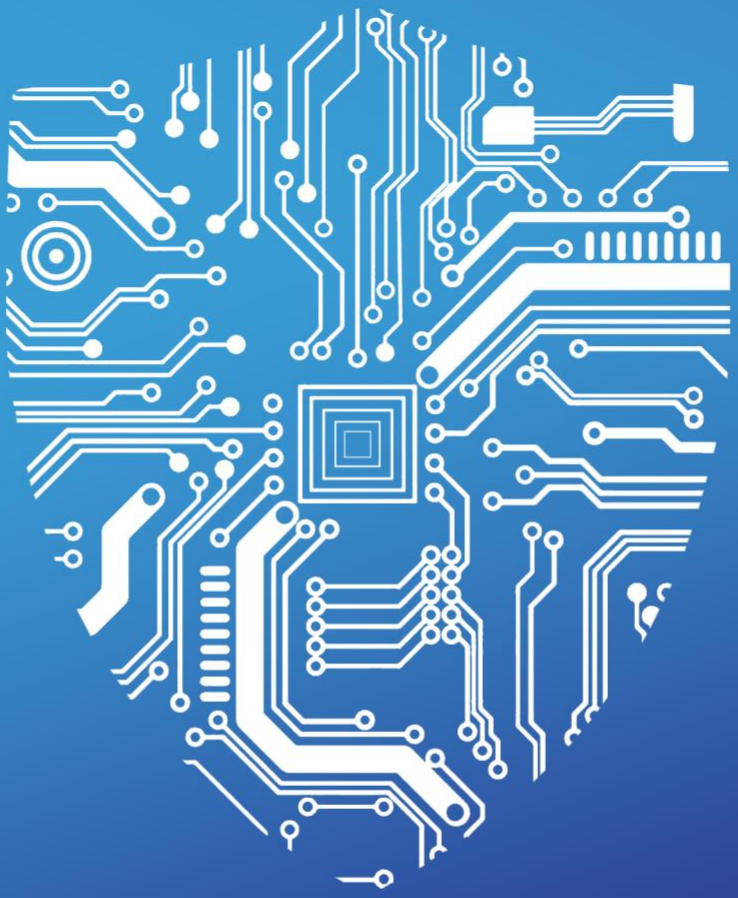
2019 TAG CYBER SECURITY ANNUAL

VOLUME 1

OUTLOOK FOR FIFTY

CYBER SECURITY CONTROLS



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

September 17, 2018

To the Reader:

This is our third year offering cyber security industry coverage, advice, and analysis through our *TAG Cyber Security Annual*. We hope our efforts have saved you valuable time, effort, and money, because *that* is our mission: *To democratize the availability of world-class cyber security industry analysis – to everyone – for free*. When we started TAG Cyber, we assumed that enterprise network teams under Chief Information Security Officers (CISOs) would be our audience. Since then, however, we've learned that investors, entrepreneurs, reporters, teachers, civil servants, managers, and even board members find our work useful.

The first guide we developed in 2016 was essentially a text-book on fifty different vital aspects of running an enterprise security function for an organization. It introduced the *TAG Cyber Fifty Security Controls*, and created quite a stir in our industry – but perhaps not for the reasons we expected. Most of the commentary was that our material was too voluminous, and tough to digest in any meaningful way. Our response was that our volumes were intended as shelf resources to support source selection and research, but we grudgingly accepted that maybe two-thousand pages of dense material was pushing things a bit.

The second guide we developed last year in 2017 was still a monstrously long work, but we spent an entire summer developing visuals to support our analysis in each of the fifty areas. A template was created that showed the first, second, and third generation observations and trends for each of the controls – and this worked out quite nicely. We have been receiving emails and notes from all over the world from practitioners finding the visuals helpful. But frankly, much of the input from our growing readership has asked that we continue to make things a bit shorter and easier to digest. (OK, we got it.)

Accordingly, this guide was designed to make things as simple and user-friendly as possible. Obviously, we have updated content and analysis, but our focus was to shape this year's Volume 1 into a much lighter read, one that could be consumed in a couple of sittings. This was a tall order for writers like me who can turn any little idea into a ten-page treatise that goes *on-and-on. And on.* But we chopped and clipped and removed, and the result – as you will see, is a much more compact Volume 1 report that gets to the point quickly for each area. (And yes, Volumes 2 and 3 are still the size of encyclopedias – sorry.)

