrated solution. With this flexible, modular solution, organizations can better protect their networks by securely storing, rotating and controlling access to credentials and keys; isolating, monitoring, recording and controlling privileged sessions on critical systems; and providing targeted, immediately-actionable threat alerts.

EA: What are some emerging areas of privilege-related risk and why?
NG: We are seeing many emerging areas of potential privilege-related risk, particularly with technologies associated with Internet of Things (IoT). Robotic Process Automation (RPA) is another emerging space - especially for customers in financial services and banking industries. RPA is software that can be used to intelligently automate rules-based business processes. RPA software interacts directly with business applications, databases and systems, mimics the way humans work, and mirrors how applications use credentials and entitlements. RPA tools need "power access" (or privileged access) to do a job — whether it be logging into a system to access data or moving a process from step A to step B. In a financial services organization, for example, RPA tools can have access to sensitive financial or transactional systems, which are tempting targets. An attacker who gains access to the RPA password

storage, console or source code can take full control of the robots. Just like any other compromised application, attackers can leverage powerful privileged credentials to do their bidding — but with RPA, it's at an even greater scale. Most organizations employ multiple — sometimes hundreds or even thousands of—software robots, which access multiple systems and perform multiple processes simultaneously. Thus, you can appreciate the magnitude of risk to the enterprise. Through the C^3Alliance, CyberArk's global technology partner program, CyberArk is integrating with some of the world's leading RPA players, including Automation Anywhere, BluePrism, WorkFusion and UiPath, to provide a simple, easy-to-deploy and cost-effective solution to manage risk associated with RPA adoption.

EA: What are some emerging cyber attack vectors you've been hearing about in the field?
NG: Over the past year, we've seen multiple organizations attacked due to increasing use of cloud and DevOps. For example, as we saw with the Uber breach a spotlight needs to be put on the critical security vulnerabilities created by privileged credentials that are often left unmanaged and unprotected – especially at companies that are using DevOps and the cloud to bring new applications to market at high velocity. Additionally, CyberArk Labs and the CyberArk Red Team are constantly researching and assessing emerging attack vectors. One area of interest is crypto-mining. Attackers are changing their ways and moving from go-to cybercrime monetization tactics – like ransomware and credit card theft – toward a new breed of malware: crypto-miners. Attackers are increasingly moving to crypto-mining-based attacks because there's more "bang for their buck." With ransomware, once it's propagated, they must hope that the target pays the ransom. In crypto-mining, it's a bit different. It's running on a target (like an infected machine), so they immediately see monetary gain. They don't need to wait for the victim, they begin mining. And we're just at the beginning stages. Organizations must prepare for the rise of the crypto-miners. In fact, earlier this year, it was reported that thousands of websites, including ones run by U.S. and UK government agencies, were infected with crypto-mining code.

AI for Cyber Security

An Interview With
Stu McClure
CEO
Cylance

PROTECTING ENDPOINTS from the negative effects of malware has transitioned from early signature-based software to advanced, modern use of AI-based algorithms. This is good news, because AI has experienced a wonderful surge in recent years due to improved parallel processing and better underlying computing support. Detecting variants and more subtle exploits are thus more feasible.

Cylance has been a clear leader in developing the technological advances required to use advanced algorithms based on machine learning and related methods to substantially reduce cyber risks to endpoints – and the entire enterprise. We recently spent time with Stuart McClure, CEO of Cylance to ask his advice on how this technology approach is maturing and to learn more about trends in this area of cyber security.

EA: Can you briefly help us understand how AI can be used to reduce cyber risk?
SM: The development of AI-based models to detect patterns is the basis for how the CylancePROTECT works. We create our models using the most advanced algorithms available, and they are designed to detect both zero-day and known exploits through automated learning assisted by our expert team. A good way to understand the power of AI to reduce cyber risk is to recognize the subtle differences that exist between malware variants. So, just as AI technology can be used to detect subtle differences in images, it can also perform similar recognition for malware.

EA: Do you see modern endpoint security improving overall – or are we just keeping up with an advancing threat?
SM: Cyber security at the endpoint is certainly improving, and we're excited that our AI technology has been playing such a vital role in this advance. But the reality is that the threat is advancing just as quickly. We've tried to create an ecosystem for the enterprise to get ahead of these threats through a combination of endpoint software as well as services we provide to improve accuracy, relevancy, and efficiency.

EA: Tell us about your solution offering and how it has evolved.
SM: Our flagship offering is the CylancePROTECT offering for endpoint security using our AI models. We also provide a consumer-oriented antivirus solution called Cylance Smart Antivirus, designed to optimize the day-to-day needs of individuals on the Internet. CylanceOPTICS provides AI driven incident prevention, machine learning assisted threat detection, root cause analysis, smart threat hunting, and automated detection and response capabilities that are fully integrated with CylancePROTECT. Our Cylance TheatZERO offering provides advanced analytic support for enterprise teams in assessing damage, managing remediation, and supporting response. We also provide our customers with a range of consulting services to enhance our support during the entire anti-malware lifecycle.

EA: Any interesting malware you've seen recently? You've had as much experience looking at exploit code as anyone in the world.
SM: Cyber exploits are growing more intense each day, as anyone attending DEFCON will attest. More frightening ransomware attacks have emerged recently, as have better social engineering methods to dupe unwitting employees and citizens into giving up their personal information. Many new attacks target credentials, especially in cases where the credential store is centralized on a flat corporate network.

EA: What are some security trends you are observing from your customer base?
SM: Just about every enterprise today is dealing with the transition of business unit activity to the public cloud. This is good news from a financial perspective, and it does introduce more flexibility in new services and reduced cycle times for business feature addition or modification. But it also introduces new demands from a security perspective, especially in the obligation to protect the endpoint from connectivity to a wider range of externally-managed services.

Applying Deep Learning to Cyber Security

An Interview With
Guy Caspi
CEO and Co-Founder
Deep Instinct

CYBER SECURITY teams have come to recognize the immense potential protection value and benefits of artificial intelligence, machine learning, and more advanced methods of deep learning that are available from the technology community. The challenge, however, is how to best integrate these exciting new techniques into practical tools that can reduce cyber risk in a meaningful way.

One company that thoroughly understands the technology associated with machine and deep learning algorithms and methods is *Deep Instinct*. We recently had the opportunity to sit down with Guy Caspi, CEO of Deep Instinct, to ask his advice on best practices in deep learning (and how it is different from machine learning), as well as how his team's platform implements such advanced technology into its cyber solution.

EA: Can you help us understand deep learning and how it relates to the more commonly-referenced machine learning?
GC: Machine learning is a field of algorithms in artificial intelligence (AI) where a machine can learn from a closed dataset and make decisions without being explicitly coded. Deep Learning is the most advanced family within AI today, and is based on advanced algorithms that focus on being highly accurate at detection, with minimal false positives. Deep learning is a unique approach in AI for the following reason: In machine learning, you must have a human expert extract relevant features from the object (file, image, text etc.), converting them into a vector of attributes, and then feeding the machine. The expert is telling the machine what to look at, and what to analyze. The problem is that humans make mistakes, and the pace of change in cyber security is so high that no expert can cover all the relevant features and their changes (mutations) by extracting features. As a result, most of the available data (content) of the file is getting lost, with some estimates at only 2.5%-5% of the data being analyzed. In addition, machine learning is a linear model, looking at each feature on its own, without analyzing the correlation and context between the data and features. With deep learning, in contrast, you don't have any feature extraction by experts. Using a deep neural network architecture, the machine is exposed to the raw data as is. Deep learning is the first and only method capable of training on the raw data as is – and the results are clear: Machine learning solutions are mostly

effective against known threats; they suffer from high false positive rates; and they cover limited files types. Deep learning is thus the only effective technology against unknown first-seen malware, providing the highest detection rates and lowest false positive with minimal human involvement.

EA: How does the Deep Instinct platform work in the context of enterprise cyber security?
GC: Deep Learning performs well when huge data sets are involved, when the problem is very hard to solve, and when the data is complex. In these cases, most existing available solutions fall short, whereas deep learning methods perfectly address the cyber security needs. Our Deep Instinct platform is thus being used to predict and prevent malware pre-execution. This means being able to predict if files or processes are malicious before they are causing any harm, and then preventing them from running. This is a fundamental difference from any of the existing detection and response solutions in the market today, which wait for something to happen. Due to the infrastructure-agnostic nature of deep learning, we are applying this technology in many different areas of the enterprise like endpoints, mobile, servers. We are also planning to expand into other areas, such as network traffic and IoT.

EA: What are some common use-cases that arise in the practical application of your platform to the enterprise?
GC: As in the previous question, the common use-cases involve prediction and prevention of malware, including attention to fileless exploits. The ability is second to none for deep learning to learn and predict – which is the same as with face recognition, voice recognition, autonomous cars and many more. Therefore, the ability to predict how new malware is going to look and behave is amazing. It can be applied to any type of organization; it can support any type of OS and type of device; and it can protect against any type of threat including file-based (any type of file), fileless threats, ransomware, and so on. We often say that If we can train it, we can protect with it. An additional value to deep learning, besides protection, is efficiency. Our Deep Instinct platform is an autonomous solution, which implies no need to have an army of SOC experts to detect, analyze, response, remediate, and run forensics to find a needle in a haystack. Everything happens in a fully automated manner without any human involvement, thus letting the human expert deal with what is truly important.

EA: How accurate is deep learning in recognizing cyber exploits, malware, and other indicators of interest?
GC: Deep learning techniques represent the most accurate cyber attack detection solution available today on the market. Typical metrics we've seen include above 98% detection success with unknown first-seen malware and less than 0.001% false positive on average. These are amazing metrics that could never be achieved with conventional malware detection methods. Enterprise security teams are strongly advised to pay close attention to this technology.

EA: Is artificial intelligence living up to the hype we all see in our industry?
GC: Well, let me answer your question this way: Saying that someone uses AI today is like saying generally that they use the Internet or are digital. Such statements don't provide useful information. For example, almost every software today uses some form of AI. We need to be

more specific and accurate in our references to the technology. We believe that deep learning has achieved the biggest advances in AI history. By some estimates, this technology has produced 20%-30% improvements in almost every field to which the method was applied, and in many cases, it performs better than human beings. But we also need to understand its limitations. Deep learning does require a huge dataset for training; it does need the know how to build the right data set, or results will be biased; and it does require complex algorithms with the commensurate need for data scientists and deep learning experts to know how to work with the tools. In addition, publicly-available deep learning frameworks aren't designed for cyber security, so you can't just take a framework built for image recognition and use it for cyber security. At Deep Instinct, we address these challenges by building our platform from scratch, using a proprietary deep learning framework for the specific needs of cyber security.

Shrinking the Attack Surface with Vulnerability Mgmt.

An Interview With
Gordon MacKay
EVP and CTO
Digital Defense

MOST PRACTICAL cyber security professionals understand the importance of getting the basics right in their day-to-day enterprise protection initiatives. Much of this baseline works centers on correctly managing vulnerabilities to the corporate assets. This has been a manual process for many years, but automation has improved its efficacy and crated opportunities for enterprise security teams to take vulnerability management to the next level.

Platforms for vulnerability management are best created in the context of detailed and expert understanding of both cyber security threats, as well as trends in information technology management. The team at Digital Defense is thus well-positioned to support this discipline. We recently connected with Gordon MacKay, EVP and CTO of Digital Defense to learn more his team's fine work in this important area of vulnerability management.

EA: We often hear your team recommend getting "back to basics" for reducing security risk. Tell us what you mean?
GM: We are discussing maximizing the return on investment of your information security program by making sure its foundational components are being used in an effective, programmatic fashion. I often see and hear about fancy new security solutions marketed as being able to protect organizations against all types of security attacks. The truth is, there is no silver bullet when it comes to cyber defense. Getting back to basics means having a sound defense strategy of cybersecurity capabilities that helps manage cyber risk. Managing risk means first understanding and knowing where you stand, and second, knowing how to continuously drive down the risk and keep it to a known acceptable level. Determining one's risk means understanding the value of one's assets and the possible weaknesses surrounding these assets, as well as the types of threats to which the assets will be subjected. Through our Frontline.Cloud platform, Digital Defense has been helping organizations determine their

security risk posture for many years by enabling our clients to get an in-depth understanding of the location of an organization's network assets and associated cyber-security weaknesses.

EA: Frontline VM™ is cloud based. How does it work?
GM: We like to say we were born in the cloud. Our Frontline VM solution has been cloud-based from day one. Our VM solutions "scan" an organization's IP address space both from outside the network, as well as from within, to effectively identify all network devices and applications and evaluate the security posture of each device and application found regardless of type. This network and application scanning and vulnerability analysis allows organizations to understand the external and internal risk postures of these network assets. For external scans, premise-based hardware or software is not required. We scan externally facing endpoints from our cloud, which now resides in the Amazon Web Services (AWS) cloud. For internal scans, we send clients one or more scanning appliances, which are placed in strategic locations within client networks and/or virtual private clouds (VPCs). These appliances, available in many form factors (virtual which can be sourced from the AWS marketplace or physical) then call-home, and take command and control from our Frontline.Cloud platform. The internal scanners, when directed to do so, assess internal network-based devices. In both external and internal scanning cases, the results come back into our cloud. The client benefits from the ability to view and manage these findings within our proprietary Frontline VM portal. This cloud-based architecture has many advantages for our clients including, but not limited to, fast deployment around the globe and the availability of multiple VPCs in different countries enabling us to effectively address data residency requirements. Our cloud-based platform architecture also allows us to scale to any size to meet the needs of clients, both large and small.

EA: What major challenges exist in managing vulnerabilities and reducing risk?
GM: Three top challenges we have observed in the industry specific to managing vulnerabilities are a technical host correlation challenge (which is poorly solved by most VM solution providers on the market), SecOps challenges, and security integration challenges. The host correlation challenge is faced by all VM solution providers. VM requires ongoing assessments across time, such as monthly, weekly, daily, or continuous. Any given point-in-time scan may assess numerous devices within a network. It's important that the VM solution correctly match a given asset as assessed within a given point-in-time scan to its correct counterpart as assessed at a different point-in-time scan. If this is not correctly done, and the VM solution mistakenly matches a scanned host to an incorrect counterpart within a different point-in-time scan, incorrect conclusions are claimed by the VM solution, such as vulnerabilities having been fixed when in fact, they remain. This subtle challenge is sometimes overlooked or misinterpreted and unfortunately, organizations unknowingly spend significant time and resource compensating for the problem or leaving assets exposed to possible security breaches. Digital Defense has patented technology that overcomes this prevalent shortcoming in enterprise networks. The second challenge relates to people and processes. In many organizations, the security team is not the same as the IT operations team. When remediation is required for identified vulnerabilities, these findings are typically assigned from a centralized security team to different IT operations teams. Tensions may arise from the requests made by IT Security to IT Operations to remediate vulnerabilities, as each team may have different resource levels and

priorities. Digital Defense helps alleviate this tension by assigning optional Personal Security Analysts (PSAs) to serve as a bridge between IT Security and IT Operations. The PSA constructs scanning programs that align with the requirements of IT Security in terms of scan frequency and device coverage as well as compliance reporting. In addition, the PSA assists IT Operations in the form of remediation prioritization and resolution guidance. The third challenge is related to technology and process integrations. Since there is no security solution which solves all the world's security problems, organizations have many different security solutions which help with different parts of organizational security risk. Ideally, these are integrated and work together in a seamless security ecosystem. It's never like this, of course, in the real world and as a result, there are often blind spots and things forgotten which adds to the "I don't know what I don't know" part of the risk equation. Digital Defense works extensively with partners and customers to assist with security automation initiatives. By leveraging Frontline.Cloud Application Programming Interfaces, effective integration with a wide variety of 3rd party security and compliance platforms can occur. The same level of accuracy enjoyed within Frontline.Cloud is made available to those platforms with which Frontline.Cloud is integrated resulting in a more robust end-to-end security ecosystem.

EA: Are there activities in vulnerability management that some teams do better than others?
GM: Yes! VM includes many sub-activities, each of which has challenges we must overcome. A white paper can be found on the Digital Defense website that describes a vulnerability management maturity model – VM3. The VM3 paper covers these challenges and the evolution and processes involved in building a mature VM program. Organizations can raise VM maturity by first determining the current state of maturity of the vulnerability management program in place and then introducing new processes or process enhancements required to achieve higher levels of maturity. It is important to note smaller organizations may grapple with different issues as compared to larger ones. However, even though a smaller organization may have less money to spend on security, fewer dollars doesn't necessarily mean smaller organizations will find it harder to overcome issues that may be an impediment for large organizations to reach the next level of maturity. One such example is remediation speed. A larger organization may find it more difficult to achieve a faster remediation speed metric as compared to a smaller organization due to more complex team dynamics being present within larger organizations.

EA: You mentioned integrations help ease VM. Could you give us some details on some of the integrations that help organizations better manage the VM process?
GM: We place a great deal of importance on empowering our clients to better manage risk by way of integrating our solution with many other security, and non-security solutions. These integrations help automate organizational workflows and processes, which ultimately reduces an organization's security risk. We have a dedicated team of software developers who design and implement integrations with other solutions. For example, we have integrations with many ticketing and remediation solutions such as ServiceNow. This solution addresses a use-case enabling the automatic opening and assigning of a ticket to a member of the IT Operations team. In this case, the ticket was opened against an asset, which had been scanned by the VM solution, was determined to have vulnerabilities of a certain level (e.g. critical level

vulnerabilities) thus leaving it potentially vulnerability to cyberattacks. Another example is our integration with ForeScout, a Network Access Control (NAC) solution. This integration allows the NAC to act based on an endpoint's security posture as determined by the VM solution. For example, the NAC may prevent an endpoint from gaining access to certain corporate resources if that endpoint has been found to have high-level vulnerabilities by the VM solution. This is a great solution for organizations that have employees that are mobile in nature. Finally, one of our most recent integrations is with McAfee ePolicy Orchestrator (ePO), a security orchestration solution. With this integration, McAfee ePO pulls in assets and vulnerabilities from Frontline VM and then allows the client to set security policies based on all the information within the orchestration solution. One of the big benefits of this integration is the asset discovery capability which identifies unmanaged hosts and enables rapid, automated deployment of threat detection agents on these devices. By dramatically reducing the population of hosts that were unknowingly in an unmanaged state rapidly drives down an organization's security risk.

Advanced Data Protection for Modern Enterprise

An Interview With
Ken Levine
CEO
Digital Guardian

ONE OF the most obvious cyber security threats that plagues every modern organization involves leakage of sensitive information to unauthorized observers. The motivation for such attacks can range from disgruntled insiders wanting to cause embarrassment to their current or former employer, to nation-state actors wanting to affect or influence critical infrastructure operations – and this includes elections.

Traditional data loss prevention (DLP) addressed this threat and was a welcome risk reduction. But DLP firms have had to improve their methods to deal with the ever-increasing intensity of insider and advanced externally-controlled attacks targeting sensitive data. We recently connected with Ken Levine, CEO of *Digital Guardian* to learn how his team combined DLP with endpoint detection & response (EDR) and user & entity behavior analytics (UEBA) into a single agent for a consolidated enterprise data security solution.

EA: How does DLP fit into a modern enterprise security architecture? How does this relate to EDR?
KL: Every modern cyber security team understands that DLP functionality is required anywhere sensitive data might exist throughout the extended enterprise network. In the early days, this meant putting a solution at the Internet gateway, and soon this expanded to protecting endpoints and cloud storage. The Digital Guardian Data Protection Platform integrates protections across the modern enterprise, and we've thus developed a solution that effectively covers DLP, EDR, and UEBA needs. Protecting data is the goal; advanced data protection must contain safeguards for sensitive information from both insider threats as well as external adversaries. DLP protects against insider threats while EDR detects and responds against outside attackers who are determined to penetrate and exfiltrate sensitive data.

EA: Does your platform generally focus on insider leaks, externally controlled exfiltration, or both?
KL: Sadly, both types of attacks continue to increase in their frequency and severity. Security teams originally trusted anyone within the bounds of a perimeter-protected local area network

(LAN), which resulted in breaches of trust by disgruntled or compromised insiders. Once this was addressed by DLP, the risk of malicious breaches caused by external actors wanting to exfiltrate data became an issue, especially with the rise of nation-state originated advanced persistent threats (APTs). Our EDR solution is designed to protect endpoints that might be compromised into leaking sensitive data; we uniquely see not only these risky activities, but can tie back to the data impacted. This gives InfoSec teams knowledge into incident severity. Finally, UEBA functionality understands the actions taken by users, machines, and applications and it alerts when risky or unusual behaviors occur, regardless of the actor.

EA: What are some recent advances you've introduced to your platform?
KL: We recently became the only DLP provider to embrace a fully cloud delivered security model to eliminate the deployment and support costs and complexity with on-premises software. This SaaS is also available as a fully managed service for organizations that want to rely on data security experts to run their operations. The Analytics & Reporting Cloud (ARC) relies on a big data backend that our team has developed and built to deliver the processing power to recognize and understand the real risks in the volume of events in every enterprise. At Black Hat this year, we announced User & Entity Behavior Analytics to enhance our DLP and EDR solutions and to bring more context to data protection. We've created a visualization platform that allows CISOs to understand enterprise wide risk, and that enables analysts and hunters in the SOC to respond and remediate threats faster than was ever possible in the past.

EA: Do you think that many of the more prominent breaches in recent years, including some political and election-related hacks, could have been prevented by DLP and advanced EDR technologies?
KL: No one can ever say for sure if some incident could have been prevented, because so many factors influence an incident, especially ones as complex as political or election-related hacks. But every security expert in the world would agree that DLP, EDR, UEBA, analytics, response, and other features of the Digital Guardian platform will significantly reduce the risk of compromise to any enterprise, government, or other organizational infrastructure.