Despite this, we are pleased to announce that our longer-form reporting is not dead – in fact, much to the contrary. What we've decided to do is develop and issue more extensive writing, research, and analysis for each of the fifty TAG Cyber Security Controls in a ***series of individual reports that we will make available to you*** for free on a weekly basis this coming year. Watch our Twitter @hashtag_cyber and @TAG_Cyber or follow Edward Amoroso on LinkedIn to get more information about these reports. Hopefully, this will feed your inner need (and ours) for more depth.

We also made some necessary updates to the fifty controls – adjusting the names of some, and adding relevant functionality or procedures to others. These changes came directly from our understanding of industry and practitioners; that is, the original TAG Cyber controls included a heavy dose of pedagogical intent – which means that we included many items we believed *should* be there. But over the past three years, we have adjusted our original view to match what we see in industry. The good news is that every control change is for the better, in terms of cyber risk reduction.

We'd like to close here with a word of encouragement to those of you who work as practitioners protecting infrastructure across various business and government sectors from the potentially negative, or even disastrous, effects of cyber threats: Recognize that it is *you* who currently maintain order in our society; recognize that it is *you* who keep essential services available for citizenry; recognize that it is *you* who make business secure for innovation and progress; and recognize that it is *you* who will ensure a vibrant global future where technology makes our lives better.

Keep up the good work – and we hope the information and research in our volumes provide you with some time to think.

Dr. Edward G. Amoroso
September 2018
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 carefully down-select the list of 200-or-so, to about 50-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 logos for our amazing Distinguished Vendor sponsors are provided below and I hope you'll take a moment to review the list and visit their websites. We at TAG Cyber can personally vouch that they are doing interesting and useful work:

2019 TAG Cyber Security Annual

Volume 1: Outlook for Fifty Cyber Security Controls

Prepared by the TAG Cyber Security Analysts
Team Lead: Dr. Edward G. Amoroso

Introduction

The underlying basis for our expert industry analysis work at TAG Cyber is a so-called *periodic table* of cyber security controls that includes fifty different aspects of enterprise cyber security management that are essential to any modern information risk reduction program. The table is organized into six categories, which was done to highlight the purpose of each control in the context of an enterprise cyber security protection program:

Enterprise Controls		Network Controls		Endpoint Controls		Governance Controls		Data Controls		Industry Controls	
1	IDPS/ Deception	9	CA/PKI Solutions	17	Anti-Malware Tools	26	Digital Risk Management	35	Application Security	43	Industry Analysis
2	DLP and UEBA	10	Cloud Security/CASB	18	Endpoint Security	27	Bug Bounty Support	36	Content Protection	44	Information Assurance
3	Firewall Platform	11	DDOS Security	19	HW/Embedded Security	28	Cyber Insurance	37	Data Destruction	45	Managed Security Services
4	Network Access Control	12	Email/DMARC Security	20	ICS/IoT Security	29	GRC and Risk Management	38	Data Encryption	46	Security Consulting
5	Unified Threat Management	13	BGP/DNS/SDN Security	21	Mainframe Security	30	Incident Response	39	Digital Forensics	47	Security Career Support
6	Web Application Firewall	14	Network Monitoring	22	Mobile Security	31	Penetration Test/Simulation	40	IAM and Identity Platforms	48	Security R&D
7	Web Fraud Prevention	15	Secure File Sharing/Sending	23	Password/ Privilege Mgmt	32	Security Analysis/ SOC Hunt Tools	41	Compliance Support	49	Security Training/Awareness
8	Web Security Gateway	16	VPN/Secure Access	24	Multi-Factor Authentication	33	SIEM Platform	42	Vulnerability Management	50	Security VAR Solutions
				25	Voice Security	34	Threat Intelligence				

Figure i. Updated TAG Cyber Periodic Table of Fifty Cyber Security Controls

The original fifty controls were introduced and explained in Volume 1 of both the *2017* and *2018 TAG Cyber Security Annual*, along with cross-reference listings of world-class cyber security vendors supporting each control. Readers are advised to take some time to review those volumes to build familiarity with the TAG Cyber approach. They are available to you as a free PDF download at https://www.tag-cyber.com/.