EA: What are some key cyber and data protection-related issues you've been hearing from customers?
KL: The demand for analytic tools seems to be increasing at a dramatic pace. This explains why we've worked so hard on our ARC, and why it has been so well-received by our customers. We also see great demand for the use of cloud to augment the capabilities deployed to the enterprise – and, as you would expect, we provide virtualized analytics in the DG ARC. In addition, our solutions have been designed to help, and, in fact, drive, reduced cost and complexity. Digital Guardian's single-agent consolidated DLP, EDR, and UEBA delivers the insider and outsider threat protection for sensitive data without the complexity of multiple, standalone solutions. Our SaaS model further eliminates barriers to security.

Securing all Forms of Sensitive Data

An Interview with

Tony Pepper
CEO
Egress Software

SECURING DATA generally requires attention to both structured and unstructured formats. Most attention to date has been placed on structured data security. This emphasis is certainly helpful, but so much of what a business does on a day-to-day basis involves unstructured data in the format of emails, and documents that need to be transferred. And such transferal generally does not include much pre-arranged infrastructure support.

The team at *Egress Software* works hard to address these concerns with a range of security solutions designed to support discovery and classification, email and file protection, file collaboration and many other practical business functions primarily for unstructured data. We recently connected with Tony Pepper, CEO of Egress Software to learn more about how his solutions work and what we should expect in this important space.

EA: Why has it been hard traditionally for business users to properly protect their email?
TP: Typical collaboration and email encryption tools either struggle with usability or make significant security trade-offs that don't meet the demands of highly regulated industries or mitigate the risk presented by the insider threat. When these types of limiting, and often complicated, tools are provided to users as a one-size fits all, it's often in conflict with the way the business needs to engage with its customers in a more seamless way. As a result, users often bypass controls, use shadow IT, or take unnecessary risks. At Egress, we offer something different; a platform approach to data security that enables customers to manage the risk of sharing unstructured data. The platform empowers users to easily and securely collaborate and share sensitive data, without any security trade-offs. This includes email messages and attachments, documents, and multimedia content such as audio and video files, which are increasingly created and shared across the Enterprise. What makes our approach so unique is the way in which we wrap security around the user and manage their experience through machine learning and artificial intelligence (AI). This User-Centric approach helps individuals avoid potential mistakes, such as the accidental send, but also provides security administrators

with insight into behavioral anomalies across the business. This not only helps organizations meet and maintain stringent compliance requirements, but also mitigates the risk of a major data breach.

EA: How do your solutions work?
TP: From a technology perspective, we have always recognized that for data security solutions to be effective in today's Enterprise, they need to offer a flexible, fully integrated and easy-to-use experience that delivers real value back to the business. Which is why Egress is delivered as fully cloud, hybrid or on-premise and uses behavioral analytics and artificial intelligence to drive intuitive, easy-to-use data security solutions, aimed at promoting user engagement which in turn helps organizations improve employee productivity and awareness of day-to-day security risks. For our customers, this means they can be confident that their staff are sharing information with the right people and applying appropriate levels of protection, helping them maintain compliance with regulations including HIPAA and NY DFS 23 NYCRR 500 and GDPR and the evolving US State data privacy mandates.

EA: Many users employ in-the-cloud email and file management services today. Does your platform integrate with these virtual offerings?
TP: Yes. These days, with more and more organizations moving to Office365 and G suite, or hybrid combinations of on-premise and cloud services, seamless integration into these platforms is a must. While these third-party platforms do offer basic sharing and protection capabilities they often struggle to meet today's security and compliance requirements, be that the need to share multiple formats of unstructured data including large files, provide assurance over data residency, control and manage access from mobile devices or meet the auditing and reporting overhead imposed by todays stringent regulations. Although traditionally these have been requirements for our customers in highly regulated industries such as Government, Financial Services and Healthcare, increasingly we find organizations across a wide range of sectors facing similar challenges, which makes our technology more important than ever.

EA: How do the encryption and key management work on your platform?
TP: We're best in class – utilizing AES 256-bit FIPS 140-2 approved encryption, with a cloud-based key management platform we're able to offer end-to-end security on a global scale. We take advantage of the major cloud providers' global footprints to enable a distributed architecture with central control. Of course, besides key management, an Enterprise needs seamless authentication of users as well as the ability to recover and discover encrypted data for a variety of compliance and legal requirements. Our key management architecture supports these requirements today for millions of users, and unlike many security providers, we also offer first line support to all third-party recipients, which takes away a huge cost burden for organizations. Not surprisingly our customers and users alike love that, a lot!

EA: What are some trends you're observing in your customers?
TP: Across the board we're seeing organizations coming to us with increasingly complex security and data sharing requirements. I think there are probably three major reasons for this. Firstly, the huge increase in unstructured data, which IDC estimates has grown at over 300% in

three years means more digital files are being shared by more individual users than ever before. The question is, how do you ensure the security and management of this data whilst not getting in the way of it being shared? Well if you believe the research, the answer is not very well in most cases. Data breaches continue rise and in 2017, most records were breached because of accidental loss by staff, or to give it its fancy name; the Insider Threat*. Secondly organizations are increasingly fearful of this heightened security risk, and thirdly they are having to tackle these challenges whilst dealing with increasingly sophisticated regulations imposed by for, example NY DFS 23 NYCRR 500, HIPAA and GDPR and the evolving US State data privacy mandates. This explains why our customers are so excited by our focus on user-centric data security, underpinned by AI and machine learning, because unless technology can be used to secure and intuitively help and support users as they share data every day, the breaches and subsequent fines will continue to grab the headlines.

*2017 Breach Level Index Report

Offering Next-Generation SIEM for Enterprise

An Interview With
Peter George
CEO
empow

THE SIEM has become a ubiquitous component in modern enterprise security architectures, but significant differences exist in how the function is supported. One of the primary comparison points for any team considering SIEM platforms involves the degree to which that platform can operationalize threat intelligence at scale. This is particularly important as the speed at which the global threat surface changes continues to accelerate.

The empow team specializes in high-value contextual understanding of ingested data through use of natural language processing (NLP) technology. This enables the empow solution to read, understand and operationalize not only machine-readable threat intelligence (*aka* feeds) but also threat intelligence reports that were written by humans, for humans (in natural language). We recently connected with Peter George, CEO of *empow*, to learn more about next-generation SIEM trends and how empow develops world class technology for enterprise protection.

EA: Has the SIEM finally reached the ubiquity of controls such as firewalls and authentication?
PG: I'll start by agreeing that SIEMs have truly become a required component of any modern enterprise architecture. So, in that sense – yes, the SIEM is now a ubiquitous control. That said, I would say that most existing SIEM deployments leave much to be desired, especially in the detection and response to advanced attacks. We rectify this in our next-generation SIEM through NLP technology to determine the purpose, intent, motivation and context around security indicators.

EA: How does the NLP technology work?
***PG*:** It's easy to describe, but not so easy to implement. What we do is scour vetted sources of threat intelligence upon ingest of relevant indicators. We use the NLP to "read" all available intelligence about the threat, understand its fundamental nature, and classify it based on its "intent" – just like an experienced threat researcher or security analyst would do but orders of

magnitude faster and more effective. We then use a proprietary form of cause-and-effect analytics to “connect the dots” and find the actual attacks that are buried under all the alert noise. Our team at empow views this as a vital component of the modern next-generation SIEM for enterprise.

EA: I’ve heard you reference Gartner’s SOAR model. How does it relate to your platform?
PG: Yes, the SOAR model stands for Security Orchestration, Automation and Response, and it’s an important part of what we do. What’s unique about our approach is that we create an abstract model of the detection and response capabilities available in a customer’s security infrastructure, and then we build adaptive defense models on top of the abstraction layer. This enables our system to automatically investigate and mitigate attacks in a way that is optimized for the customer’s infrastructure.

EA: Is orchestration one of the more difficult aspects of providing next-generation SIEM support?
PG: I would say that orchestration is one of the most challenging aspects of modern security operations. Making so many different platforms work together with automation is especially hard when the number of different solutions and technologies seems to grow each day. We are proud of our orchestration capability, and we believe that automation is essential to dealing with modern attacks.

EA: What are some trends you’re seeing in your customer base?
PG: The introduction of automation to security workflow changes the game for most of our customers by allowing them to deal with the rapidly increasing speed of automated attacks. But if this automation capability is not built into a next-generation SIEM that can detect attacks with high precision and accuracy, this introduction of automation becomes more difficult, if not impossible. We see a clear trend toward recognizing this fact.

Providing Security via Application Delivery Networking

An Interview With
Ram Krishnan
SVP and GM
F5 Security Business Unit

MODERN ENTERPRISE teams and service providers must consider both infrastructure and application threats in protecting their most valuable assets. Hackers developed exploits and create attack campaigns that traverse many different levels of the business ecosystem. This certainly makes cyber security more complex, because it demands discipline from the network to the application.

We recently connected with Ram Krishnan, head of the security business unit at *F5* to learn more about how the company's application services fit in the context of advanced cyber security, and what sort of new capabilities we should expect in this crucial space in the coming years. The discussion is especially relevant in the context of modern cyber threats which typically include components that touch on the various focus areas for F5's security offerings.

EA: What are some security trends you're observing that are impacting customers?
RK: I think one of the first things organizations are adjusting to is that the threat surface has significantly expanded. Some of this is due to the transition from traditional and virtual data centers to public cloud and hybrid environments. That progression alone adds many new dimensions to the security playing field. Similarly, we've seen industry-wide, that web applications have emerged as a top attack vector. Among the most essential assets today's organizations maintain are applications and the data they contain. So, it follows that if applications are now the modern gateways of business value, they have become attractive as targets for attackers. And this is something our threat researchers within F5 Labs have found as well, noting that web application attacks are the largest cause of reported security breaches, accounting for 30 percent. With the reach of our customers' applications expanding, the role we play as a security vendor correspondingly grows alongside. At F5, we're evolving our foundational application security solutions and branching further into application analytics, threat detection, and orchestration to ensure our customers have full visibility into the risks to their apps and can manage their security response accordingly.

EA: How does organizations' increasing use of cloud technologies impact application security?
RK: The most obvious one is complexity. Organizations today have hundreds or thousands of applications in distributed—or what we'd refer to as 'multi-cloud'—environments. This includes

public and private clouds, data centers, co-location facilities, etc. Besides just a wider distribution, you also have the necessity of automation and orchestration capabilities to make sure these elements can perform efficiently and consistently in concert. And beyond the cloud deployments themselves, you have all the things that cloud and on-demand access to IT resources enables. For example, the way organizations build and deploy applications has changed radically. Historically, you'd typically have 9–12-month cycles within a 'waterfall' model. In a relatively static legacy production environment, security aspects could be addressed within a more predictable context. By contrast, today's customer environments (and the way apps are introduced) have evolved considerably. Agile methodologies, DevOps, and continuous integration/continuous delivery models are becoming essential for modern workflows, operations, and scaling requirements. While there are real advantages there—such as giving revenue-generating applications a quicker path to market—you must be ready to leave behind the previous notions of a more static production environment, and to accept that you are now working to defend a collection of multi-faceted moving targets.

EA: How should customers be thinking about application security given these challenges?
RK: F5's approach to app-centered security centers on three principles: Visibility, Context, and Protection. A full proxy solution like F5 gives comprehensive visibility into the app health and performance, as well as app threats. From this visibility, you can derive context—that is, an understanding of all the characteristics of the application environment. This includes the app's normal/expected behavior, so you can recognize anomalies such as latency due to a DDoS attack. Once you have both visibility and context, you can better assess risk and make informed decisions about which protections to apply to safeguard your apps and data. These protections may involve blocking, redirecting, or quarantining traffic, or otherwise customizing how certain traffic (or types of traffic) is received and handled. At an even higher level, what you're really looking at is a better path to "risk-based security." This is where system technologies can help you combine, correlate, and interpret information and performance characteristics from different sources through heuristics and advanced pattern detection. The idea here is, if you can identify behaviors or conditions associated with attacks that your environment is exhibiting, you can start by looking in the most likely places for threats and build your security response from there.

EA: Can you give us some examples illustrating how F5 solutions are addressing security needs for customers today?
RK: Sure. If we consider the idea of risk-based security from the previous question as a unifying theme for our key solutions, a few examples come to mind. One is bringing the idea of risk-based authentication to customers – that is, based on where a user is logging in from, and associated conditions or behavior patterns, you can adapt to require different levels of authentication credentials to grant access. Our Advanced WAF and DDoS protection solutions are another example, where our focus is moving beyond signature-based attacks to analyzing behaviors and patterns—and then using that information to detect (and act on) potential attacks and exploits. And the last example I'll mention centers on the number of organizations moving to real-time payment solutions. For these to be effective, you need to be able to determine immediately if a given transaction is legitimate or fraudulent. This is another case

where the ability to comprehensively view application environments for any anomalies can help signal conditions where additional scrutiny is required—and this kind of granularity is a real differentiator for our web fraud protection solution.

EA: What are some future directions for F5 technologies?

RK: One key priority will continue to be around simplifying the way F5 services can be consumed by customers. Certainly, we're expanding our efforts around containers and micro-services to better match the ways that application developers are looking to apply services to applications in the dev and testing pipeline and throughout their lifecycle. At a high level, we want to make it easier for NetOps, DevOps, and SecOps not just to coexist, but to really benefit from a similar toolset. Another area—briefly touched on earlier—is a continued focus on combining and analyzing information from disparate sources to make better security and risk determinations. It might be the case where you'd see two seemingly normal events that themselves are relatively routine, but if you can quickly detect and correlate these two events, it'd be much more obvious that something's up and that you should investigate further or take corrective action. You can make an argument that's doable today, but it takes a lot of investment in infrastructure and analysis—and most organizations are challenged to tackle this kind of problem to an appreciable degree. They have the information, but not the time, expertise, or capacity to put it to the best use. It's this kind of thinking that will inform the direction of our next-gen security offerings, leveraging multi-cloud threat analytics. Our goal is to bake this expertise into the infrastructure and make it easy for customers to benefit from the immense amount of data being created from a security standpoint, without getting in the way of their primary objectives to keep the business and applications performing at full tilt.

Implementing a Fabric of Cyber Security Controls

An Interview With
Jonathan Nguyen-Duy
VP of Strategy
Fortinet

MANY ENTERPRISE teams implement a patchwork of individual point solutions in their security architecture. This has the advantage of allowing security architects to pick and choose products, but it often creates a complex mesh of systems that might include seams or leaks that can be exploited by an intruder. Supply chain teams also complain about such patchwork approaches involving many different vendors.

The Fortinet team offers an alternative, with a well-integrated fabric of platform solutions that are pre-integrated into a seamless solution for enterprise. This includes its signature next generation firewalls, but also much more We recently connected with Jonathan Nguyen-Duy, VP of Strategy at Fortinet to discuss trends in cyber security, and how the Fortinet solutions address this on-going evolution.

EA: What does Fortinet mean by the term 'security fabric'?
JN: The Fortinet Security Fabric is what we call our architectural approach for unifying security technologies deployed across a digital network. To elaborate further, the fabric is an integrated framework of devices that collect, share and correlate data giving users the ability to manage complexity of today's security frameworks. Our Fabric addresses common and advanced threats supports digital transformations and the achievement of business objectives all accomplished with delivery at a reasonable level of due care. The essential elements of our Fabric are automation, open interfaces and best-in-class threat intelligence. Our approach is also unique in its approach to acknowledging and leveraging legacy investment by supporting third-party integration.

EA: Any trends worth mentioning with respect to next generation firewall protection?
JN: The emergence of hybrid network environment brought about by the expansion of IT ecosystems paves the way for new ways of looking at the security protection provided by the next generation firewall. As new networks emerge and require connection to each other, that expansion is based on the nexus of three things – the control plane, the data plane, and the management plane. Sitting at this point will be the next generation firewall supporting network

interconnection with security, network management, WAN optimization, resilience and potential other functions. The next gen firewall will play a key role in supporting the transition of security from disruptive risk to normative risk.

EA: You've spent time in both government and industry; any trends in cyber security that you've observed across the two sectors?
JN: The options for addressing cyber security is probably one of the areas that I've observed to be changing over time. I think that one of the key questions organizations now find themselves asking is should security be run in-house. In the past, there was a need for 24/7 operation and deep control. Now, maintaining an operation of that type requires deep pockets and may be difficult to justify. Cybersecurity is now a team sport and organizations need to pick the right partners. No one team can handle all the disciplines required for maintaining an effective security posture. Cloud is forcing companies to take another look at their cyber security strategy. The movement of functions from traditional datacenters to cloud warrants a rethink of where activities including security should occur.

EA: What security features is Fortinet working on for its future platforms?
JN: The advent of hybrid networks is driving our approach to security evolution. There are several areas of focus for us as a security innovator. First, growing our Fabric capability is one area. With our recent addition of Bradford Networks for example, we are adding NAC functionality to our capability because the new network environment requires that there be ways to see every device attempting to access networks, understanding who or what functions are associated with those devices and maintaining an end to end view of what is happening in the network. Second, AI and machine learning are another area of focus since they offer ways to manage the complexity of today's environments. In this instance, context is important to understand as we search for and identify anomalous behavior and find ways to provide an effective response to it. Third, looking at security from an outcome based perspective is also something we're focused on as more of our customers seek to measure efficacy in terms of how we're able to support the business outcomes that they use to measure success. For us aligning security to ensure that critical workloads and applications function as designed to deliver intended results is an area that we will continue to dedicate time and resources to. Fourth, intent-based security is also an area of focus as we look for ways to translate business outcomes and personal outcomes to security controls that support more effective risk management strategies.

EA: What are some attack trends you're observing from your customers?
JN: Generally, outside of FinServ and Critical National Infrastructure, everyone continues to struggle with cyber security and the pace continues to increase. Speed is a major issue. One recent estimate from a reliable source suggests that targets of attacks can suffer damage to 30% of their networks in as few as 2 to 3 minutes from detonation. Another general observation is the accelerated development of several precursors of Swarmbots and Hivenets are especially worth revisiting. Others include the increased targeting of critical infrastructure, the development of automation in malware exploits, and the use of blockchain technology to anonymize the command and control of botnets.

Implementing Secure Remote Browsing in Hardware

An Interview with Henry Harrison *CTO Garrison*

THE CONCEPT of isolation is powerful in cyber security, because it involves separating bad activity from good resources. When browsers are visiting content rich websites, especially ones with embedded scripts and other executable, it becomes the obligation of the security team to find a way to isolate this potentially dangerous activity from the important files and other information found on the initiating endpoint.

Garrison is a UK-based company that has pioneered solutions for isolated browsing using a creative hardware solution. The hardware produces high assurance gaps between the content site activity on the browser and the rendering the user experiences on the local browser. We recently connected with Henry Harrison, CTO of Garrison to learn more about how secure remote browsing solutions work and how they are likely to evolve.

EA: What is meant by secure, isolated remote browsing?
HH: Pretty much since the web was born we've had web security - but as the threat environment evolves, we're now finding that the traditional approach of detecting and blocking bad sites is failing to keep up. Our customers are recognizing that some sites are too hard to call - they might be legitimate, but they might just be too risky to allow access from the desktop. In those cases, the user can visit the site using a secure, isolated remote browsing platform which will take all the risk - delivering only "guaranteed good" data to the user's endpoint.

EA: How does your platform solution work?
HH: We focused on the concept of "guaranteed good" - something that's easy to claim but much harder to justify. The way we do it is by delivering just the pixels of a browsing experience. What we found was that doing that cost-effectively meant building a completely new hardware platform - and when we set out to do that we ended up designing something that was not only cost-effective but also much, much more secure than any competing software product. At the heart of our Silicon Assured Video Isolation technology (Garrison SAVI) is the concept of using large volumes of the sort of low-cost silicon you typically find in cellphones,

and running these in pairs. One chip in the pair does the risky browsing - and delivers just the pixels that it renders to the second chip in the pair.

EA: Do you see only high-end users requiring such high assurance isolation?
HH: There's no doubt that we deliver a high assurance solution - indeed, our solution is being used by some very high-end, security-sensitive customers (who of course I can't talk about!) But what is perhaps surprising is that our platform is actually more cost-effective than competing lower assurance solutions - so it's not just those very high-end users that are finding us attractive. Those ordinary customers find that they get that extra level of assurance "for free" with Garrison! Of course, some competing solutions are just much lower security than Garrison - this is of course a market where there's always scope for unfounded claims of security. We're not keen to engage in a race to the bottom with those.

EA: Can you scale this hardware solution to a large deployment?
HH: As I say, it's perhaps counter-intuitive that large deployments can actually end up being more cost effective with Garrison than with other competing solutions that are "software only". I use those quotes advisedly - because software always has to have hardware to run on. And for software solutions that genuinely use a convert-to-raw-pixels approach, it turns out that they need really a very large amount of hardware to run on. Their hardware demands are driven by the need to compress the pixels so they don't flood the network - because of Garrison's unique hardware approach, our compression is delivered in low-cost dedicated silicon (like in your cellphone) which makes for much better price/performance at scale.

EA: What are some features you're working on for your next generation platform?
HH: Right now, we're providing our platform to customers as an on-site appliance, but our key focus is building out Garrison-as-a-Service - racking up our appliances ourselves and using them to supply an ultra-secure browsing experience as a cloud service. We're always going to have high-end customers who want their appliances on-site, but the market is telling us they'd like to consume secure browsing as a service and that's something we're committed to delivering.

How to Better Align SecOps and NetOps Teams

An Interview with Paul Hooper *CEO* *Gigamon*

OPTIMIZING SECURITY tools is a fundamental need in both security operations (SecOps) and network operations (NetOps). Balancing security without sacrificing performance is tough, because infrastructure has become faster, more distributed, often virtual, increasingly in the cloud, and encrypted. Threat actors are adept at leveraging network access for sophisticated attacks. To stop persistent threats, rich network metadata – the ultimate source of truth in your organization – must be visible with the right tools, at the right time, so they can do what they were designed to do: Secure the enterprise.

Gigamon is one of the innovators driving the alignment of cybersecurity and network teams by offering a suite of proven solutions that help both teams maintain clear, real-time views of the flow of data to the appropriate security tools, while ensuring the business can run at the speed they need to be competitive. We recently connected with Paul Hooper, CEO of Gigamon, to learn more about how the Gigamon solutions work today and are likely to evolve in the future.

EA: How does the Gigamon platform enable the convergence of network and security operations?
PH: That's a great question, because it captures what we strive to do: Leverage speed and agility to deliver full visibility to the single source of truth – the network data. We see the need for security and network operations to work together to ensure that businesses remain open, and to deal with a daily barrage of threats. Teams must work together within a common infrastructure. The GigaSECURE Security Delivery Platform provides next-generation network packet broker capabilities – a built-for-security solution that moves data to where it needs to go. We see just as much enthusiasm for the solution from security teams as from networking teams as our goal is to provide the highest level of data visibility, so that effective detection and remediation by the appropriate security tools can proceed as efficiently as possible.

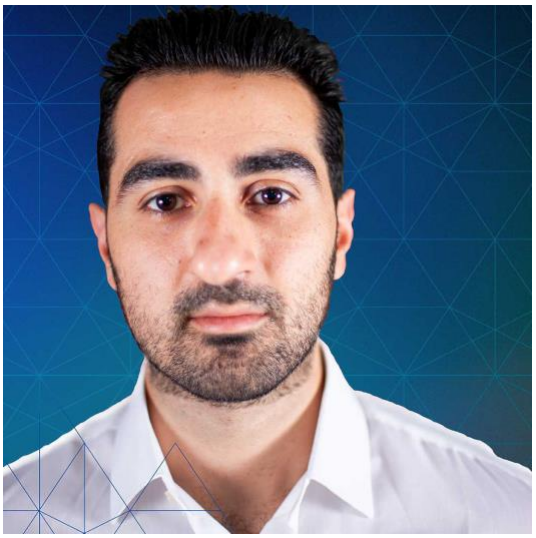
EA: You recently acquired a small security company called ICEBRG. How will the ICEBRG product complement existing Gigamon solutions?
PH: ICEBRG is a natural extension of our portfolio. In addition to managing data in motion, we can now store rich network metadata and run security applications on that data store – some of

which we will author and sell, and some that other security ecosystem partners will create. ICEBERG has built and sold a network traffic analytics solution that we now call Gigamon Insight, with Gigamon Detect and Gigamon Investigate being the initial Insight applications.

EA: What does Gigamon Insight bring to the table?
PH: While the traffic traversing your network enables your global business, it is also the conduit of entry and exfiltration for an attacker. What Insight delivers is the ability to generate powerful intelligence regarding attack vectors – across both individual networks and a global customer base – from network data which we have long believed to be the ultimate source of truth. This intelligence is then leveraged by powerful analytics to detect patterns that help identify the most dangerous attacks and quickly signal the need for containment and remediation.

EA: What is the effect of cloud and virtualization on cybersecurity visibility?
PH: As organizations move workloads into the cloud they need to have the same visibility to network traffic that they do for their on-premises environments, both for security and network monitoring needs. The same is true for virtual infrastructure. SecOps and NetOps leaders want to use the same tools across these varied environments, and Gigamon can ensure they can do just that.

EA: What are some trends you're observing in your work with network and security teams?
PH: A blog I recently published when we acquired ICEBRG addresses this question. Over the last few years I have been telling customers, partners, prospects, employees, essentially anyone who would listen, that a change in our approach to securing our most vital personal, commercial and federal data is needed. Numerous vendors in our industry regularly tout the abilities of the latest greatest mousetrap that will solve this challenge. But are the mice becoming entirely too smart to fall for the next mousetrap? Is it time to disrupt our thinking and take a completely different approach to managing the protection of information? While the mousetrap may still have its place, it's time to ditch the old approach and turn to a new line of thinking. What if you were easily able to analyze the patterns of movement of the mice across a global grid of homes? Patterns would emerge and the home entry methods with highest likelihood of success would appear. Having this knowledge in real-time could alert you to take preventative action before your infrastructure experiences the same outcome. Once the attack is underway, and within your environment, it's too late for traditional security solutions to protect you. As soon as one attacker has successfully penetrated the perimeter and traversed to your mission-critical data, their footprint may be difficult to detect, leaving you exposed to future attacks. Security is fundamental to everyone today. It's time to consider a new element to your security arsenal. As an industry, we need to turn the tables on the mice.



Advances in Decentralized Authentication

An Interview With
George Avetisov
CEO
HYPR

A MAJOR security vulnerability involves centralization of credentials and authentication information. The traditional approach of storing centralized passwords results in easy targets for attackers. Many prominent incidents have occurred in recent years from credentials being stored in one place. Furthermore, companies that are well protected and have *not* suffered a data breach are still susceptible to credential reuse attacks from passwords stolen during other breaches. It is human nature to reuse passwords, so enterprises that centralize those passwords remain at the mercy of the habits of their users and other breached companies. Security experts have thus come to recognize that improved techniques are needed.

HYPR has been a great innovator in developing decentralized authentication solutions for customer and employee facing applications. They've also taken full advantage of mainstream adoption of biometrics to accelerate the rise of a true password-less world. We recently asked George Avetisov, CEO of HYPR to help us understand this transition from centralized to decentralized credential and authentication security management.

EA: Why is centralized management of credentials a problem?
GA: We're always hearing about major data breaches that have leaked millions of user login and payment credentials. It's been a factor in beaches at Home Depot, LinkedIn, Yahoo!, Orbitz, Equifax, and the list goes on and on. If you take a close look at the large-scale data breaches you'll notice that they have one thing in common. It's not how the hackers got in, it's what they are going after – namely, the centralized credential store. It doesn't matter if you're storing passwords, biometrics, PINs, or bankcard numbers; when companies centralize user credentials, they create a single point of failure often targeted by hackers. Centralized passwords are the hackers' primary target, and have remained the top cause of mass breaches and credential reuse. And that's not even the worst part. Businesses that invest millions of dollars in securing their credential store, and thus avoid large-scale attacks, remain susceptible to credential reuse from other major breaches. Instead of trying to secure the target, what if we just remove the target? That's what decentralized authentication is all about. We are

witnessing a paradigm shift away from centralized passwords and shared secrets, towards a true password-less ecosystem.

EA: How would such decentralized management work in practice in an enterprise?
GA: Surprisingly, decentralized authentication enables a *higher* level of control over transaction logic, modalities, security policies, and preferences at administrator and user levels. Why is that? Reasons may vary among different vendors and implementations, but HYPR focuses on control, flexibility, and interoperability. The HYPR Control Center provides an intuitive visual interface for management of decentralized authentication. Enterprises can manage millions of users in real-time with a level of control that has never been possible with centralized passwords. The HYPR Control Center provides a deeper level of supervision and insight into the user's device. This includes MITM mitigation, root detection, and giving enterprises a direct way to manage keys stored on the trusted device layer. PKI-based authentication has been notoriously difficult to manage at scale. HYPR aims to simplify and enhance the administrative experience through commitment to interoperability. We believe that integrating decentralized authentication with existing identity providers should be a one-two-three step process, and should not force a customer into making any significant changes to their identity stack.

EA: How does the HYPR platform work?
GA: When designing HYPR, we focused on time-to-value. Some companies have taken years to deploy FIDO, password-less experiences, or omni-channel authentication to their users. From a practical standpoint, we believe that is unacceptable. We asked ourselves this: How can true password-less security be deployed in weeks instead of years? HYPR's goal is to enable true password-less security by eliminating the centralized credential store. This is achieved by replacing legacy authentication with a PKI-based scheme deployed via a software update. In doing so, we focus on interoperability, ease of deployment from the enterprise level, and ease of use at the user level. Consumer and employee-facing applications receive a software update that prompts users to enroll a public-private key pair. The private key is isolated, encrypted, and secured on their personal device. Once registration is complete, the centralized credential is no longer necessary and is removed. This is what enterprises mean when they aim to "remove the target."

EA: What are the pros and cons of using biometrics for authentication?
GA: There are many pros and cons that depend on how a business approaches biometrics. One advantage is that doing biometric authentication the right way can enable true password-less security. This is a path to reducing fraud rates, eliminating credential reuse, and preventing phishing attacks. A challenge, however, is that deploying biometrics alongside centralized passwords can become a problematic smokescreen for information security and fraud teams. A password-less experience may be easier to use, but companies are stunned to find out that credential reuse rates have not improved and that account fraud remains constant. This is due to the continued centralization of passwords. Many companies have taken steps towards password-less experiences by using biometrics such as Touch ID and facial recognition to enhance user login. While this is a step in the right direction, many of these companies still use centralized passwords alongside the biometric login, leaving users susceptible to credential

reuse, fraud, and phishing. Doing biometrics the right way means deploying decentralized authentication as part of your biometrics strategy. This is how companies have achieved true password-less security.

EA: What are some credential-related trends you're seeing in your customer base?
GA: Business leaders are turning credential security into business-driven initiatives rather than just isolated security projects. This is likely due to the massive impact that centralized password elimination has on all lines of business, their fraud rates, and revenue. They are seeing an opportunity to latch onto digital transformation projects and incorporate the true password-less security story as a component of the digital transformation initiative. On the security side, customers have done a great job building higher walls, but there's a recognition that they can't control for credential reuse, which happens due to mass breaches outside of their domain. This recognition of the collateral damage caused by centralized password breaches has accelerated the adoption and urgency of true password-less security.

Automating Security and Compliance for Multi-Cloud

An Interview With
John De Santis
CEO
HyTrust

WHEN ENTERPRISE teams commit to the use of virtualized infrastructure, they immediately realize benefits in operating cost, feature flexibility and time-to-market improvements for new capabilities. As one would expect, however, a balancing consideration amidst these amazing benefits involves the management and orchestration of security for virtual workloads across hybrid data center and cloud infrastructure.

HyTrust has been at the forefront in delivering advanced solutions that address the challenges teams face in ensuring the trustworthiness of workloads, especially in the context of VMWare infrastructure with a shift to multi-cloud infrastructure. We recently caught up with John De Santis, Chairman and CEO of HyTrust, to better understand how his team is developing security and compliance solutions to address the challenges that virtualization and multi-cloud adoption pose for the modern security team.

EA: What are the compliance challenges you see today for teams moving to virtualized infrastructure?
JDS*:* These days, being the compliance officer or the person trying to build secure and compliant infrastructure can be a tough job. Teams face several major challenges when they move to virtualized infrastructure. First is the unprecedented rate of technology change. Teams are under pressure to adopt DevOps practices, public cloud services, containers, server-less computing and more. Never in the history of the world have organizations had so many new innovations thrown at them so fast. Second, gone are the days when teams could rely on a single infrastructure provider for most of their deployment. Most of them face a multi-vendor, multi-cloud world in which their infrastructure has more and sometimes very diverse providers. Lastly, teams need visibility into their infrastructure and, with it, controls that they can deploy to help them automate the known good states (what I call automating ethics, or allowing policies to automate the right thing) in a very dynamic and rapidly changing environment. Despite these compliance challenges for virtualized, cloud and multi-cloud deployments, there are solutions that can help.

EA: Do you see the primary challenges being with cloud infrastructure or with data (or perhaps both)?

JDS: The challenge starts with the data for security, and sometimes cloud for the team building cloud infrastructure. And therein lies the problem many organizations are facing. Protecting the data must be Job No.1 for the entire organization, be it customer data and PII, intellectual property and the crown jewels, or operational financials for the corporation. The real challenge is evolving teams' understanding of cloud infrastructure so that they can meet both concerns for security (risk, compliance, data loss) and infrastructure (agility, efficiency, scale) as organizations migrate workloads or begin new cloud deployments of workloads. Automation can play a key role here. It's analogous to a driverless car, where automation enforces traffic rules and regulations without giving the driver a chance to make a mistake. In the same way, once you've figured out your security policy — which is whatever you decide a priori is the correct behavior — you automate it in a scalable way. This is how we at HyTrust meet the challenges of protecting the data and building cloud infrastructure. Our customers almost always have deep engagement with both the security and infrastructure teams as they pursue building secure infrastructure. In fact, our deployment often drives greater collaboration between these two teams.

EA: Tell us how your platform integrates with a planned or existing virtualized deployment.

JDS: Every organization has virtualized some portion of their infrastructure, even if they have not begun to deploy workloads in a public cloud. Most of this is deployed on VMware platforms that have enabled a software-defined data center (SDDC) with software-defined compute, storage and network. HyTrust integrates across a VMware SDDC deployment to add visibility and security controls for those deployments. That might be supporting separation of duties and access controls for VMware vSphere. It might be enabled key management for VMware vSAN deployments or enabling encryption for VMware Cloud on AWS (VMC on AWS). HyTrust was founded on the opportunity to amplify the trustworthiness of VMware platforms. Our initial focus was on virtualization and VMware. Since then, however, we have moved to support our customers' needs for multi-cloud security as they embrace public clouds for workload deployment and begin to shift those workloads from virtualized workloads, but also to containers deployed in public or private clouds. HyTrust is allowing our customers to develop policy-based security controls that span a multi-cloud deployment, across public and private clouds, but also across different infrastructure providers.

EA: Which compliance frameworks do you focus on in your work?

JDS: Compliance is clearly an important driver for many of our customers. Compliance regulations of some type affect almost every industry now in some way. The General Data Protection Regulation (GDPR) that took effect in May 2018 has caused even more companies to expand their efforts to meet compliance. Our company has developed specific capabilities in our products to help our customers achieve compliance faster and with less manual cycles. These investments have been made to help customers with compliance mandates including GDPR, PCI, NIST 800-53, CJIS, HIPAA, HITRUST, FedRAMP, NIST 800-181 and others. The visibility and controls that HyTrust can put in place across multi-cloud infrastructure constitute best practice, aligned with efforts such as the NIST Cybersecurity Framework. They can help to

ensure that infrastructure operates at the highest levels of trustworthiness, and produces the desired outcome of compliance mandates.

EA: Have you seen a major shift in attitude amongst compliance and security teams regarding the use of cloud for critical applications and systems?

JDS: Yes, but it didn't happen overnight. People and organizations often resist change. Perhaps some of these teams thought that cloud would be a passing fad or would be limited to rogue developers who wanted to experiment with it. But it's become clear that cloud adoption is real and is here to stay. More and more businesses are moving parts or large chunks of their infrastructure to the cloud, driven by the compelling business benefits and potential to achieve efficiencies at scale. At the same time, security and compliance must evolve and keep pace with DevOps initiatives and cloud adoption, and teams are beginning to embrace this. They know their companies' infrastructure is moving to a new world, and they are coming to expect the visibility and controls that enable them to maintain security and stay in compliance. There will always be laggards and late adopters, but at least the progressive thinkers are shifting their attitude.

Advanced Security Analytics for Networks

An Interview With
Dr. Michael Ehrlich
CTO
IronNet Cybersecurity

THE NEED to ensure security for enterprise networks is unquestioned, but the functional means for doing so is less obvious. Dr. Michael Ehrlich has been at the forefront of this challenge both in his previous capacity as part of the US Intelligence Community and in his current role at IronNet Cybersecurity. He understands the need for security solutions to keep up with the massive data volumes and speed increases in today's commercial networks and the need to incorporate analytics to efficiently process network anomalies at scale.

IronNet Cybersecurity is one of the great innovators in developing a comprehensive security analytics platform that allows enterprise customers to deal with the growing risk on their evolving networks. We recently connected with Dr. Ehrlich to learn more about how IronNet Cybersecurity is approaching this problem and how their commercial platform continues to evolve and grow.

EA: Dr. Ehrlich, give us a brief overview of how your platform works.
ME: IronNet's products offer high-fidelity detection and visibility to close gaps in an enterprise's security infrastructure. IronDefense is our flagship platform that analyzes network traffic at machine speed to deliver scalable network behavioral analytics, integrated packet-level cyber hunt, and the application of tradecraft expertise to detect advanced threats often missed by existing commercial cybersecurity solutions. Our IronDome solution leverages anomalies detected by IronDefense and anonymized triage information to common anomalies observed across the industry to link enterprise peers, third-party suppliers, and other stakeholders into a collective defense. Adversarial tactics used against any member of IronDome are anonymously shared at machine speed, improving threat detection, risk mitigation, threat visibility, and real-time situational awareness for all members.

EA: Do you see much difference between industries in the use of the platform?
ME: Our customers are critical infrastructure companies where a large-scale cyberattack can put lives as risk. These companies care deeply about cyber security and realize that the only way to consistently defend against a determined, deep pocketed adversary is to work together with peers and the public sector to collectively defend against the threat. In practice, the

collective defense combines technology with the business and operational side of things. For example, energy and utilities companies work together across a national grid and with government. IronDefense and IronDome are extensions into the cyber realm. This is in contrast with the financial sector, where IronDefense and IronDome help address competitive issues. On the operational side, customers have different preferences on how they consume IronNet services. Some prefer to do everything in house; others prefer a "co-drive" model, where IronNet cyber hunters work side-by-side with Security Operations Center (SOC) analysts; the rest prefer a Managed Detection & Response relationship, where IronNet hunters hunt for advanced threats independent of their SOC analysts.

EA: How do you ensure that your analytics can keep up with advances on the offensive side?
ME: Testing real world techniques and behaviors used by advanced threat actors is critical to measuring detection performance. IronNet employs a rigorous methodology to ensure high efficacy. This includes the creation of use case teams comprised of Threat Intelligence Researchers, Cybersecurity Subject Matter Experts (SME), Red Team Operators, Cyber Hunters, Data Scientists, and other experts to prioritize detection development on new malicious techniques or malware. Once prioritized, IronNet Cyber SMEs focus on analyzing the threat and creating real-world threat emulations. These are then applied nightly against IronDefense and IronDome in a cyber test range, and can used, for example, by the financial sector for their biennial Quantum Dawn exercise. A confusion matrix for statistical classifications is created to analyze false-positive rates as well as *true and false-negative rates*. The results are fed back to the use case teams for further enhancements to our detection capabilities.

EA: Do you see any new trends in nation-state cyber offensive activity?
ME: Cyber is becoming an element of national power, and many nation-states are continually adding cyber offensive capabilities to support their goals. While this has been the case for many years, what we have seen recently is a pivot from espionage, IP-theft, and spying to an increase in destructive, and potentially destructive, activity against computing systems and physical infrastructure.

EA: What advice do you have for enterprise security teams regarding emerging threats?
ME: Defenses must continue to evolve to meet the threat. Defending against nation-state threats requires a concerted effort at enterprise, industry, and national levels. This requires the ability to analyze enterprise traffic at network speed and enterprise scale using behavioral analysis techniques to identify and prioritize threats based on risk. No commercial company can defend against a deep pocketed nation state adversarial in perpetuity. However, if each enterprise can close visibility and detection gaps across their own networks and share anomalous information with trusted peers and the government at machines speed, then it is possible to improve individual enterprise response, while also enabling a collective response at the highest level against threats targeting the industry and the nation.

Advanced Protection for Mobile Calls and Texts

An Interview With
Elad Yoran
Executive Chairman
KoolSpan

THE PROTECTION of mobile communications is a traditional aspect of the information security industry. With the advance of mobile services, however, the primary focus to date has been on protecting data and apps, rather than addressing the growing risk of mobile calls and texts. With increasing focus on disclosure of sensitive email and other communications to places like WikiLeaks, the risk of voice and text discussions being recorded and leaked is now high.

KoolSpan has been in the business of protecting calls and texts through use of advanced encryption for several years. The company now offers an end-to-end solution for encryption of calls and texts that addresses many of the risks that executives and other individuals must mitigate in their use of mobile. We recently caught up with Elad Yoran, Executive Chairman of KoolSpan, to solicit his views on this aspect of modern cyber security.

EA: Should everyone be encrypting their mobile calls and texts?
EY: Yes, absolutely, especially business people and government employees. Until recently, however, it was impractical to do so because encrypted call quality was poor and solutions were inflexible. With KoolSpan, encrypted calls sound better than regular calls and the TrustCall platform is available with several, flexible deployment options. TrustCall can be integrated into customer IT systems, managed to enforce policy, and more. With a secure solution that works well, why would anyone opt to make an insecure call?

EA: Do you expect to see more sensitive business and government mobile communications leaked to the Internet?
EY: Unfortunately, we've largely ignored the systemic vulnerabilities of the telecommunications networks over which we speak, text, and share information. Everything we say and text traverses these networks in the clear and is readily intercepted and monitored from around the corner or, just as easily, from around the world. The game today is economic warfare and corporate espionage, where not only government employees, but also business people are prime targets. It is a safe to assume that the things we say and text, especially internationally, are monitored by governments, non-state actors, criminals, and business competitors. We are already seeing the impact. Texts and audio from calls are leaked to the Internet at an

accelerating rate. The problem is growing because the attacks are easy, cheap to implement, effective, and impossible to detect.

EA: How does the end-to-end encryption work in the KoolSpan TrustCall solution?
EY: KoolSpan TrustCall is a secure communications platform. Each part of the platform plays a role. End-users have an app on their phone to call and text others. The TrustCenter is a management console that organizations can use for provisioning, revocation, management, reporting and more. Together they form a solution that enables secure communications globally. Calls and texts are protected with strong, end-to-end (E2E) encryption regardless of what networks they transit. Furthermore, KoolSpan continuously deletes TrustCall metadata and does not aggregate, sell, share or otherwise disclose it.

EA: Does the voice disclosure risk increase when executives travel internationally?
EY: Phone and text interception are domestic and international problems. That said, travelers should understand that they have a bullseye on their backs. In a variety of ways, travelers are identified before they arrive in another country, and certainly as soon as they arrive, turning on their phones while still on the airplane. Our phones are subject to direct manipulation by the local phone companies, and our calls and texts are routinely monitored, not only by the local phone company, which is often controlled by the government, but also by others operating in environments, where the laws are different and the rule of law is not as well enforced.

EA: What trends are you seeing in mobile communication security across the industry?
EY: Over the last few years, significant time, effort and money have been spent on solutions, such as MDM/EMM, to manage and protect mobile devices. On the flip side, we have not focused on protecting ourselves against risks from systemic vulnerabilities in the networks over which we talk, text, and share information. Imagine if your phone was a bullet-proofed armored vehicle, but to talk with anyone in a different vehicle, you had to get out of the vehicle and walk over to the other car, thus exposing the communication. That is essentially how our mobile calls and texts are exposed at intermediate points between your phone and the other person's phone. We can protect devices, but we must also protect the communications in transit between the devices. Our communications transit across networks designed to be interoperable and backwards compatible. So, next time you go on a safari on vacation or travel internationally on business, you can expect that your phone will work when you arrive. The technology that makes this work is called Signaling System 7 (SS7). Even as SS7 will be slowly replaced by a newer technology, Diameter, it too puts "just working" ahead of security. In other words, it is the very design of our telecommunications networks that makes things insecure. The good news is that there is a straightforward and cost effective solution, protecting all communications with strong end-to-end (E2E) encryption, so they are protected even as they transit across networks that are open and interoperable globally.

EA: What considerations should businesses or government organizations have when thinking about mobile communications security?
EY: An easy way to think of it is in categories. One category is the user experience, beginning with how the calls sound, how easy the app is to use, etc. There are additional categories that

apply to businesses and government organizations such as manageability, reporting, policy enforcement, integration into other IT systems such as AD, ERP, CRM and other systems. Also, flexibility in deployment options is a critical consideration for businesses and government organizations. TrustCall is available as a cloud based service, a hybrid solution with dedicated TrustCenter, or with TrustCall for Government, a fully on-premise solution providing complete direct control.

EA: There are several free solutions out there, such as WhatsApp. Why not use one of these?
EY: WhatsApp and other solutions provide a degree of security and are an option for some consumers. However, while seeming "free," they come with other costs that may be more expensive in the long run. In the case of WhatsApp, Facebook sucks up all the data about how people use it, when they use it, where, with whom, for how long and much more. All this information is aggregated with other data and is used to paint shockingly detailed and invasive profiles on each of us. The same thing is true with other free apps. We pay the price with the loss of our privacy and control over our data. Remember, if you are not paying for a product, then you are the product. Of course, businesses and government organizations have additional considerations, discussed above.

Making Anti-Malware Solutions More Effective

An Interview With *Eddy Bobritsky* *CEO, Minerva Labs*

ANTI-VIRUS SOLUTIONS have always suffered from the challenge that attackers can evade detections, even when the AV approach incorporates advanced methods beyond signatures. As a result, most users of anti-virus express disappointment with the efficacy of the control. *Minerva Labs* is a start-up cyber security firm that has developed a novel means for dealing with this problem, and their approach focuses directly on this issue of malware evading the known protections.

What Minerva does specifically is introduce an anti-evasion control for malware protection on the endpoint. With the Minerva technology, anti-malware solutions are thus made better, because evasion is no longer a strategic offensive option. We recently connected with Eddy Bobritsky, CEO of Minerva to ask him about this unique approach to anti-malware and how his solution is changing the game in endpoint security.

EA: What is meant by evasion in the context of anti-malware?
EB: As anti-virus solutions evolve, the adversaries aren't standing still or "retiring" simply because AV approaches now incorporate artificial intelligence and other advanced methods. These very advancements are causing attackers to implement measures for evading detection by anti-virus and other anti-malware controls. Defenders improve in response to the attackers, which causes the attackers to improve, and so on. Such cat-and-mouse dynamics are inherent to the cybersecurity industry. Minerva Labs' mission is to disrupt this cycle by turning the very strength of the adversaries—their incentive and ability to evade—into an advantage for the defenders.

EA: How does the Minerva technology work?
EB: Minerva's Anti-Evasion Platform interferes with attempts to evade other security measures. We do this by using elements of deception on the endpoint in a way that causes malware to self-convict, instead of attempting to distinguish between legitimate and malicious programs. For example, malicious software is often designed to terminate its execution or go to sleep if it's being analyzed. This extends the time during which the threat can remain undetected. One of Minerva's approaches involves lying to malware in a way that causes it to believe it's always

being analyzed. By simulating the environment that such malware considers hostile, we cause the malicious program to choose not to run. This is just one illustration of how our way of protecting endpoints is effective against never-before-seen threats, defending enterprises even against malware that AV cannot detect.

EA: Does the Minerva solution complement or replace existing anti-virus products?
***EB*:** Our Anti-Evasion Platform does not replace AV, it augments the AV to cover the gap that any AV leaves on the endpoint, even those products that incorporate advanced techniques such as machine learning. To accomplish this, our solution resides on the endpoint together with anti-virus software. This approach allows us to focus on the problem we're uniquely qualified to solve—causing evasion techniques to stop working—while allowing anti-virus vendors to stop threats that are not as evasive. Many customers used Minerva's Anti-Evasion Platform to augment their existing AV products, forgoing the expense and risk of replacing these products with others.

EA: How advanced has malware become in recent years?
EB: Adversaries increasingly incorporate some form of evasion throughout the attack process. For example, in the 99% of exploit kit attacks that Minerva examined, at least one evasion tactic appeared somewhere along the path. Given the reactive nature of detection-based approaches to protecting endpoints, attackers continue to succeed at compromising enterprise defenses. Unfortunately, evasion techniques and tools are now available even to novice adversaries and are often incorporated into even commodity threats. The more evasive the malware, the greater the chances that AV software will fail at stopping it. It's the opposite with our solution: The more evasive the threat, the greater the likelihood that it will be subject to our interference.

EA: What are some new features you're working on for your platform?
EB: Just to name a few: We've seen an increasing demand for our Anti-Evasion Platform from not only end-user enterprises, but also from Managed Service Provider. In response, we're releasing functionality that makes its especially convenient for our MSP partner to deploy and oversee our solution. In addition, we're continuing to enhance our unique value proposition for incident responders who seek to contain malware outbreaks with incredible granularity. This includes the ability to "vaccinate" endpoints against malware families that avoid infecting the same system more than once—a capability we're continuing to expand based on feedback from the field. Also, we're expanding our Critical Asset Protection features that involve principles of deception to protect special-purpose devices such as ATMs and Industrial Control Systems.

Embedded Cyber Solutions for Emerging IoT

An Interview With
Bill Diotte
CEO
Mocana

JUST AS PC and mobile endpoints supporting businesses and consumers require a range of cyber security solutions, so do emerging Internet of Things (IoT) endpoints. The threats to IoT are slightly different than for PCs and mobiles; for example, devices are memory and power constrained and cannot support standard PC endpoint security software. But the overall protection need is comparable, and the emergence of commercial solutions for IoT and operational technology (OT) security is welcome.

Mocana is one of the pioneering technology companies supporting the development and support of a comprehensive suite of solutions for IoT security. We recently connected with Bill Diotte, CEO of Mocana to ask him about this important trend toward improved protections, reduced risk, and embedded security solutions for the plethora of IoT devices, systems, and infrastructure emerging across the world today.

EA: Is IoT endpoint security following a comparable process as PC endpoint security?
BD: IoT endpoint security is following a different process than PC endpoint security. IT systems rely on endpoint security and virus protection software complemented by layered network defenses. These approaches are not as effective in protecting IoT devices because the embedded devices may not sit within a firewall and cannot support a heavy weight software implementation. Rather, IoT devices themselves must rely on strong authentication, encryption and cryptographic controls to ensure the devices are trustworthy and tamper-resistant.

EA: What is unique about security for IoT devices and systems?
BD: One thing that is unique about IoT devices is that they are typically deployed in environments that are not easy to secure. In IT, the key servers may be located in a data center or within a physically protected room or cabinet. In IoT, the devices are deployed in areas that have poor physical security, making the devices easy to physically compromise. For example, wireless access points, home set top boxes, home surveillance systems can all be physically attacked easily. If the embedded systems aren't tamper-resistant, a sophisticated hacker could compromise the device and steal data or take control.

EA: How does the Mocana platform work?
BD: Mocana provides a system of cyber security that is comprised of Mocana TrustPoint™, an IoT endpoint security software, and Mocana TrustCenter™, a services platform to manage the IoT device security lifecycle. The Mocana TrustPoint and TrustCenter work together to ensure supply chain integrity and simplify and secure IoT security management. They were designed to provide complementary support for teams concerned with growing IoT security risk.

EA: Are threats to IoT different than other aspects of computing?
BD: Yes, IoT cyber threats are different than threats to enterprise and computing systems. Typically, hackers targeting enterprise systems are trying to steal private data, such as passwords, emails, intellectual property or credit card data. In the IoT world, however, the most capable hackers want to take control of systems that compromise safety, production uptime or the environment. The consequences of successfully hacking into an IoT device may cause more physical harm than an average computer system. As a result, the risk to these systems is enormous, and begs the need for advanced cyber security protections.

EA: What are some trends you're seeing in your customer base?
BD: Our customers are being driven by the business advantages that IoT provides, such as improved performance visibility, lower maintenance, and reduced support costs. At the same time, they are concerned about the rise in cyber attacks. Finally, they are concerned about compliance with industry cybersecurity standards such as IEC 62443, NIST US 800-53 and NERC CIP 003.

Supporting High-Availability for Systems and Apps

An Interview With
Darren Ansee
CTO for Security
NETSCOUT

WHEN CYBER security experts describe worst-case scenarios for the most consequential attacks on critical infrastructure, they always include denial of service events in the mix. Whether for direct impact or diversion, the use of volume-based attacks on the availability of on-line services has become a staple in the modern cyber offensive actor's playbook. Sadly, this remains successful too often.

Arguably, the most experienced team dealing with this threat has been *Arbor Systems*, which was acquired in 2015 by *NETSCOUT*. We recently sat down with the head of NETSCOUT's CTO for Security, Darren Anstee, to learn more about how distributed denial of service (DDOS) attacks are evolving, and how the modern enterprise can take positive steps to avoid this serious cyber risk.

EA: How would you characterize the present state of distributed denial of service risk?
DA: Unfortunately, the risk for business has never been higher, partly due to changes in the DDoS threat, but also due to increased dependence on the connected world for pretty much every business activity. Over the past couple of years, the weaponization of botnets, some based around IoT devices, has reached the point where complex, multi-vector DDoS attacks can be ordered with a single click. This is demonstrated by the 20% increase in the proportion of enterprises who reported multi-vector attacks in our 2017 World-Wide Infrastructure Security Report (WISR), and the 30% increase in those reporting application layer attacks. We also saw a broadening of the services being targeted by more sophisticated attacks, with VoIP and email seeing increased attention from attackers, alongside the usual DNS, HTTP and HTTPS targets. Looking at the simpler, volumetric attacks we have seen the numbers of attacks decrease slightly in the first half of 2018 - to around 2.8 million globally, based on data from our ATLAS intelligence. However, there has been a spike in terms of peak attack sizes with the terabit barrier broken twice in successive weeks in Feb '18, with 1.3 and 1.7Tbps attacks utilizing Memcached to reflect and amplify attack traffic. Last year we saw attackers metering their attacks to levels where they were effective, but did not overly attract attention from ISPs and law enforcement. This behavior is likely due to the monetization of the botnets being used to generate attacks today; re-using infrastructure, on the part of the attacker, improves the

economics of their service. This has continued this year, but we have also seen more larger attacks driven by use of Memcached, as mentioned above. DDoS continues to escalate as a threat, for businesses of all shapes and sizes.

EA: Are the volumes of attack continuing to grow?
DA: This is a difficult question to answer as there is always some regional variation in what is happening. Globally, we have seen the numbers of volumetric attacks we are monitoring decrease slightly in the first part of 2018. However, ATLAS still monitored 2.8 million attacks - so we are talking about very big numbers. Looking at the upper end of the scale we monitored a big increase in the number of attacks over 300Gbps, up from 7 in the first half of 2018 to 47 in the first half of 2018 – driven by Memcached. So, mixed news looking at the global picture for volumetric attacks. Looking at the more sophisticated attacks, we are seeing a continuation of what we saw last year with weaponized botnets being used to deliver multi-vector and application layer attacks. DDoS is continuing to evolve, with a broad range of organizations being targeted.

EA: Tell us how your platform works and how it deals with attacks across the protocol stack from layers 3 through 7.
DA: NETSCOUT, through its Arbor DDoS business, was the first to advocate hybrid DDoS defense, now the established best practice across the industry. Different kinds DDoS attacks can impact different aspects of our infrastructure: volumetric attacks cause network congestions; state-exhaustion attacks target the state tables in our firewalls and load-balancer; and, application layer attacks target our applications directly at layer-7. Businesses need comprehensive defenses from all these cases. NETSCOUT, and many of our service provider customers, offer the hybrid / layered approach. This approach uses combination of a cloud or service provider based DDoS protection service, that can deal with high-volume attacks e.g. Arbor Cloud currently has 9Tbps of capacity, allowing it to deal with even the largest attacks. And, there is a customer perimeter component that is always-on, closely monitoring traffic near to the enterprise or data-center edge, so that it can proactively protect against any form of detected DDoS attack. This is NETSCOUT's Arbor Edge Defense platform, which can be deployed as a physical appliance or virtual network function, and which incorporates counter-measures to deal with volumetric, state-exhaustion and application layer attacks. Arbor Edge Defense also integrates with the cloud / service-provider DDoS protection layer, using Cloud Signaling, so that information can be exchanged to ensure attacks are dealt with seamlessly. Arbor Edge Defense also offers additional value through its ability to apply high-scale reputation intelligence to traffic in / out (Threat Intelligence Gateway type functionality), and it can integrate with other elements of the security stack as a perimeter enforcement point.

EA: Are smaller companies beginning to see DDOS attacks and if so, what can they do about this problem?
DA: Yes, one of the big changes we have seen over the past 5 years is the broadening in the spread of the organizations being targeted, in terms of both type and scale. Historically, people tended to associate DDoS risk with the larger organizations within the gaming, gambling, finance and government sectors – now pretty much anyone can be hit, with campaigns

targeting everything from Internet start-ups to educational establishments over the last year. The good news is that many more organizations are aware of their dependence on the connected world, and the threat that DDoS poses, and there are multiple options available. Hybrid defense, as mentioned above, is the best-practice and is the most effective way for businesses to ensure they are protected. For organizations who want their own control and visibility, they can deploy their own perimeter DDoS protection solution – such as Arbor Edge Defense - and pair that with a cloud or service-provider based DDoS protection service. For organizations that want a fully managed solution there are options available from NETSCOUT, with our Arbor Cloud service, and from ISPs and MSPs around the world. Fully managed, hybrid DDoS services are becoming more readily available as the perimeter component is increasingly being delivered as a virtual network function (VNF).

EA: Are you seeing any clear trends in the management of DDOS risk in the industry?
DA: There are a few things that have changed. First, there is a better understanding across business that DDoS attacks are not 'just' about large floods of traffic that cause network congestion. There is a broader understanding of the more sophisticated state-exhaustion, application and multi-vector attacks that are out there today – and this is making people re-consider their defensive posture. Hybrid DDoS protection is now being adopted by a broader range of organizations, as shown by a couple of recent analyst reports. Second, we are seeing DDoS being incorporated into business and IT risk planning activities in many more businesses. Our 2017 Worldwide Infrastructure Security Report indicated that 77% or enterprise organizations now factor DDoS into their processes, up from 70% the year before. Businesses are increasingly aware of their dependence on the Internet for business continuity, and they know they need appropriate defenses. Third, we are seeing DDoS defense being brought more into traditional security operations. Historically DDoS has been viewed as network issue, handled by network operations, but the use of DDoS to mask bad actor infiltration / exfiltration, for other types of cyber-attack, has seen this change. There is also a growing interest in leveraging the capabilities in perimeter DDoS defenses to block a broader range of threats – as security teams look to consolidate around a smaller number of platforms and reduce the complexity of integrating their security stack. Last, but not least, we are also seeing a change in the service provider space. Increasingly we are seeing mobile operators become concerned around the potential impact infected user-endpoints or IoT devices could have on their services. This is driving them to look for new solutions that can be used to both provide service protection, and to drive new revenue generating services.

Active Defensive Solutions for Enterprise

An Interview With
Justin Zeefe
CEO
NISOS Group

THE CYBER security experience one can gain working in the deepest recesses of the federal government in intelligence and defense are unparalleled. Consider that the most intense nation-state actors can only be truly observed and learned through the intense active defensive strategies employed by the best cyber warriors. And the United States is certainly best-in-class in that regard.

The *NISOS Group* was born of that experience base, with a team of experts trained in the most intense cyber security trenches. The group offers customized solutions, assessments, testing, and consultation – and has been a delight to learn more about. We recently connected with Justin Zeefe, CEO of the NISOS Group to ask him about trends in active defense, and predictions about where cyber security is now headed.

EA: You and your team members have unique backgrounds. Can you share a little bit about your own legacy?
JZ: When it comes to our legacy, it all comes back to the Mission: that's where everything started and it's what led us to form Nisos. We saw talented people accomplish amazing things through the common goal of defending our nation's interests and assets. Our hope is that we can apply that passion and with it help our clients find success in defending against the evolving threat landscape. At the core of this is our culture; we wanted to create a place where talented people would want to work, where they become better because of the people they worked with, and they could get that same sense of accomplishment, and have a measurable and meaningful impact on the world around them.

EA: What is meant by the term 'active defense' in the context of cyber?
JZ: Enterprise security leaders have realized over the years that traditional security controls and technologies are insufficient, especially when you're talking about advanced or nation-state level threats. Security vendors are getting better and better, innovating new ways to detect and prevent attacks – but there hasn't been a meaningful reduction in cyber events or the impact of breaches. Active defense is an emerging term that refers to using all the tools and techniques legally available to the commercial sector to defend against and respond to threats and attacks.

For Nisos, all our services fall under the rubric of 'Active Defense'. When we conduct a red team, we do not employ a fixed methodology and toolkit. We leverage the deep experience and creativity of an elite team of network operators to fully stress test an environment, because that is what nation state actors do. We also pursue attribution leveraging proprietary investigative tools and datasets. The enterprise is tired of fighting bold and sophisticated adversaries with both hands tied behind their backs – employing and Active Defense posture gives some of that advantage back to the defenders. To be clear, when we say, 'Active Defense", in no way do we mean, or advocate, 'hacking back'. We believe there are meaningful and lawful measures still available, and we employ those measures to accomplish a hardened defensive posture and an aggressive response capability without the need to violate the law.

EA: Do you see nation-state actors getting better and in what ways?
JZ: In terms of techniques and tools available, nation state actors will always be a cut above rest, simply given the time and resources available to their operators. The most significant "change" we've observed in the past few years, as it pertains to the private sector, is the willingness of nation states to take these advanced technical capabilities and apply them in new ways. Everyone knows China targets Western companies to steal IP and nations conduct operations against each other to steal defense plans and government secrets. But in the past few years, we've seen North Korea brazenly using cyber operations to steal money from foreign banks, we've seen Middle Eastern actors deploy wiper malware who's only purpose is to disrupt and destroy and of course we've seen Russia employ cyber influence campaigns on a massive scale to destabilize western governments. These are troubling developments and they are evolving very rapidly – there are no fixed rules of engagement in cyber space. From our perspective, no one is safe.

EA: Are threats to government different than commercial entities?
JZ: The targets and objectives may be different, but the tools and techniques are the same. Government agencies don't have secret cyber defense mechanisms that can magically thwart attackers. They rely on the same technologies and defensive policies and procedures as those in the private sector. For sensitive government agencies, their security programs are at a very high maturity but they do not employ anything defensively that the private cannot also do themselves. It's a matter of will, and understanding the risk. We have been impressed at the security programs of many financial institutions in which we are engaged. Some industries really are starting to get it. The defenders inside government also approach their objectives with a mission focus. This impact cannot be overstated – to protect your country's secrets and crown jewels is an incredibly motivating mission. This used to be tough to replicate in the private sector, which offers a lot more in terms of monetary compensation, but a lot less in terms of impactful work. We don't accept this and have proven that this doesn't have to be the case. The threats the private sector is facing can be as critical for our nation's best interest as anything we saw while inside government. For example, the commercialization of space presents an incredibly alluring target for nation state espionage. I would argue that defending SpaceX and defending NASA are on the same level of positive and critical impact to our nation's interests. Moreover, a vast segment of US critical infrastructure lies under private sector

ownership, management, or control, and there should be a mandate for higher levels of protection and response in protection of these assets.

EA: What are some threat trends you're seeing in your consultation work?
JZ: The prevailing wisdom in security leadership of mature programs had always been "a breach is not a matter of if but when". To that point, we have not had a single attack simulation engagement that did not result in us achieving domain level access. Sure, some environments are better defended than others, but with enough time, resources and creativity, everyone can be breached. The shift now seems to be towards no longer fully accepting this inevitability or at least more towards an attitude "at least we'll go down swinging". The private sector is fighting back. You see Microsoft pursuing criminal threat groups and coordinating botnet takedowns with law enforcement. You see Google spending millions to hire the world's best hackers and ensure those skills are directed at helping to secure ubiquitous software. Our clients have shown an enormous willingness to push the envelope – they are no longer sitting ducks, and we view this as extremely positive for our industry and for our country. Relating to threat hunting and mitigation, a sophisticated and strategic approach is necessary, given the fact that threat actors have also been known to respond destructively to perceived deterrence.

EA: What are some of the roadblocks that companies face when trying to deal with problems like the insider threat?
JZ: The insider threat is not a mature domain – there are absolutely organizations that have grown mature and capable programs and likewise there are some very experienced professionals out there, but most organizations do not have a dedicated insider threat practice, nor the right talent to build one. Many of our clients are left scrambling when an incident occurs and are left trying to make technology decisions while still in crisis phase. This is obviously not a recommended way to handle this critical threat. We understand the gravity of the threat and are familiar with the tools that give the advantage back to the defenders – in fact, we've developed our own proprietary technology with a strong insider threat use case. We also have on our Advisory Board Dawn Cappelli, the CISO of Rockwell Automation – she literally wrote the book on the Insider Threat that most domain professionals reference. We advise our clients to take proactive measures, deploy the monitoring and protection technologies now, develop a playbook, so that when an incident does occur, your response will be fast, authoritative and impactful.

EA: I was wondering about attribution. Is this always necessary or helpful?
JZ: There is a lot of debate about this question. In our minds, it shouldn't even be a debate. It was Sun Tzu that said "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Yes, it is extremely important to know by whom you are being targeted and attacked because that informs your defensive strategy. It allows you to go to company decision makers and board members and give an accurate representation of risk and active threats without relying on the tired image of the random, hooded, faceless hacker. That said, attribution is difficult and tricky. It seems to be such a trend in the security industry these days to attribute threat groups and campaigns. When we analyze this research, unfortunately most of it falls

short. We find a lot of conclusions being drawn seemingly with the goal of reaching a dramatic conclusion rather than sound analysis. A good attribution investigation takes skill, determination and the experience of knowing what to look for. What mistakes did the attacker make? Are there any indications that those mistakes were made purposely to lead to an incorrect attribution? At Nisos, we were the advanced attackers, so we know how such players would hide their tracks and leave clues to confuse the investigations. People who don't have a lot of experience in formal intelligence analysis can reach and publish hard conclusions based upon insufficient or partial evidence. At Nisos, our assessments are always provided with context and confidence statements.

EA: Why is the commercial sector so attractive to nation-state actors?
JZ: Nation state actors are always seeking to accomplish some objective. The primary objectives used to be espionage and intellectual property theft. Those objectives have broadened in recent years, which should worry the entire private sector. Nation states are brazenly using cyber capabilities against private sector entities for a whole range of objectives – it doesn't take a whole lot of creativity to conceive of why any company would be the next target. It also doesn't help that the private sector has over the past several decades obtained more and more of a hand in the ownership and support of US critical infrastructure.

EA: What do board members need to understand about cyber-risk which is being inadequately-messaged to them?
JZ: Board members and company decision makers have a lot of issues top of mind, of which security is only one. Unfortunately, to this point, these conversations have been uphill battles because most of the C-Suite/Board continues to view security as a cost center. This is starting to change, and eventually, we believe security will take the path of IT and become viewed as a 'business enabler' instead. Framing the messaging in this context is important. Recent high impact breaches are also important events to communicate. The NotPetya cleanup cost Maersk hundreds of millions of dollars. The Equifax breached caused the removal of the CEO of an F1000. Additionally, the Shamoon attack against Saudi Aramco cost them an estimated $1B due to the massive disruption it caused across their corporate network. These are demonstrable and serious ramifications of breaches and no responsible board member or executive can dismiss the risk.

Insider Threats: People, Process, and Technology

An Interview With
Mike McKee
CEO
ObserveIT

FEW WOULD argue that the insider threat has emerged as perhaps the most insidious of threats to the modern enterprise. What few recognize, however, is that often this insider threat involves innocent insiders inadvertently breaking security policies, or compromised systems causing havoc across the network. So, it is in the interest of every employee – and this includes every user – to seek behavioral protections.

ObserveIT has been developing world-class cyber security solutions to detect and prevent insider threats for many years. Their solution offering is designed to reduce enterprise risk of compromise, with no privacy implications for employees or third party contractors. We recently sat down with Mike McKee, CEO of ObserveIT to learn more about trends in this area of cyber security and how his company is focused on reducing this risk.

EA: Is the insider threat the number one challenge today for enterprise security teams?
MM: When we talk with customers, we do in fact hear that insider threats are their number one challenge. And this is probably no surprise to anyone reading this interview. When insiders – employees and trusted vendors - are trusted with access to the organization's most sensitive information, then they can cause considerable consequence if they abuse this trust. The challenge is to ensure that trustworthy employees and partners see no impact to their great work, and that everyone benefits from the enhanced protections.

EA: What are the benefits of ObserveIT's user-based focus?
***MM*:** Observing the actual behavior of users is essential to providing the highest levels of assurance that data is not being compromised. Having visibility into a user's actions before, during, and after a possible incident provides context and insight into intent. You can certainly review logs and try to piece together activity using forensic tools, but visibility into behavior provides the highest fidelity understanding of potential mischief or exploitation of innocent users and employees.

EA: How does the ObserveIT platform work?
MM: We utilize software agents at the user level that capture data about insider activity by recording user actions such as screen, mouse, and keyboard activity as well as local and remote activity. Anomalous and risky behavior is immediately detected as alerts are triggered based on ObserveIT's Insider Threat Library which, out-of-the-box, includes more than 300 indicators of insider threat. The security team can quickly investigate alerts via easily searchable metadata as well as video-like recordings. With flexible prevention capabilities, risk can be reduced through real-time user notifications all the way to hard blocking. For security-minded organizations, all user data can be anonymized.

EA: Do you worry about observational tools pushing employees to shadow IT?
MM: With most insider threats being accidental in nature, when employees are treated with respect and they understand the benefits of having insider threat protection in place to protect the corporation and them from being an accidental insider threat, the threat of shadow IT goes away. We understand that a subtle balance is required in the enterprise. But the need to protect against insider threats is real – and our customers report excellent experience with our tools.

EA: What are some insider threat-related trends you're seeing in your customer base?
MM: As organizations increasingly shift their focus from external to internal threats, they are taking a holistic approach that includes people, process and then technology. While it may sound counterintuitive coming from a tech vendor, we strongly recommend our customers focus on the people and process aspects of insider threat first (for example, identifying the user personas and organizational risks, building an insider threat team, building a business plan and process as well as an insider threat playbook). By thinking people and process first, they have a solid foundation upon which to implement insider threat technology to effectively detect risky or anomalous behavior, streamline the investigation process and prevent insider threats.

End-to-End Cyber Solutions for Enterprise

An Interview With
Dan Burns
CEO
Optiv

HISTORICALLY, ENTERPRISES have taken an outside-in approach to cyber security, buying point-solutions based on outside influences – the latest trends, vulnerabilities, compliance mandates, or public attacks – rather than investing in the right people, processes, and technologies to balance security and business needs. This approach has allowed the threat and regulatory landscape, rather than enterprise objectives, to dictate security infrastructure and operations. This has saddled enterprises with expensive and complex infrastructures that are non-integrated, and difficult to manage, measure, and maintain. This, in turn, has created an operations environment in which staff is consumed by an ever-increasing number of fire drills.

We see symptoms of this approach everywhere. An industry shortage in skilled staff, escalating costs and investments in misconfigured tools. *Optiv Security* enables clients to reduce risk by taking a strategic approach to security. Instead of letting external factors dictate security spend and strategy, Optiv begins with each client's risk profile and objectives, and then builds a unique program with strategy, rationalization, optimization, and measurement. This enables clients to build a sustainable risk-centric foundation for proactive and measurable security programs. We recently asked Optiv CEO Dan Burns to share his views and insights into the evolution of the cyber security landscape.

EA: **What are the biggest challenges the industry is facing today?**
DB: It may sound trite but it's true – complexity is the biggest challenge the industry faces today. The threat landscape is populated by skilled and well financed adversaries, whether they are nation states, criminal organizations or hacktivists. Meanwhile, most organizations have very complex security technology infrastructures that they're trying to run against the headwinds of a cyber security skills shortage, so there are not enough skilled professionals to effectively manage all the security tools in the typical enterprise. When you consider these issues together, it becomes easy to see why we are seeing so many breaches around the world.

EA: How did the security industry get to this state?
DB: Since the emergence of the internet, many public and private entities across the globe have taken a reactive approach to cyber security, buying technologies in reaction to the latest trends

and vulnerabilities rather than investing in the right people, processes and technologies to balance security and business needs. Over time, this approach to security left many enterprises with an overwhelming array of disparate security tools in their infrastructure, and to this day the threat landscape continues to dictate security strategy and spend. This issue also inflames the cyber security skills shortage –there simply are not enough skilled professionals in the world to manage all this non-aligned, and non-integrated infrastructure. If you're a CISO, this is a very difficult environment in which to function – you have too many tools and not enough people who know how to run them, so you're never sure if your security technology is properly configured, maintained and managed. You can in almost guarantee that it is not. Meanwhile, adversaries are taking full advantage of the security gaps this infrastructure and operations crisis creates, which is why we are seeing so many breaches.

EA: What does it mean for Optiv to be a security solutions integrator, and how does this play into the company's ability to turn the tide on cyber security for clients?

DB: It means that we have the security-specific expertise, along with the breadth and depth of capabilities, to help our clients set the right security strategy, rationalize their infrastructures and optimize operations, so they can build more manageable, measurable and effective security programs. We create customized engagements that can address virtually any security challenge for our clients. We at Optiv are uniquely able to plan a cyber security program, build the program and all its components and run the program. The big consulting companies, for example, may provide high level strategy, but they're not going to be able to help when it comes to run security operations. Likewise, managed services organizations may be able to provide an outsourcing option for operations, but they're not going to have the expertise to develop corporate risk profiles and set security strategy. We are a single source for *everything*, which we believe is the definition of a Security Solutions Integrator. From a practical standpoint, Optiv can support clients in a true end-to-end fashion, whether it's conducting initial security assessments and building corporate risk profiles, setting security strategy, managing the technology evaluation, procurement and deployment process, providing ongoing security intelligence, or running security operations through our managed services organization. All of this is governed by our approach to security, which is the opposite of the outside-in approach. Not surprisingly, we call it the inside-out approach, which begins at the core of the security operation: understanding enterprise risk. When you truly understand your business objectives and the most likely risks that may be involved with achieving those objectives, you can then make sensible decisions about your defenses. Your security strategy becomes governed by the specific risks you face, rather than trying to protect against every threat in the universe. Once we build an enterprise risk model for our clients, we can then move into setting the security strategy, rationalizing infrastructure and optimizing operations. Ultimately, we evolve our clients' security programs so they are tuned to address the actual risks to their organizations.

EA: What does it mean to optimize and rationalize infrastructure and operations?

DB: These are the two key deliverables of the inside-out model. Once you fully understand your risk profile, you gain a clear understanding of the people, processes and technologies you need, versus those you don't need. You also can identify any gaps in your infrastructure. We help

clients understand all of this so they can rationalize their infrastructure – to make better use out of the technologies they have, and to put systems and processes in place to measure performance and better understand future needs. Once this is done, we also help clients optimize their operations. As I mentioned earlier, there is an acute cyber security skills shortage today, so understanding the capabilities of your staff, and deploying them into the right situations with the right processes in place, is critical. Too many security professionals today are stretched too thin or mired in mundane tasks that prevent them from performing higher-value duties. Optiv helps clients optimize operations so employees are doing more of the right things, outsourced options are used to offload duties that employees either should not or cannot perform, and we also develop strategies for orchestration and automation that enable employees and partners to be more effective. Finally, we help clients develop metrics to measure overall program effectiveness, which also provides intelligence for maintaining optimized operations over the long term. When you rationalize infrastructure, and optimize operations, you create a sustainable, measurable, and more effective security program.

EA: How will we see the cyber security industry evolve over the next five years?
DB: We're seeing an interesting shift in focus today toward automation and orchestration. I mentioned earlier how the outside-in model caused organizations to purchase too many tools for too many threats, and that there are not enough skilled professionals today to run all these tools. As a result, we are seeing dramatically increased investment and interest in capabilities that orchestrate and automate operations. We saw this dynamic play out in general IT operations more than a decade ago, where automation relieved IT pros from many routine tasks, while also enforcing best-practice processes. I believe we will see a similar business-process-optimization dynamic play out in security over the next five years. This all fits into what I've been talking about with rationalization and optimization. By orchestrating work processes and automating away routine and repeatable tasks, security organizations will become much more efficient and effective. This is good news – because when that happens, it will be more difficult for adversaries to penetrate defenses, and we may finally see the tide turn on the current breach epidemic. Optiv will be at the middle of this trend – and we believe the inside-out approach to security is the methodology organizations will adopt, because everything begins with enterprise risk.

Secure Access for Hybrid IT

An Interview With
Sudhakar Ramakrishna
CEO
Pulse Secure, LLC

ENABLING PRODUCTIVITY while ensuring protected and compliant access to applications and resources is a challenge as enterprises take further advantage of a mobile workforce, data center virtualization, and cloud-based applications and infrastructure. Business appetitive for anytime, anywhere access, and improved user experience, have resulted in an amalgamation of infrastructure and tools to quickly satisfy IT demand. As such, organization are re-assessing their technology stack that comprise secure access.

Common misperceptions are that previous access security capabilities can be readily applied across private cloud, public and SaaS. Or that new devices, including IOT and IIOT devices, and new mobile and cloud applications can be managed using the same controls as other corporate devices. Even the often-difficult question of "who is accessing what, from where, with what" has become more complex. A flexible, comprehensive platform can make the difference between simplifying secure access management and costly piece-meal approaches.

Pulse Secure is one of the few vendors focused on software-defined secure access for hybrid IT, building upon its Juniper heritage and expanding its solution set across mobile, virtual and cloud. We recently had a conversation with Sudhakar Ramakrishna of Pulse Secure to explore how the company and its customers are migrating from remote access to hybrid IT access protection.

EA: What is meant by secure access?
SR: Secure access is all about allowing IT to deliver seamless user connectivity to applications and resources- wherever, whenever and however is needed, without compromising security. These solutions provide IT the orchestration and interoperability crucial for connectivity, authentication, controls, data protection, availability and threat response on-premise and in the cloud. That is a direct definition. In practice, I am often saying that secure is "more about access, not control." We are not talking to customers about restrictive endpoint or network security products. We ask customers how we can enable user and staff productivity among

increasing requirements and limited budgets. Simply put, mobility and cloud drive greater agility and more options, but comes with increased security and data privacy exposures. So how can we mitigate these risks to allow our customers the means to push the boundaries of mobile and cloud applications use, user experience, and data center and cloud resource optimization.

EA: From a technology perspective, how has Pulse Secure and customers moved from Remote Access to Secure Access?

SR: Remote access is straightforward using SSL VPN appliances when devices are corporate managed, and the corporate data center holds the apps and resources. With the adoption of mobile and IOT devices, mobile and cloud applications, and data center capacity leveraging virtualization and cloud computing, our customer's operating environment and their threat surface has evolved - and our products have had to progress as well. The Pulse Secure Access suites encompass mobile, network, cloud and application access. Our unified client and policy engine allows for consistent user and device access visibility and control. Our mobile security for IOS and Android devices supports BYOD initiatives without intruding on a user's personal space. Our VPN solution provides a wealth of MFA, VPN and endpoint compliance functionality with open standards such as SAML to enable unified remote and cloud access. Our network access solutions allow for real-time network device discovery and profile checking, as well as extensive NAC features. And our ADC acquisition from Brocade provides us with virtual and cloud application load balancing with WAF. We have over 20,000 enterprise customers and millions of users worldwide. Ultimately, we want to provide our customers the confidence that as their requirements, applications and environments evolve, Pulse Secures capabilities, interoperability and adherence to standards will meet their needs.

EA: How does Pulse Secure provide enterprises visibility and compliance?

SR: Visibility and compliance are essential, and we are hearing that from the executive boardroom to security operations. Our VPN, profiling and Network Access Control (NAC) solutions provide an incredible amount of visibility and compliance functionality. As users, devices and systems connect to data centers, applications and cloud resources, each of our solutions allow IT and security staff to gain insight on user, device and application behavior, security state, and compliance violations. This data can be easily shared with others to enhance reporting, inventory, auditing and most importantly threat response. This helps network administrators and CSOs understand if systems are accounted for, if guests and IOT devices are managed, if endpoint security is active, if their environment meets corporate, industry and regulatory obligations, and even how applications are being used. Within our Pulse One management console and Secure Access suite, administrators can get a unified, dynamic view into users, devices and applications across remote, network and cloud. The breadth of coverage and level of fidelity is extremely useful. More so, policy-based controls allow administrators to enforce access policy and invoke remediation or mitigation actions which allows reduced IT staff to gain greater oversight and protection coverage.

EA: Where does Zero Trust play a part in Pulse Secure's on-going development?

SR: Zero Trust security is a security model that aims to advance conventional access security mechanisms to one that directly assures authentication, compliance and secure connectivity

directly between users, devices and applications/resources held in data centers or the cloud. In essence, our Secure Access solutions have always provided Zero Trust capabilities. In particular, Software-Defined Perimeter (SD-P) solutions offer Zero Trust functionality that aim to enable more rapid deployment, less infrastructure dependencies, greater application and resource protection, and improved user experience. The SDP security model is often associated to a "zero-trust" approach of trusting nothing and verifying all. However, it does not mean that other trust models should be excluded or invalid. Every SDP approach must accommodate some level of trust that is established while creating a user session, and typically remains valid throughout the session duration. This trust can be based on a combination of current and past assessment of user identity, authorization and reputation, device compliance and reputation, client application type, originating network, geo-location and connection type, information access patterns, and other factors. Not all scenarios or resources require a true zero-trust based policy, all the time. Different applications or classes of information can be mapped to a spectrum of trust levels that need to be established, per secure access policies, in order to grant access. That being said, current SD-P solutions are often easier to implement with web applications, less complex applications and fewer legacy IT dependencies. This limits SD-P adoption by a majority of mid-tier and large enterprise. At Pulse Secure, we see SD-P as another modality within Secure Access. Fortunately, the solutions and proven technologies that our customers rely on today are fundamental building blocks for Pulse Secure to bring an enterprise-class SD-P solution to market in the near term.

Advanced Tools to Support the Hunt

An Interview With
Eric Hipkins
CEO
R9B

AS CYBERSPACE has emerged as the fifth domain of warfare, now with its own combatant command, addressing challenges has shifted. This is complicated by the crossover that exists between what might constitute an act of war and what is better classified as criminal activity. We are still on the frontier of sorting it all out. What we do know is that organizations across the public and private sectors need a new approach to defending networks.

Recently, threat hunting has become the buzzword across security circles. As the company that first introduced this concept to commercial markets in 2013, *R9B* has made it a priority to develop the best threat hunting products and services. R9B focuses on building powerful analysis and support tools to assist the modern hunter with the often-complex task of dealing with cyber threats. These tools range from credential-based risk analysis to active adversary tracking and hunting across either an enterprise or a larger infrastructure. We recently sat down with Eric Hipkins, CEO of R9B to better understand how R9B supports this critical task.

EA: What are the typical tasks of the modern cyber hunter?
EH: Most of the actions by threat hunters are dependent on mission requirements, so it is difficult to identify a typical set of tasks. Some organizations still view hunting as analysis against passive collection techniques, such as reviewing logs or network traffic. At R9B, we view hunting as a human-led approach to pitting a thinking defender against a thinking adversary. In this regard, some common skills needed for any hunting mission include experience with operating systems and networking, as well as an understanding of how threat intelligence integrates with mission parameters to guide the hunt and adapt to the adversary. On top of technical knowledge, a hunter's greatest ability is in creative thinking; generating hypotheses that can identify adversaries that bypass traditional defenses and hide in the network.

EA: What are the offerings from R9B that assist hunters in their work?
EH: Since 2011, we have provided training on a broad range of topics that can significantly improve the efficiency and effectiveness of a hunter. That includes courses in cyber threat intelligence analysis, adversary tactics and techniques, PowerShell foundations, and OS-specific

hunt certification. Our proprietary ORION platform was purpose-built for threat hunting. It is an agentless means of detecting, pursuing, and eliminating threats from networks. We recently gave it a new user interface and incorporated an API so that advanced hunt teams can customize it to their needs. Originally launched in 2013, ORION is currently used and has proven effective in both corporate and military environments. We also offer a credential risk assessment tool called ORKOS, which aids hunters by helping them quickly survey networks to identify connections that could make it easier for attackers to escalate privileges, moving from low-level to critical systems.

EA: Can you tell us more about how your solutions focus on credential risk?
EH: Early on, we recognized the importance of credential theft in the execution of malicious activities. In response, we developed software called ORKOS; a credential risk assessment tool designed for rapid deployment and credential risk vulnerability analysis. Administrators can quickly plug ORKOS into their network to get instant visibility into weak credentials (we use proprietary rainbow tables and hash matching to identify weaknesses while protecting privacy). Where ORKOS differs from less robust solutions is in its graphical representation of privilege associations, how they can create risks, and remediation recommendations. We believe strengthening passwords is a good first step, but we also want to make sure administrators know how an attacker might use a low-level frontline user to escalate privileges and move laterally through the rest of victim networks. ORKOS builds scenarios to provide custom remediation recommendations to mitigate identified credential risks within a virtualized environment.

EA: Do users have to be highly experienced in their craft to benefit from your tools?
EH: We have invested significant time and energy in making all our solutions easy to use. Our experiences have taught us that even the most experienced operators still appreciate quick deployment, good design, and intuitive controls. Threat hunting against advanced adversaries can still require a highly-specialized skill set and tools are only part of the equation. At R9B, our mantra is “human-led. technology accelerated.” So, to be an effective threat hunter, it does take a lot of knowledge and experience, but for those who know what they are looking for, our tools make life a lot easier.

EA: What are some hunt-related trends you’re seeing in your customer base?
EH: As the security industry continues to adopt threat hunting, it has been encouraging to see an uptick in the pace of technological development. There is better collaboration across the board. Overall data management is still a major challenge, but artificial intelligence and expert systems are powering faster and more accurate analysis. We recently made a significant strategic investment in a company called Champion Technology Company, Inc., whose DarkLight® AI expert system is helping our hunters find threats faster, so they can focus more on cleaning up the network. I look forward to continued collaboration, more development for API integrations, and better ways of making sense of the data.

Automated Virtual Security Analysts

An Interview With
Mike Armistead
CEO
Respond Software

THE MODERN security operations center (SOC) suffers from the practical limitations of finding experts who can perform the required combination of analytics, investigation, and expert technical analysis to be effective. Sadly, the supply of such people continues to wane, and for organizations hoping to beef up their SOC-based controls, this trend is neither welcome nor acceptable from a security perspective.

*Respond Softw*are addresses this challenge by introducing expert automated tools to support these essential tasks. In addition to automating SOC tasks, the Respond platform can help modernize the SOC and improve the quality of analysis being performed. We recently asked Mike Armistead, CEO of Respond Software to share his insights in this important area and to help us understand how automated analysis can be introduced to the SOC.

EA: Is it now a given that finding experts to work in a SOC is near impossible?
MA: Our customers tell us that the idea of having an expertly-skilled virtual analyst becoming part of their security operations center is a great idea. This suggests that it is hard – and yes, perhaps sometimes it seems near impossible – to find human experts to come and work in your SOC. But more importantly, the type of virtual support that comes with the Respond Analyst brings capabilities that are more powerful than just hiring a human expert – even one with great experience.

EA: Was there an important insight that helped you design the Respond platform?
MA: It was our observation that unless analysis is done at machine speed, the potential to successfully keep up with the advancing cyber threat is diminishing. And we could see that this emerging requirement to automate advanced protections in the SOC provides an opportunity to introduce AI-based methods to the defense. This enables a new type of self-adaptation to a real-time cyber attack.

EA: How does the Respond Software platform work?
MA: The Respond Analyst is built using our patent-pending Probabilistic Graphical Optimization (PGO), which identifies and uses the various dimensions of internal and external environment

context related to cyber security and then make decisions. The Respond Analyst engine uses PGO to basically model the judgment of a human, but to do so in a more comprehensive and effective manner – if only because so many more factors can be ingested, analyzed, and synthesized quickly.

EA: How would a typical enterprise introduce your solution to the security infrastructure?
MA: The platform is designed to integrate smoothly into the existing SOC lifecycle, which includes the first vital step of ingesting and gathering relevant information related to present and future threats. The second step involves scoping and building a case that something important has occurred or is occurring – and this requires analysis and input from many different groups within and related to the SOC. This is then escalated and prioritized based on the specifics of what has been identified. Response activities then commence, followed – hopefully – by improvement through feedback. The Respond Analyst was designed to provide support, assistance, and automated improvements in all aspects of this SOC lifecycle.

EA: What are some SOC-related trends you're seeing in your customer base?
MA: The most obvious trend is the inability of existing manual procedure-oriented SOC teams to keep up with the speed, size, and scope of modern cyber threats. This originally led to increased attention to finding SOC analysts – and this continues to be an important activity. But most SOC teams today have accepted that automation is likely to provide the greatest return on investment, and will be the key to dealing with the advancing modern cyber attacks coming from increasingly smart attackers.

Advanced Support for Threat Hunting

An Interview With
Mario Vuksan
CEO
ReversingLabs

THREAT HUNTING solutions from ReversingLabs were created to locate advanced malware with a focus on undetected malware that has penetrated a company's defenses. To enable threat hunters, ReversingLabs provides a rich set of tools and services that include automated file decomposition and static analysis, integrated YARA rules for hunting, contextual pivoting, retro-search, high volume file classification, and integrated file reputation services.

We recently asked Mario Vuksan, CEO of ReversingLabs to share with us how his company is developing a platform based on these next-generation methods. We also wanted to learn how ReversingLabs customers, who work in enterprise security operational settings, performing threat hunting tasks are putting these capabilities to use in their day-to-day work dealing with advanced adversaries.

EA: Mario, I know you have some strong opinions about how threat intelligence should be implemented and shared, can you explain these opinions to us?
Mario: Let me focus the answer on the sharing portion of the question. We strongly advocate that organizations should *not* be pushing as much intelligence data as possible to their internal security teams, as well as friends and partners. We also do *not* believe that organizations should be trying to grab as much intelligence data as possible from all the commercial and free partner sources, because that generates unnecessary work. We advocate instead a pull-method where the incident response teams look at investigations to make sense of them and convert them into rules – something like Yara rules. Specifically-defined threat intelligence converted to actionable data like Yara rules can then be shared across security teams and with partners who then can look through their repositories to find the matches and activate responses. Partners can run the results through their legal teams and then share them back.

EA: ReversingLabs talks about the difference between global threat intelligence and local threat intelligence, can you explain the difference and why local threat intelligence is so valuable?

Mario: We want to make sure people focus on the data that they really have. We see many organizations using outside vendors to collect as much intelligence data as possible, much of which is not relevant to their local environment. Today, everyone is focused on SIEM and pushing more log-based data into solutions like Splunk, Elastic Search, or Hadoop. That's all interesting, but it's not complete, because most producers of logs tend to filter out relevant data. Examples include sandboxing solutions that filter things they cannot process, and endpoint solutions that focus on things running in the memory. They do not look at all the other data that is available to them. ReversingLabs' believes that local threat intelligence is absolutely necessary if you are going to look for things unknown, like zero-day artifacts. Local threat intelligence is important if you are going to successfully find threats that are in the early stages of the kill chain.

EA: Mario, you place a specifical emphasis on file intelligence as a subset of threat intelligence when talking about understanding threat context, can you tell us about that?
Mario: Absolutely. We see little focus on files, objects, and transactions. That is not surprising, because it is hard to process millions of objects a day to derive their context. So, it is normally not done. However, as we move into the cloud, the network context becomes muddy. Knowledge about what really flows through those network sessions, what's packed into those emails, or what's shared through different endpoint sessions, becomes more and more important, and much more difficult to see. We advocate a single infrastructure that will cover pretty much everything an organization sees from Windows, Linux, MAC OS, and mobile, to anything that can be emailed or found on an endpoint. This file-level visibility is the only way that security teams are going to truly understand what threats are entering or are inside their network. This also becomes an important stepping-stone toward inspecting commercial applications and understanding transaction-based payloads which these days are more like self-contained operating systems. This includes SAP, Swift, or more important things like Union Pay, Allpay, and Wepay.

EA: Let's look at a specific example, NotPetya, a how would this type of Defense have helped us prevent the damage that NotPetya achieved?
Mario: What is interesting about NotPetya is the initial vector. It was emailed with a trusted updater for Ukrainian auditing software which it could control. It wasn't something that could be dynamically detonated. Using static analysis file technology developed by ReversingLabs, we can analyze any type of object to determine whether it is good or bad. We also provide rich static behavior report on that object without detonation. This information would have allowed security analysts to determine the identity of the attack (NotPetya versus Petya) and provide the information so that they could have taken much faster action to contain the attack. This illustrates the need for an effective local intelligence repository, where you store all possible evidence. You can then down-sample with the help of global intelligence. Our research team could quickly down-sample to the actual attacker components that were part of the NotPetya. In the early days of the attack, organizations were subject to a large deception campaign. They were dealing with about half a million decoy components. We found and shared the 18 real components of the attack that were essential to be able to produce appropriate protective measures.

EA: How does your platform integrate into existing SOC environments and with third-party security tools?

Mario: Our integration includes network forensics, email, EDR, and storage (like S3) whether local or cloud-based, or whether a commercial application emitting transactions that need to be inspected. These are the starting points for scalable, in-depth file inspection. The benefit of ReversingLabs is to give organizations tens of thousands of indicators organized around a unified database schema that enables advanced search and hunting. On the other hand, ReversingLabs can integrate with a slew of security technologies like Sandbox products for additional context, SOAR for orchestration, SIEM for alerting, and analytics solutions for hunting.

EA: What are some hunt-related trends you're seeing in your customer base?

Mario: One trend involves analyzing components that cannot be detonated such as third-party updaters. As we already discussed, NotPetya's initial vector was not a document lure or an exploit, but a trusted third party software updater. Similarly, detonation was not helpful when analyzing proof-of-concept Spectre and Meltdown samples. Our customers are increasingly crafting complex rules, as can be expressed with YARA, to look for zero-day malware, activities of various APT groups, and to search for exfiltrated or sensitive data. For most global organizations, text search is really a binary problem as they operate in areas that do not run on western alphabets. Finally, only with binary search of richly extracted indicators, can one start discovering new document malformation techniques that are still a quintessential part for all phishing campaigns.

Vulnerability Risk Lifecycle – Prediction and Validation

An Interview With
Srinivas Mukkamala
CEO
RiskSense

WHEN AN enterprise carefully examines its overall cyber risk, a so-called *attack surface* emerges, which is the set of entry points where vulnerabilities can be exploited by malicious actors. Viewing cyber risk in this way, results in the strategic objective of reducing that attack surface, generally through careful discovery of vulnerabilities combined with purposeful action designed to reduce the risk of exploits to such weak points. Predication and validation are the key activities in this regard.

RiskSense is one of the leaders in this growing area of vulnerability and cyber risk management for the enterprise. The team was instrumental in predicting WannaCry, and subsequently released useful safeguards after the initial infiltration. We recently sat down with Srinivas Mukkamala, CEO of RiskSense, to better understand how his platform addresses this area, including how his company utilizes intelligence-driven risk analytics to lead to actionable cyber security mitigation.

EA: What are the primary internal and external inputs to intelligence-driven threat analytics?
SM: Today, the best input involves collected data from vulnerability scanners. This provides a good starting point, which covers networks, applications, and databases. You then need to enrich this scanner data with threat data to truly understand what is actively being exploited. Next, users must assign criticality to those assets that have been scanned. This helps produce an overall picture of the risk of the IT infrastructure being analyzed. The resulting combination of this data supports a truly intelligently-driven threat analytics platform.

EA: How can ingested vulnerability data be normalized into an enterprise view of risk?
SM: We aggregate vulnerability data and normalize it for common terminology and data scales, mapping it to CWE, CVE, CPE, and OWASP. We then contextualize the data by correlating vulnerability relationships with multiple external threat data sources. This includes zero-day, malware feeds, exploit databases, exploit and penetration testing frameworks, dark web, and DShield. RiskSense penetration test results, as well as business criticality (e.g., asset classification and assign asset risk), deliver a complete view of the risk a given vulnerability

represents to the business. This allows us to map the results into our risk scoring model and to provide a single, credit-like risk score for every device, thus providing useful information for each business unit in an organization.

EA: Tell us about the RiskSense platform and how it addresses the attack surface.
SM: We already see that enterprises have expanded to mobile devices, networks, applications, and databases. We are also moving toward containers and IoT devices across IT and OT infrastructure. The attack surface is thus expanding rapidly and dynamically. This increases the likelihood that an attack can occur from all entry points. The RiskSense platform focuses on these attack surface entry points and allows you to incorporate vulnerability scanner data, enrich it with our 60+ threat data sources, and then factor in the criticality of your assets to derive a risk rating for each asset. The resulting risk rating drives your remediation efforts, guides your IT team on the best order for installing fixes, and ensures that you are focusing your security and IT resources wisely. The asset risk rating rolls up into department/LOB/agency risk rating, and then into an overall risk score. This score provides executives with a simple credit-like scoring framework to assess organization risk and track this over time.

EA: What is the best way to drive proper remediation once vulnerabilities have been identified?
SM: Once you have identified your vulnerabilities, you need to add threat context, basically enriching the data around these vulnerabilities, and specifically identifying which ones are exploitable in your IT infrastructure and which ones will be weaponized. Then you need to assign business criticality to each of your assets. This provides a true risk score for your specific organization, and provides prioritization on what really needs to be fixed first.

EA: Have you seen any significant trends in how your customers view and manage cyber risk?
SM: The most security mature organizations are going beyond just what to fix, and are now building out an overall security rating framework for each LOB or department or agency. They are then rolling that up into an overall cyber risk score. We call this the RiskSense Security Score (RS3). This allows organizations to track their journey in reducing risk, while keeping a continuous watch on it. These best-in-class organizations understand that their attack surface changes constantly with new devices, applications, and databases being added and removed every day. With attackers developing new attack models, they must be vigilant. Building a Threat and Vulnerability Management Program mandates a risk scoring model that guides both the security and IT Operations team which inform executives of current risk standing for an organization, this is a game changing model.

Known Device for Strong Authentication

An Interview With
Steven Sprague
CEO
Rivetz

AUTHENTICATION, WHEN performed at the application level, suffers from its dependency on operating systems and other software that are vulnerable to common malware exploits. A better approach involves the use of hardware roots-of-trust, using a chain of cascaded assurance from the hardware to the specific interaction with an entity being asked to validate their identity. Trusted platform modules (TPMs) are useful resources for this type of approach.

Rivetz has been one of the great innovators in this area, developing solutions for smart phones, tablets, PCs, and other devices to be more "known" with high assurance, rather than to serve as lower assurance platforms for less secure authentication protocols. We recently asked Steven Sprague, CEO of Rivetz, to offer his ideas and views on this approach, and to help us understand where authentication of "known" devices is headed.

EA: What is meant by known versus unknown devices?
SS: A known device is a device that has Identity and has been measured. In general, it is hard to measure the whole OS to trusted computing, and Global Platform has defined standards for the Trusted Execution Environment (TEE), which is a measured environment running measured code that can easily store and process keys and messages/instructions. An unknown device would be the PC you have today that is on the network you have logged into, but the computer processing and sending you data could be controlled by an advanced persistent threat. It could be feeding you false information that you believe is correct, or it could intercept and alter the data you are sending.

EA: What role does hardware play in the high assurance process your team supports?
SS: Hardware is required because hardware can provide an immutable root of trust. Hardware can hold data that cannot be altered by software and that root of trust can be used to build a measured execution environment. Today Rivetz uses TEE, which is built on the hardware foundations of ARM TrustZone architecture. As the platforms and technologies evolve, Rivetz intends to support them all.

EA: How does the Rivetz platform work? What types of devices do you support?
SS: Rivetz is built on the ARM Trustzone capabilities and we have partnered with a company called Trustonic who provides the TEE OS we use to enable the hardware. This technology has been deployed on more than 1.4 billion devices to date. Rivetz's focus is the major Android providers such as Samsung, HTC, LG, Sony, ZTE.

EA: Do you see authentication evolving in the coming years along the lines of what you've been doing?
SS: Yes. Authentication is no longer enough. What is required for blockchain and IoT is secure instructions or messages. The messages contain the transactional information that will be delivered across the public networks and process within the devices. Secure instructions are the foundations of payment as well – many of the core technologies were developed to enable secure banking and e-commerce.

EA: What are some trust- and assurance-related trends you're seeing in your customer base?
SS: The world is moving in the direction of greater privacy and greater decentralization. The shift from an enterprise having cybersecurity controls that are applied to all things at all times is over. The security model is moving to the endpoint. Trusted computing enables a decentralized software-defined security model that results in provable controls embedded within every transaction. The mixing of trusted computing and blockchain technology will enable the global evidence-driven model that is needed for GDPR, privacy and blockchain.

EA: Why does blockchain need Rivetz?
SS: Blockchain is a new model for storing a fact on the internet. The ability for data to be proven has not changed. Rivetz is building the tools to embed within the blockchain the evidence that the data recorded on the chain was what was intended. The tools will provide proof that a measured device in a known condition wrote the instruction to the chain. This evidence can easily be stored with every transaction as a second hash or signature. We're delivering strong, provable cybersecurity controls as part of every chain. A new model is emerging – a model that is built on the foundations of identity and not connections. The heart of the new networking and service delivery model is not the identity of the user, but rather the identity of the device. All information-sharing, and all secure transactions, must be done from known devices in a known condition. The Rivetz solution provides a strong first step in the direction and can be easily be used to define new models for decentralized security.

Advanced Cyber Security Solutions from RSA

An Interview With
Doug Howard
Vice President, Global Services
RSA

FEW BRANDS have the iconic status in cyber security as *RSA*, now a Dell Technologies company. RSA's solutions-oriented approach leverages their platform, which includes RSA NetWitness Platform (Evolved SIEM), RSA SecurID Suite (Identity authentication and governance solutions), the leading Integrated Risk Management platform – RSA Archer Suite, and the powerful RSA Fraud & Risk Intelligence Suite. The company is also well known for the RSA Conference that helps define our industry. Driving security, risk management and fraud prevention innovation for enterprise customers around the world, RSA has more than 750 full-time global employee security experts - making them one of the larger security and risk consulting firms.

We recently sat down with industry veteran Doug Howard, who serves as the global leader for services at RSA. We asked Doug to share his insights into the emerging cybersecurity marketplace and to help us understand the strategy and direction of RSA, including the company's growth in security services. Few people have the experience of Doug and the RSA executive team, so their collective guidance is certainly worth listening to.

EA: What are the primary security-related issues and pain points you are hearing from enterprise security teams?
DH: The fast-paced industry has quite a few players messaging how point products can solve a specific problem. We know there are a lot of threats and solving with point products has resulted in nothing more than noise to most organization. The cybersecurity industry is a gluttony of purpose-built products with more than 1,500 companies all vying for enterprise dollars. Often underlying all this is the fact that customers haven't firmed up their foundational approach to managing risk and security. Many ask us to help them formulate and prioritize their execution, specifically around: Rapid detection and response to threats through deeper visibility; frictionless identity management and governance; and fraud prevention that they want us to wrap it all up in a risk management program. RSA considers these four pillars foundational to any risk and security program. In fact, our strategy has been focused on these areas to help create efficiencies and effectiveness by optimizing existing resources and processes and maximizing economics through leveraging technology. RSA Risk and Cybersecurity Practice is a combination of expertise, process and technologies. In addition to

our products, we bring the experience of completing 2,500 unique engagements a year. Candidly, one of our first exercises is to optimize the technologies and people in which an organization is already investing. Experience shows that customers purchase most products for a specific need or use case; rarely do they achieve 100% of the value they aspired to with that purchase. The flip side is that these products can provide far more value than the specific need they were purchased; leaving organizations receiving only a fraction of the technology value they have on-hand.

EA: Tell us about the solutions approach at RSA from the perspective of existing and new products and services.

DH: Our approach remains constant – namely, to bring high-value solutions that can be operationalized and to provide the flexibility to evolve based on the risk and threats that organizations are trying to protect against. By continuing to invest in foundational needs that help customers create efficiencies, effectiveness and continue to evolve their capabilities to reduce risk, we believe we can remain a trusted advisor to our customers. Because of our risk management heritage, we align the underlying capabilities of RSA, in both products and services, to help organizations reduce their risk to reputation, risk to revenues/mission, and risk in achieving regulatory requirements. In all this, we help organizations not only defend against risk, but to flourish in the digital transformation they are undergoing. The new solutions, product innovations, acquisitions, and thought leadership allow us to continually enhance and expand our solutions in ways that bring more value, faster, and with less effort to our customers. The RSA Risk Frameworks are just one example.

EA: What are the RSA Risk Frameworks and what are your future plans?

DH: Let me answer the future part first. As I mentioned, we aspire to provide our customers with foundational technology platforms that bring value today and far into the future. That means RSA acquires or partners with feature and point solution companies leveraging our foundation, or those that allow RSA's platforms to provide more value. Our services approach is to help organizations achieve an optimal operational state while continually reducing risk. For RSA, this is often oriented around digital risk management and is related to cyber. Sometimes this is more business risk oriented - such as Third-Party Risk Management, Business Impact Analysis, and other business-aligned risk reduction activities. To best serve the industry, RSA has worked with other industry players to create RSA Risk Frameworks that provide customers an easy approach to quantify their maturity in continually reducing the probability and impact against a specific risk. Initially focused on Cyber Breach Risk, Third-Party Risk, Resilience and Data Privacy Risk, this approach allows us to take a macro risk, reduce it down to segments and quantify each. With the quantification, we then apply our experience to help clients prioritize the activities with the biggest impact on risk reduction at the most optimal level of effort.

EA: As a veteran in our industry, you must be seeing some important, and perhaps recurring themes in the cybersecurity ecosystem. Do any of them stand out in your mind?

DH: One of the benefits of being part of Dell Technologies is the increased access to higher level executives – those managing or influencing more broadly across the IT footprint and business. This has given RSA even more visibility into the lack of business, risk and security alignment.

RSA believes there are many alignment opportunities that allow risk reduction and cybersecurity to be better understood by the business leaders, but equally leverage quantification as a common point of reference to establish ongoing strategy and execution alignment. Often, helping customers better defined what mature, or even what good looks like is the starting point in this Digital Risk Management journey. Leveraging this quantification to better define short-term and long-term goals, prioritize and measure progress is key to progressing as an industry.

Driving Continuous Validation through Attack Simulation

An Interview With
Guy Berjerano
CEO
SafeBreach

PENETRATION AND functional security testing are obviously necessary controls in any enterprise or infrastructure environment. A major challenge, however, is that while both forms of testing provide point-in-time validation, neither offer continuous validation on an on-going basis. Such continual validation can only be obtained properly through automation techniques such as simulation.

SafeBreach has developed a platform for continuous validation through an attack simulation platform that enterprise teams integrate with their live systems to demonstrate various security properties. We recently asked Guy Bejerano, CEO of SafeBreach to explain how his team accomplishes this mission and how his platform works in the context of enterprise and infrastructure systems.

EA: How does attack simulation work?
GB: Attack simulation works by executing real attacks on simulators in live production environments. Actual attackers use techniques to infiltrate environments, move laterally to find sensitive data or systems, and then either exfiltrate data or attempt to control systems from outside. With SafeBreach, our simulators replace the real attacker across the kill chain, from email and web infiltration to endpoint infection. Since our platform controls all simulators, we can ensure the attacks are safe and contained, and we can visualize which attacks are blocked by security, and which are not. The results of the simulations show, with no false positives, where the risk lies. The platform provides the tools to sort, filter, and prioritize findings to help security teams stop attacks, and get the most out of their security investment. And of course, it's integrated with platform automation and orchestration to ensure that operations teams can address issues quickly. And since our platform runs continuously, all fixes are automatically re-validated over time to ensure their effectiveness, and to minimize exposure as new issues are identified.

EA: Can attack simulation go awry and cause problems in a live production environment?
GB: Not the way we do it. My co-founder and CTO and I have built our platform to be completely safe. Imagine, for example, a next-generation firewall segmenting an organization's

environment into production and corporate. One simulator is placed in production, and the other in corporate. SafeBreach will validate the effectiveness of that next-generation firewall by attempting to transfer a malicious payload from one simulator to the other. The payload is only sent between simulators, and either blocked, or immediately destroyed by the receiving simulator. Other attack techniques might try to send sensitive data; for example, hashed credentials from one simulator to another, to see if IDS or DLP tools will see that traffic and block it or raise alerts. In these cases, the payload isn't malicious, but the data could present a security risk. So, SafeBreach simulates that hashed data with our own credentials. That keeps the accounts safe, but still proves whether defenses are configured to stop these kinds of attacks. Likewise, SafeBreach simulates data relevant to the phase and type of attack used. Credit card data, customer record data, and source code are simulated by SafeBreach, so customers can validate controller effectiveness without putting data at risk. Validating endpoint and host-based simulators includes network actions, and local methods such as dropping malware to disk, executing remote commands, and attempting to lock files. Again, our simulations are safe, because malware isn't executed on any endpoint. Instead, the behavior of malware is simulated without unleashing live worms or Trojans within production. Since the techniques mirror those of actual attacks, endpoint security solutions should stop our simulations or trigger detection alerts

EA: What are the components of your platform and how are they deployed?
GB: The SafeBreach platform is comprised of a management server and simulators that play the role of the virtual hacker. The centralized management server incorporates the complete Hacker's Playbook™ of breach methodologies, and manages a distributed network of breach simulators from a centralized location. This includes the ability to manage all aspects of simulator configuration, to review breach methodologies that have been successful or blocked, and to generate reports on breach patterns. The management server can be deployed on-premise or in an enterprise cloud infrastructure (AWS, Azure). The SafeBreach simulators perform the role of the attacker, simulating traffic within the cyber kill chain. Three different types of simulators are supported: Network simulators are deployed as virtual machines, and run network breach methods; host-based simulators are deployed as lightweight agents on endpoint or server systems; and cloud simulators act as infiltration and exfiltration points, located in the enterprise cloud infrastructure. Cloud simulators participate in network breach methods only.

EA: What attack strategies do you simulate and where do you come up with these strategies?
GB: Our threat research team, SafeBreach Labs, has built over 3,600 attacks that run continuously in our customer environments. These attacks range from tried-and-true favorites like malicious email, DNS tunneling, and NTP exfiltration, to more modern threats like file encryption. We're proud to have a team of experts that's recognized within the industry at shows like Black Hat and DEFCON, because they are always building new and never-before-seen attacks. We follow many emerging threats closely; for example, when new US-CERT alerts are issued, we reverse-engineer and simulate those campaigns, typically within 24 hours of announcement.

EA: What are some security threat-related trends you're seeing in your customer base?
GB: The primary trend we see across our customers is the overwhelming complexity of today's security deployments and the risk that introduces. All too often, companies have deployed dozens of defensive tools, but the rules and policies conflict, which leads to attackers slipping through defenses. Similarly, most of our customers find that they don't need to add new products. Instead, they already have what they need, but existing tools are simply not optimized. Many security teams tend to get caught up in the race to buy more defenses, but might achieve the same goal by optimizing what already in place. On this same theme, most of our customers tell us they are absolutely buried in the challenge of addressing cyber risks to the enterprise.

Managing Risk and Compliance for DevOps

An Interview With
Nish Bhalla
CEO
Security Compass

IN THE past decade, there's been an under-reported shift in enterprise security. Many organizations have adopted automated platforms to support governance, compliance, and risk (GRC). Originally developed to reduce mundane paperwork, GRC platforms evolved to support compliance controls in business unit infrastructure. And, more recently, businesses have recognized the need for GRC in the context of DevOps.

Security Compass has led the on-going movement in supporting security compliance and risk management in software development. We recently asked Nish Bhalla, CEO of Security Compass, to provide an overview of modern GRC protections in legacy and modern DevOps lifecycles. We also asked him how the Security Compass platform works in the context of such software processes.

EA: Why should we care about software security, and why isn't it a priority for most industries?
NB: As software applications become more prevalent in business and more crucial to organizational success, it becomes critical that we protect our assets. Unfortunately, this isn't a priority for many organizations due to a lack of awareness regarding the potential consequences. However, new regulations will be enforced soon, meaning that security will start to become a greater priority. For example, the proposed PCI Software Security Framework and the New York State Department of Financial Services (DFS) Cybersecurity Regulation 23 NYCRR 500 Section 500.08 (Secure Application Development and Auditing) which is being enforced as of September 4, 2018.

EA: Does DevOps introduce more security threats, or does it have a more risk-reducing impact?
NB: In a DevOps environment, you can deploy applications faster which in turn allows you to respond faster to identified security defects. Ultimately, this reduces the cost of fixing defects as well. The main drawback related to the introduction of DevOps is that, those organizations who have dispensed with their old security activities haven't necessarily established compensating activities that work with the new DevOps methodology. Without encountering

any immediate negative consequences, organizations will proceed with business without sufficient security due diligence in place, until they encounter an issue.

EA: How does the Security Compass platform work?
NB: We provide tools that integrate security and compliance directly into the DevOps process. Some people have referred to our platform as supporting governance, risk, and compliance (GRC) for DevOps – and this is an accurate reference. The whole idea of the Security Compass solution is to ensure that the automation inherent in DevOps is complemented with security automation to create a DevSecOps approach – thus resulting in more secure products being developed. The central part of our solution is SD Elements, which translates policies to prescriptive, measurable procedures that are used by IT and Engineering teams to achieve their security and compliance objectives. SD Elements generates and tracks granular security controls with a flexible, rule- based engine and integrates those controls into Application Lifecycle Management (ALMs) and enterprise workflows used by development teams. SD Elements also delivers Just-In-Time training to developers, providing concise, contextual guidance on how to implement controls right when they need it.

EA: What are some software-related threat trends you're seeing in your customer base?
NB: With the trend towards Agile every part of the software development life cycle is moving more quickly, which is why an automation platform, such as ours at Security Compass, is essential to every software development team. Automation is the key to dealing with the rapid pace of development vs. the rapid advancement in adversary capabilities and ever-growing complexity of regulatory compliance. Customers also seek our help in dealing with privacy, compliance, and other non-functional requirements. The trick is creating and establishing a system that allows you to operationalize the identification and tracking of these requirements throughout the SDLC, which is one of the features of our platform. This gives management the visibility into the security posture of all their applications at a glance, but also makes it easy to prove to regulators and auditors that best practices in secure software development have been followed by the organization.

DATA:*empowered* to Reduce Enterprise Risk

An Interview With *Greg Taylor* *CEO* *Sertainty*

ONE CONCEPT that unites and is agreed-upon by the entire security community is that we all need better solutions for protecting our data. The old concept of relaying on a perimeter so that we can just leaving structured and unstructured data largely as-is, has exposed itself as a bad idea. What's needed instead is some way for data to self-protect – and to basically become empowered to respect the access policies that are desired by the data owner.

The team at Sertainty has been hard at work for several years on this idea of self-empowering data to enforce policies. We recently caught up with Greg Taylor, CEO of Sertainty, and asked him to help us understand Sertainty's idea of empowered data, and how the typical enterprise or service provider might benefit from taking a new approach to preventing data breaches to malicious criminals and adversaries.

EA: Greg, help me understand the origins of Sertainty product term that you use – namely, 'data: empowered'?
GT: What we mean by data being empowered is that it can basically act and react to its environment. With our technology, the data becomes an active participant in the relationship between the data creator/owner and the data user/receiver. This owner-user relationship can be a machine-to-machine communication, or it can be human-to-human. Because the data is in control of this relationship, it is very difficult for either the owner or the user to abuse their privileges. This is what we mean by our term: 'data: empowered.'

EA: Does your technique differ from traditional digital rights management?
GT: Information rights management (IRM)/digital rights management (DRM) solutions for enterprise are typically single encryption, whereas our solution uses encryption that is multi-layered and multi-facited. We manage multiple, dynamically created keys from within the file, thus eliminating the need to share. Traditional DRM, in comparison, stores keys externally, requiring a share. We embed and enforce the security policies from within the file, where

traditional DRM governance rules reside on and are enforced by the server. Most DRM solutions are limited to file-level decryption. Sertainty technology enables software developers to selectively decrypt information within a file at a much more granular level, and without compromising availability.

EA: What are some use cases you see as being optimal for the Sertainty solution?
GT: Our software development kit (SDK) consists of robust routines that allow for a custom deployment to utilize data:*empowered* just as it would with data in the clear. Virtually any data-centric value proposition can thus be driven in some way by data:*empowered*. The Sertainty technology is as much an operational technology (OT) play as an IT one, introducing many possibilities such as data-as-a-sensor, data-as-a-user, and data-as-an-end-point. I know you're keenly aware of machine learning, so just imagine data that can learn! Now, regarding use-cases, let's go through a few of the more instructive examples: We've deployed our technology into a B2B application for transaction processors in the customer critical communications market segment. The customer replies on a variable-user, multi-step workflow that consumes client data from banks, utilities, or insurance companies, and produces statements, legal notifications and invoices for customers. Ordinarily, this data would be encrypted, decrypted, copied and archived, yet there were cases where clear data was vulnerable and HIPPA or PCI compliance was difficult to audit and enforce. With data:*empowered*, the process prevented clear data from being exposed and from any potential theft. Additionally, audits are self-generated and compliance automatically enforced. Many other interesting use-case scenarios come from customers using data:*empowered* to protect data transfer of critical flat files and customers using our technology to protect licensed content such as music, video, film, and literature. By integrating Sertainty technology into the licensed content workflow and the master-file itself, *each of the rights holders* can once again irrefutably associate the license with their content. Once copies of the master are distributed to the Digital Service Provider, there will exist permission-based level of transparency of the entire process to all rightful parties; an immutable validation of plays and ultimately; and real-time automation of accounting and distribution of royalties.

EA: Can you tell us a little more about the encryption technology used in your platform?
GT: What we do is implement an industry standard AES-256 cryptographic algorithm at a very granular level. That is, we randomly determine and create some number of segments of a data-file, and we then apply encryption to every segment of the file, where every segment can only be decrypted via its own unique key. The approach we take to manage this not only enhances the overall protection schema by integrating governance into the mix, but does so in a way that is not disruptive to the workflow. The overall benefit is a reduced dependency on infrastructure for data at rest or in transport. Sertainty, while utilizing but not modifying today's AES-256 encryption standard, has developed a way to combine the external governance mechanisms, as an input to the "internal" cryptographic protections. With Sertainty technology the governance rules which were externally applied by the operating system are transferred into the data file as is the KMS. These functions are controlled by the Sertainty Intelligence Engine which becomes part of the file. This provides a means to simplify the cryptographic implementation process, eliminate the need to separately pass keys, and by association have them stolen, eliminate the

risk of data exposure if an encrypted file is stolen, and eliminate the need to use differing encryption methods when the file is moved from one protected enclave to another. We created a process that combines all previous internal protections with most of the external protections that extend those protections in a synergistic manner rather than just be additive. The best example of this synergism is that a file can report back to the data owner when it has been opened, giving the owner proof positive of who, when, where, and on what device a file has opened, or was attempted to be opened. Previously, this type of information was only available from an application acting on the data, not the data itself initiating the confirmation.

EA: What are some data security-related trends you're seeing in your customer base?
GT: A few years ago, not very many people believed they were vulnerable or even a target. They basically felt they were safe. The Equifax breach changed all that. Our Sertainty Workflow Tool is thus now getting a lot of attention, because it conveniently and seamlessly addresses that kind of data loss. The customer can implement a data:*empowered* solution without disrupting the existing communications channels, or the existing infrastructure and applications.

Detecting and Mitigating Imitation Attacks

An Interview With
Sumit Agrawal
COO
Shape Security

WHEN MOST people think of cyber hackers, they often picture teenagers breaking into and tampering with sloppily designed computer systems (this started with Matthew Broderick in *War Games* and continues today with DEFCON attendees). This view of hacking obviously celebrates the skill of the hacker, seated at a console directing each action based on observation and skill, both of which can be studied and exploited by the defense.

But the modern reality is that cybercriminals now leverage the intense power of automation in so-called *imitation attacks*, which are designed to exploit inherent weaknesses of publicly-facing applications. There are certainly human beings involved in the design, but the execution is controlled by software. We recently asked Sumit Agarwal, Cofounder of *Shape Security*, to help us understand how this new vector expands an organization's risk surface, and how the modern enterprise can utilize Shape's platform to detect and counter such insidious threats.

EA: What is meant by an imitation attack?
SA: An imitation attack refers to a situation in which bad actors commit fraud via web and mobile applications by appearing like normal users. Attackers blend in with legitimate traffic in lots of ways, such as by spoofing legitimate browsers like Google Chrome, introducing human behavior like mouse clicks, and timing their attacks to coincide with the target's normal business hours. One of the most common imitation attacks is credential stuffing, in which attackers test out millions of leaked usernames and passwords to try to take over users' accounts. Credential stuffing is a widespread problem, costing US industries millions of dollars *a day* in fraud losses.

EA: How do you differentiate between a normal user and an imitation attacker?
SA: The key is to know exactly what your normal user population looks like, and then you can more easily identify anomalies that suggest an attacker is trying to blend in with their traffic. Without getting too technical, you must capture hundreds of data points about every user's session as they interact with the web or mobile application, including details about the browser, behavior as the user navigates the page, and network information. The data must

then be processed by machine learning models to accurately and precisely differentiate attackers from legitimate users in real-time.

EA: What is the best mitigation approach once imitation attacks are detected? Do you just block the traffic?

SA: Great question, a long-term strategy is a bit more nuanced. When you first deploy a solution that can effectively identify attacks, absolutely go ahead and block the malicious traffic. That will deter 70-80% of all the attack groups, who will immediately move on to softer targets. Another 10% of attackers will try to retool; for example, they might add in some mouse movements or try to launch their attacks from residential ASNs. But you can continue to detect and block them on those simple identifiers, and those attackers will eventually go away. The last 10% are your most sophisticated and motivated attackers. These bad actors can and will go to extreme lengths to disguise their attacks. You want to be careful about what feedback you give these attackers, as you don't want them to evolve so quickly that you can no longer identify them.

EA: What are some attack-related trends you're seeing in your customer base?

SA: One major trend is the equivalent of a thief climbing through the hole in your neighbor's fence to rob you. We are seeing attackers exploit whitelisted partnerships, such as the relationship between the banking industry and financial aggregators. Attackers want to take over victims' bank accounts, but can't easily launch a credential stuffing attack on the bank because they have employed significant anti-automation defenses. The attacker can still validate those credentials by attempting to create accounts on a financial aggregator like Mint or YNAB. The bank might see a minor uptick in authentication requests from the aggregator, but, because the bank is accustomed to unpredictable automated traffic from the aggregator, it will allow the requests to go through without further scrutiny.

EA: How does Shape help organizations mitigate attacks?

SA: Organizations rely on Shape Enterprise Defense to detect and mitigate imitation attacks on their behalf. Our technology sits in front of their websites and mobile apps and autonomously deflects attacks while creating zero friction for genuine end-users. In addition, we have a dedicated SOC monitoring customers' traffic on their behalf, so that we can immediately detect and respond when attackers evolve. By acting as an extension of organizations' security teams, we allow customers to dedicate their resources to more differentiated, strategic initiatives.

Integrated Protections for Cloud-Enabled Enterprise

An Interview With
Hugh Thompson
CTO
Symantec

IT IS IMPOSSIBLE to underestimate the impressive power and positive influence that Symantec has wielded across our community for several decades now. From endpoint solutions, to advanced R&D, to compliance controls, to identity security, and on and on – Symantec has been one of the iconic technology leaders and innovators, helping defenders build effective security protections to maintain sufficient control for business and government to continue to operate.

We recently caught up with industry veteran and expert, Dr. Hugh Thompson, CTO of *Symantec* to ask him to share his unique perspectives on cyber security. Hugh helps lead one of the largest teams in the world focused on cyber, and he has had the privilege to work for many years at the forefront of the cyber security industry and technology development for citizens, businesses, and governments around the world.

EA: Let's start by talking about some of the trends are you seeing across the cyber security industry and the cyber threat landscape?
HT: Threats continue to evolve, and threat actors continue to become more innovative. Vendors have been driven to continuously evolve and innovate to get ahead of those threats. This means that it's more critical than ever for vendor products to become more intelligent and to leverage the data telemetry they collect from their ecosystem. Big data is certainly a trend, and many vendors say they leverage their data to defend their users. But given the size of Symantec's Global Intelligence Network and the trillions of pieces of telemetry we analyze along with the full set of solutions and platform we offer, I believe we are in a better position than most to do this. The move toward cloud is also a massive trend and Symantec has made our cloud service solutions a leading priority. That said, we still must be able to bring our customers into the cloud at a speed that works for their business. Again, here we're one of the few companies that can do that at scale. Given our long-held leadership in on-premise solutions along with our growing leadership in the cloud, we can help our customers transition between on premise and cloud deployments via a hybrid solution to deploy their security footprint in a way that make sense for them. We also see attacks on mobile devices growing at a rapid pace. It fact, individual mobile attacks which can quickly threaten entire enterprises have become one

of the major new vectors for cybercrime as more users and consumer turn to their phones and tablets for work and personal use. It's a trend we spotted early and via acquisitions and organic development have made the protection of modern operating systems one of our top priorities. Finally, we are seeing Privacy as one of the new drivers of digital safety around the world and here too we've been investing and innovating in both our enterprise and consumer digital safety platforms.

EA: Symantec has built a portfolio of best-in-class products and services which you deliver on an Integrated Cyber Defense platform. Why did you take that road and how do you compete with smaller vendors who are primarily focused on a single point product?

HT: Enterprises understandably want to deploy best-in-class products. We understand that, which is why we have doubled down on our R&D investments in key product areas to maintain a best in class status that can compete head-to-head with any point product vendor. It can be hard to compete with vendors who've created a lot hype around point products because many of their customers lack the resources to do a fulsome evaluation of those products. This is an area where the analyst community has become essential and we are quite proud of our positions in the ranking documents that have examined our products versus our competitors. Our decision to create a platform that integrates our best-in-class products was the next logical step for us as enterprises increasingly want less complexity and lower-cost in the solutions they deploy. When you can seamlessly integrate world-class products in customized configurations, not only do you reduce the total cost of ownership and make it easier to manage those products, but you also improve visibility and accelerate threat response times. Symantec's approach is to offer an integrated suite of products and services that exchange data with each other – not only the threats they're seeing but also what they're learning in order to make better, faster and less intrusive decisions. An example of this might be a user who visits a site to get their news or read a white paper where our web gateway solution spots a threat and signals the Symantec Endpoint Protection Manager to engage our application hardening technology, protecting both the user and the enterprise, all without getting in the way of the user's browsing or work experience.

EA: How do you continually improve your products to make sure they lead the industry as best-in-class while ensuring they integrate seamlessly into your platform?

HT: It really all comes down to innovation. Only a company the size of Symantec can make the innovation investments that we do. With over 500 threat analysts constantly monitoring the threat landscape in real time as it evolves we can innovate more rapidly than almost any other vendor to stop threats as they happen and make our solutions smarter and stronger all the time. If you took a snapshot of the researchers in our Symantec Research Labs on any given day, you'd find them working on solving fundamental problems for the future – taking what they've learned and building it into our platform through machine learning that uses an adversarial approach to make artificial intelligence both safer and more effective. It's a way to ensure that we continually innovate on a platform of solutions to stay ahead of threats. In fact, you might say that our platform is the delivery vehicle for innovation.

EA: How does the architecture of Symantec's platform ensure that both Symantec's solutions and other vendor's products can be integrated to make your customers safer overall?
HT: We understand that we will never be able to offer every product an enterprise needs and that many enterprises will need to deploy other vendor's solutions. To make sure that can happen seamlessly we've built our platform on open standards that, through our Integrated Cyber Defense Exchange (IDCX) allows customers to rapidly integrate other solutions that they may have already deployed, amplifying the power of multiple vendors across our platform. We've built a Technology Integration Partner Program with nearly 100 technology partners and more than 175 technology integrations and those numbers will continue to grow as more and more of our customers take advantage of the open-ecosystem and flexibility our platform provides.

ET: Why do enterprise customers choose Symantec's Platform over other vendors' platforms?
HT: It's the number of best-of-breed cyber-security technologies we offer and the depth of our threat intelligence that makes our platform hard to beat when you put it head-to-head against what other vendors offer. To begin with, we have more of the most critical cyber security technology building blocks than any other vendor. We also have an Integrated Cyber Defense platform architecture that enables our customers to seamlessly and flexibly integrate those technologies in the way that best suits their business needs. At the same time, because of that base of technologies, the millions of users we protect worldwide, and the trillions of security events we see every day, we can harness the best, and most globally comprehensive threat intelligence of any other vendor in the world, the driving factor in making our platform smarter and stronger. It really takes a company with the size and capabilities of Symantec to build out a winning platform. When customers look at our platform they are increasingly going "all-in" with Symantec.

Crowdsourced Security Testing

An Interview With
Jay Kaplan
CEO
Synack

IDENTIFYING EXPLOITABLE vulnerabilities in enterprise environments is a difficult pursuit – one that CISOs and their security teams spend considerable time and effort trying to accomplish. An important resource that can be unleashed to drive progress in this area is the collective power of vetted and skilled security experts – sometimes referred to as ethical hackers or white hats – to identify problems before a malicious adversary can do so.

Synack is a company that has been innovating for several years now in crowdsourced security testing. Their solution offering involves the use of a vetted community of researchers who can provide risk reduction for the enterprise through controlled crowdsourced penetration testing and vulnerability discovery. We recently caught up with Jay Kaplan, CEO of Synack, to ask about his team's newest updates and how the enterprise can adopt this important area of crowdsourced security services.

EA: What are the differences between bug bounty programs and Synack's crowdsourced security testing?
JK: Bug bounty programs create marketplaces for researchers to report vulnerabilities. This approach has improved security testing, but extends an invitation to outsiders to test your systems, which could add risk to your organization. Synack utilizes the bug bounty concept as part of our offerings, but we focus on a platform, rather than a marketplace. Synack's crowdsourced testing platform supports efficiency, effectiveness, and control levels unattainable through a bug bounty marketplace. With our platform, you can augment and scale your team's efforts without extra operational and resource burdens. We triage vulnerabilities submitted through the platform so that only valid ones are passed to customers; we also handle bounty payouts and researcher community management. Often it takes 24 hours to start an engagement, 24 hours to find the first severe vulnerability, and less than 72 hours to verify a patch. We deliver real-time security intelligence that bug bounty marketplaces cannot achieve. Customers can see their testing coverage data, researcher engagement data, and security scores based on real performance data. This helps managers make prioritized decisions to minimize security risk. And lastly, the Synack platform gives the customer a lot of control

over the crowd. Security managers can activate and pause the crowd's activity with the push of a button, and they can have visibility into all test activity, as well as full ownership of all findings and IP.

EA: How does the Synack solution work?
JK: All client asset testing is conducted through Synack's secure VPN gateway. Directing all traffic through a VPN gateway helps us capture data behind the testing, and gives customers control to start and stop testing at any time. The testing data powers intelligence like testing coverage maps, attack type analysis, and security scores in our portal. The Synack Red Team (SRT) is our private network of highly-curated, skilled and vetted security researchers that power the testing. We have proprietary scanning technology that provides automated analysis to human researchers. During an engagement, we continuously scan all assets in scope, and researchers are alerted to detected changes, suspected vulnerabilities, and defensive technology sensing. The Synack Mission Ops team is our internal team of vulnerability experts that work closely with customers during an engagement. Mission Ops helps with asset definition and scoping, manage researcher communication and payouts, triage submitted vulnerabilities, and hold customer support meetings regularly. We offer our customers crowdsourced vulnerability discovery, crowdsourced penetration testing, continuous testing, and a managed responsible disclosure program.

EA: What is your process for selecting, vetting, and deploying your security researchers?
JK: Synack Red Team (SRT) researchers go through a rigorous 5-step vetting process to prove their technical qualifications and trustworthiness. Only 10% advance to become a Synack Red Team member. The first step involves evaluating and cross-referencing the candidate's claims surrounding work experience, certifications and education with Open Source Intelligence (OSINT) sources. The second step involves a live behavioral interview, where determine the candidate's character, motivations, and goals, and we get a sense of the candidate's primary technical competencies. We also gather secondary information relevant to the vetting process to help us uncover any potential red flags. The third step involves a written skills exam, designed to evaluate the candidate's fundamental understanding of a specific technical domain. The fourth step involves a background and ID check with identity verification and criminal background check, completed by designated and qualified third-party assessors. The first step involves acceptance and monitoring, where, once a researcher is accepted, we closely monitor them on the platform for a 45-day qualifying period. The researcher is required to submit a valid vulnerability report before fully being on-boarded. Even after researchers make it through this process, we still have controls in place to minimize risk. We uphold a zero-tolerance policy, actively monitoring all researcher traffic. Any inappropriate behavior results in termination of their SRT membership. We also give the customer control to activate or pause testing, based on their visibility into testing traffic through the customer portal.

EA: What are some of the more interesting vulnerabilities that your team is finding?
JK: Due to confidentiality requirements that protect our customers and researchers, we don't disclose specific details about vulnerabilities we find during our engagements. But I can give you a breakdown of the vulnerability types that we see most frequently. Cross-site scripting is

by far the most common vulnerability reported and validated through the Synack platform, followed by authorization/permissions and information disclosure vulnerabilities. The average payout for these vulnerabilities ranged from $200 to $900 last year. SQL injection and remote code execution vulnerabilities were the highest-paying vulnerabilities reported and triaged through the Synack platform last year. The payouts for these vulnerabilities averaged over $2,500 and made up close to 10% of total vulnerabilities reported and triaged last year.

EA: Have you seen any shifts in the selection and use of crowdsourced security testing solutions by enterprise?

JK: This year, Gartner published a paper about the crowdsourced testing market called *Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing*. In it, they estimate that more than 50% of enterprises will utilize automated and crowdsourced security testing platform products and services by 2022. In the next few years, crowdsourcing will be standard among enterprise. It won't be a matter of *if* companies will utilize a crowd for their security, it's a matter of *how they're going to do it.* The conversation around crowdsourced security and the success metrics measured against these solutions are shifting. I think CISOs are becoming more concerned about their resistance to cyber threats and less preoccupied with just complying to regulatory standards. And rather than security teams focusing on the number of vulnerabilities being found, they are starting to care more about security scores, resilience or resistance to attack, and measurable risk reduction. As a result, CISOs and their security teams are more concerned about getting data and intelligence from their crowdsourced security, because that will help them better understand their security posture, prioritize their resources, and minimize their risk over time.

Disrupting Cyber Security Industry Analysis

An Interview With
Ed Amoroso
CEO
TAG Cyber

EVERY HEALTHY industry includes expert observers who comment on the status, quality, and trends associated with that industry's products and services. Across (virtually) all aspects of technology, excellent industry analysis is available from professional analysts who work hard to be unbiased, accurate, and helpful in their assessments. In cyber security, however, much of the industry analysis to date has been pay-for-play and created by many non-experts.

A healthy recent trend, however, led by Manhattan-based *TAG Cyber*, involves the expert provision of cyber security industry analysis in a way that democratizes the guidance for practitioners. In a recursive interview (uh, with himself), Ed Amoroso interviews TAG Cyber's CEO about how this progression toward less biased, more expert analysis has progressed and how TAG Cyber continues to lead this important trend in our industry.

EA: You've been critical of existing cyber security analysts. Why is that?
EA: First, thanks for interviewing me. I have great respect for your creative interviewing skills. The problem is not really with the security analysts, but rather with the rigged business model that governs how they write about our industry. If your primary objective is to maximize the revenue associated with your reports and consulting, then you are going to exaggerate your emphasis toward companies that can pay the most. This is Business 101. So, everyone should recognize that the large existing companies that sell cyber security industry analysis are completely and totally biased.

EA: Should CISO teams pay attention to the reports from large analysts such as Gartner and Forrester?
EA: I think they should be careful assigning too much weight to these reporting sources, especially in the context of quadrants and waves. The most poorly kept secret in our industry is that the way to the top right of any analyst's graph is by paying your way there. So, if you see that some vendor has found its way to the top right of a quadrant, and you are using this placement as the basis for your source selection, then please be sure to ask if they were placed there because they paid for that placement. At TAG Cyber, we never rate vendors; instead, we

do everything we can to educate buyers about all the various products and services that are available from vendors we review, interview, examine, and learn from.

EA: What services are available from TAG Cyber?
EA: We produce content that we hope generates helpful learning for CISO teams – and we charge zero for the use of that content. That's why we refer to our work as democratizing cyber security. We monetize through special vendor-paid sponsorships, commissioned technical writing, paid ads in our original video content, and through various products and services we offer customers. You might have seen our original Charlie Ciso cartoons developed with our lead illustrator, Rich Powell. We have a growing base of enterprise customers who use these cartoons for their security awareness programs. We also provide consulting and managed services for a select set of customers.

EA: I've heard that you also do CISO coaching. How does that work?
EA: Thanks for asking, Ed. And yes, I do provide personalized coaching for a small number of CISOs – although TAG Cyber is expanding this service with many new experienced, former CISOs and security executives who will serve as our coaches. I think it's crazy for CISOs to not have an excellent coach they can confide in and get some help from when things get sticky. I had a coach when I was starting out as a CISO and it helped me immensely.

EA: Any trends you are seeing from an analysis perspective?
EA: We see advanced analytics, public cloud usage, and increased dependence on automation as three technology trends driving much of what's going on in the cyber security industry today. We also expect to see continued consolidation of the enormous number of start-ups into a more reasonable and workable community of security vendors offering world-class cyber security solutions to government, enterprise, and citizens.

Embedding Security into IT Utility Infrastructure

An Interview With
Bruce Flitcroft
CEO
TenFour

THE NETWORK infrastructure supporting enterprise teams can be roughly partitioned into support layers one-through-three, and application layers four-through-seven. Companies such as *TenFour* have come to recognize that the lower layers can be supported via an IT utility model, where teams can rely on an expert network service team to take care of the operational support, day-to-day maintenance, and technology refresh details.

An additional benefit to this model is that security in the lower layers can be addressed more effectively. Where the higher layers are characterized by rapid application changes that are tough to embed into a utility model, the lower layers exhibit a more predictable evolution, hence the potential for added security. We recently asked Bruce Flitcroft, CEO of TenFour to share his thoughts on security in the context of this creative service delivery method.

EA: What is meant by IT Utility Infrastructure?
BF: What we've pioneered at TenFour is the design and delivery of a set of standard IT utility infrastructure components into agile and reliable on-demand network solutions. In the Digital Age when companies are looking for Cloud-first strategies, we've taken the Cloud model and applied it to all the core IT infrastructure that was previously considered "uncloudable"—from routers, switches and firewalls to phones, WiFi, cameras and IoT devices—and deliver them as a utility service. We've even included all the bandwidth and circuits.

EA: How does your team integrate security solutions into the delivery model?
BF: The fact is that bad actors are going to try to infiltrate your network. We make it hard for them to get on the network by addressing and standardizing of all the network and host level security. If they do get through, we make it easier to identify them and throw them off. All our services are integrated with embedded security. We provide all the Network layer security and most of the Host/System layers. Our service is embedded with AAA, NetFlow, SGT, 802.1X, patch management and syslog—these are included as core capabilities. Additional advanced cyber security capabilities can be added as an IT Unit (ITU) in a consumption-based model. With our network security services, our customers' underlying network infrastructure contains

the requisite protections so that their teams can focus their real-time security efforts on the much more vulnerable inner layers: Application and Data.

EA: Do advances or changes in malicious threat require that your team adjust its protection model?

BF: It was probably correct to say that the earliest original security attacks clearly targeted the lower layers of the network stack. We all remember those early TCP/IP packet attacks that hackers liked to launch in the nineties. Today, however, the biggest security challenges seem to exist at the higher levels, usually targeting applications and users. Many attacks are moving up the stack and beginning to target applications. This requires more tailored solutions based on the specifics of the application. Our utility service is designed to support this activity by ensuring solid network controls. We use a reference architecture design with smaller and more simplified surface attack areas. As a result, we see attacks decrease since there are easier targets elsewhere. The challenge we take on is to make sure that these threats do not create serious problems for our customers. We use standard components to put together sensible security protections for network layers 3-4 and below, and we export the alarms, logs, and notifications we receive up through our service interface to customer security systems such as security analytic platforms and SIEMs.

EA: How do enterprise teams integrate your security solutions into their larger program?

BF: No matter what enterprises do, they are going to be understaffed in cyber security in the Digital Age. Aligning security and IT teams to focus on the right areas is ever more critical as companies will be judged by how trusted their environments are. With so much at stake and so much to defend, it can be difficult for enterprises to decide where they focus limited security and IT resources. Our model allows them to move their security and IT resources from the Network and most of the Host/System layers to the Application and Data layers so they can focus on protecting the information that's critical to their differentiation.

EA: What are some enterprise IT-related trends you're seeing in your customer base?

BF: Enterprises have focused on first defining their Digital Strategy; now it's about execution. We are seeing an increase in interest on how to speed the delivery of IT and make it more agile, flexible and secure. Enterprise IT departments increasingly do not want to own their own IT infrastructure. The forward-looking driver is the need to focus on new technologies—AI and automation—that will drive innovation, stronger customer engagement and top line growth. Whatever the use case, their IT staff does not have time to deal with yesterday's problems as they focus on adapting to their new roles and skills required for the Digital Age. But with IT that was built for a different era, IT leaders struggle with getting ahead of the technology debt and the new security challenges. We are seeing enterprise IT increasingly embrace IT Infrastructure Utility to eliminate technology debt and build a more secure foundation. More and more security features, such as log management, access controls, intrusion detection and firewalling, are just going to be a requirement of the standard service and not sold as standalone elements. TenFour has taken this approach by embedding network security as a core service of its IT infrastructure utility.

Automated Email Authentication for the Enterprise

An Interview With Alexander García-Tobar

CEO
Valimail

WE TAKE authentication for granted in most everyday activities. For example, we log into bank websites using a username/password or stronger form of authentication, we would never start our Internet banking without this critical step. Yet we don't think twice about opening an email without any sense of whether it has been authenticated — leading to rampant impersonation attacks on employees and executives, and significant damage to company brands. It is trivially easy to spoof messages so that hackers and criminals can impersonate a trusted source. As a result, more than 90 percent of cyberattacks start with an email.

Because of this threat, email is a key focus for enhanced authentication. The goal is to enable email recipients to trust the sender identities. This is a welcome advance, since email has until recently lacked such authentication. *Valimail* focuses on automating email authentication, with a range of different capabilities including support for an alphabet soup of authentication protocols: DMARC, SPF, ARC, BIMI, and DKIM. We recently asked Alexander García-Tobar, CEO and co-founder of Valimail, to share how his team sees this expanding market, and how his anti-impersonation platform provides authentication support for enterprise security and messaging teams around the world.

EA: What are the most common threats to modern email?
AG-T: There is a wonderful quality to email: It's neutral, and nobody owns it. It just works, and it works everywhere, thanks to the open standards that it's built on. Someone in Uzbekistan, for example, can send an email to someone in Canada without having to ask anyone permission or go through any gatekeepers. And it could be an important email message, potentially life-changing for the recipient. This explains why literally half the planet uses email. By some estimates, this includes 3.7 billion active users, more than any other digital social network. But that openness is also email's security downfall because that email from Uzbekistan could easily be a phish. That is, a fraudulent message designed to trick the recipient into downloading a malicious file, giving up the password to a critical account, or sending back personal information. There's very little in email's basic technology set to prevent senders from purporting to be whoever they want to be.

EA: What is meant by email authentication?
AG-T: Simply put, email authentication depends on widely accepted standards (DMARC, SPF, ARC, BIMI, and DKIM) to ensure that only designated and approved senders can send messages using your domain name in the "From" field. With authentication, you can trust that a message originated with the organization it appears to have come from. Recall that, in the 1980's, credit cards were becoming an increasingly popular payment method. A merchant would create a carbon copy imprint of the credit card, the holder would sign the paper, and the merchant would cross their fingers that they would get paid. As credit cards proliferated, increasingly complex and manual processes were put into place to authenticate the card — ever thicker booklets listing fraudulent cards, for example. Fraud exploded, so a new approach was launched: Visa, First Data, and Verifone POS terminals created a real-time, automated authentication process. Each company went on to multi-billion dollar valuations and the credit card market exploded. In the modern email scenario, we are replacing the POS terminals and Visa with the largest ISPs (Microsoft, AOL, Google, and Yahoo!). Email authentication is the email equivalent to the credit card clearinghouse function described above.

EA: What does the Valimail platform include?
AG-T: We automate the deployment and running of real-time email authentication. We also provide in-depth reporting to help organizations gain visibility into which services are sending email on their behalf, and interact with third party services to ensure authorized email is delivered while unauthorized email is rejected — both inside and outside your organization. This is a relatively complex set of procedures and typically it is extremely challenging for companies to do it on their own. Why? In the cloud era, it's not uncommon for a single company to be using dozens of different cloud services, most of which send email "as" the company, using its domain name in the "From" field of the messages. For example, such services might include a marketing automation service, a payroll management service, a lead-scoring app, even a tool to support legal discovery and legal communication. Your IT people may not even know all these services are in use, since they may have been set up by line of business owners or department managers. With Valimail's detailed reports, these "shadow email" services become instantly visible — and manageable.

EA: Do customers have to employ experts to properly publish DMARC records?
AG-T: Email authentication is unique in that it's public, so analysis of public DNS records shows the success rates, how long each project has taken, and whether a company is doing it themselves or with a vendor. About 65 percent of all DMARC projects are do-it-yourself (DIY) — and looking at millions of DNS records shows the DIY approach fails 80 percent of the time, even with 2-3 full-time employees working on it for 12 months. First-generation DMARC vendors provide consulting expertise and some technology that can reduce the load to about one full-time employee. But even there, the success rate after a year ranges from 20 to 40 percent depending on the vendor in use. Valimail was born out of these unacceptable stats: The notion was to create a fully automated system that works invisibly. We created the only company in the email authentication market to offer a guarantee that we will get you to DMARC enforcement. As a result, our success rate is well over 90 percent with a median of 60 days to enforcement and near zero FTEs.

EA: Do you see email authentication expanding to other forms of online communication including OTT apps?

AG-T: Our expanded mission is to "Authenticate the World's Communications." The need for authentication comes to every major form of technology sooner or later. Authentication of people is possible now through unified login products like Duo, Okta, Gigya, and OneLogin. These services give enterprises control over who is logging in and accessing key digital resources, whether those are employees using internal apps or customers accessing the public website. Cloud access service brokers (CASBs) like Skyhigh and Netskope help enterprises manage what resources various services can access. They provide a centralized point of control, detection, management, and enforcement for cloud services, giving IT staff simpler control and visibility into the various services used throughout the organization. Authentication for communications is coming into its own, starting with a massive surge of adoption for email authentication. Over the past year, the number of domains with DMARC records tripled. Usage of DMARC has also been spurred by the U.S. Department of Homeland Security's mandate that all federal agency domains use DMARC, with a strict policy of enforcement, by October 16, 2018. The U.K. government issued a similar mandate a few years ago, resulting in a remarkable surge of adoption. After email becomes authenticated by default, who knows what's next? We see authentication expanding into any area where the identity of who you're communicating with needs to be verified. That could include IoT applications and many other areas. Once you grasp the power of authentication, it's hard to believe it's not used everywhere, which is why we think the growth potential in this market is so huge.

Orchestrating Virtual Perimeters for Modern Enterprise

An Interview With
Marc Woolward
CTO
vArmour

THE PROGRESSION for many in the cyber security industry has not been easy from a single DMZ-based enterprise gateway to the current hybrid collection of cloud and premise services accessible from a range of devices including mobiles. The challenge has been finding an effective way to virtualize the resulting perimeter to maintain the desirable attributes of firewall protection while also encouraging and supporting use of cloud.

The *vArmour* team has helped to pioneer this concept of virtualized, distributed security through its advanced cyber security solution offerings. We recently asked Marc Woolward, CTO of vArmour to help us understand the trends in hybrid cloud-based, virtualized security and to share his perspective on the best means for an enterprise team to reduce its risk as its architecture continues to evolve.

EA: Do most organizations recognize the changes occurring to their perimeter?
MW: By this point, a large proportion of Enterprises have recognized the business advantage of multicloud architectures to their business and determined that the traditional 'security perimeter' is no longer relevant in protecting such environments. Not only do these static architectures impede the agility required but they also fail to protect applications deployed across the multicloud, and certainly no longer provide the level of visibility and control needed to defeat attempts at lateral traversal associated with Advanced Persistent Threats (APTs) and Advanced Targeted Threats (ATTs), particularly now we see nation state-developed malware in the hands of criminal hacker groups.

EA: How do CISO teams best address the challenge of virtualized enterprise security?
MW: We are now seeing Enterprises thinking strategically about securing their multicloud applications, of which their 'on-premise' virtualized estate is a part but which also includes PaaS and public cloud IaaS. Any solution addressing just the virtualized or the containerized environment, is going to add security complexity to the complexities associated with heterogeneous cloud environments. Clearly security controls need to encompass applications wherever they execute, and provide consistent levels of protection, but more importantly enterprise security teams need the tooling to allow them to manage security risk through the

application lifecycle across the multicloud. They need the tools to understand their applications wherever they execute, assessing the risks and computing the requirements to protect them.

EA: How does the vArmour platform work?
MW: vArmour provides our customers with the visibility and computed policies to secure their applications wherever they are deployed. Our Application controller ingests telemetry and metadata to produce application models which can be turned into validated, measured policies. Our sensors collect l7 application telemetry and allow security policies to be enforced in the environments without native controls or telemetry.

EA: Can teams easily orchestrate policy across multiple platform instances?
MW: Yes. The application controller provides a consistent pane of glass from which to secure applications and abstracts the differences within each of the public cloud environments, virtualized and physical on-premise deployments, and containers wherever they may be deployed.

EA: What prediction do you have in this important area of enterprise security?
MW: Securing applications from today's nation-state class attacks across heterogeneous multiclouds can be complex, and any solution that is itself complex will make the problem worse since complexity is the enemy of security. We are focused on driving application security towards an autonomic, self-securing model based upon a data driven approach. We believe that although Data Science techniques have been applied broadly to reactive threat detection and response, they are particularly suited to the automation of proactive policies which provide application security proactively, reducing the need for response.