For this year's work, we have decided to update, rename, and enhance several of the original TAG Cyber controls as follows:

- The *Perimeter Controls* category was renamed *Enterprise Controls*
- *Deception* was added to the IDPS control
- *UEBA* was combined with DLP into a common control category
- *CASB* was added to the Cloud Security control
- *DMARC* was added to the Email Security control
- The Infrastructure Security control was renamed *BGP/DNS/SDN Security*
- *Sending* was added to the Secure File Sharing control
- The Two-Factor Authentication control was changed to *Multi-Factor Authentication*
- The Brand Protection control was changed to *Digital Risk Management*
- *Risk* was added to the GRC Platform control
- *Simulation* was added to the Penetration Testing control
- *SOC Hunt* was added to the Security Analytics control
- *Identity Systems* was added to the IAM control
- The PCI/DSS Compliance control was changed to *Compliance Support*
- The Security Recruiting control was changed to *Security Career Support*

The purpose of this new volume is to provide an updated industry and enterprise perspective on each of the updated controls as we enter 2019. But this year, we are doing things a bit differently than in the past. First, we have shortened the treatment here – at the request of so many of our readers. We are grateful that our constituents are happy with our messaging, but fully acknowledge that perhaps thousands of pages of writing is a bit much. We hear you.

So, this Volume 1 is shorter and more to the point than previous efforts – and we justify this as follows: First, we believe that our Volume 1 works in 2017 and 2018 still stand as correct and relevant to modern enterprise (some of the earlier vendor references are out of date). But second, we plan to issue in 2019 a series of more extensive versions of these fifty chapters as longer separate reports. (You didn't think we'd avoid the Big Words, did you?)

The sections below thus follow directly from the new, updated periodic table of controls for 2019. Each section briefly introduces the associated control, and offers a summary outlook based on our current views of the industry. This guide can be read stand-alone, or can be used as a companion document to the original TAG Cyber Security Annuals in 2017 and 2018. We hope it is useful for you.

It is worth mentioning that reading a TAG Cyber Trending chart requires a bit of effort, but we offer guidance to the reader in each section below. We have tried to include several dimensions on the same visual – so it is valid to criticize the charts as being somewhat busy. Nevertheless, we stuck with the approach and we welcome any suggestions for improving our approach in future versions of this TAG Cyber Security Annual.

1. Intrusion Detection, Prevention, and Deception

The design of *intrusion detection/prevention systems (IDPS)* was originally focused on simple devices that used signatures to detect indicators on networks and hosts. Soon-to-emerge network-based IDS (NIDS) and host-based IDS (HIDS) were part of a subsequent decade of uneven protections starting in the late 1990's. The challenge during this period was two-fold: Signatures were easy to evade, and coverage of relevant activity was difficult, if not impossible.

The progression from detection to prevention – that is, from IDS to IPS – was also uneven during this period and since. Many enterprise security teams were originally driven to the notion of actively shunning offending sources during an attack. But these same teams grew wary of the side-effects of such powerful automatic blocking. Most teams thus ran in a combined mode, where the baseline was to remain passive, hence the IDPS moniker.

A major addition to this control area for 2019 involves effective use of *deception-based security* solutions that include probes, lures, and content designed to detect evidence of cyber attacks. Deception was originally based on simple honey content, but more recently has evolved to effective commercial products that offer realistic means for security teams to catch bad actors in the process of live exploitation. This is now necessary functionality in the enterprise.

2019 Trends for Intrusion Detection, Prevention, and Deception

This general technology area has evolved from a less effective first generation, to an effective second generation, to a more effective third generation (see Figure 1-1). This progress has been achieved as follows: First, the introduction of behavioral security in the early 2000's by several security vendors, which reduced the dependence of enterprise security teams on pure signature processing. Virtualized behavioral analytics emerged from this technological advance.

Second, the introduction of deception as a component of the overall detection and prevention process created a new live means for dealing with clever adversaries. Deception had been a clumsy technology with poorly conceived honey pots during the 1990's, but the technology improved considerably in the 2000's and 2010's with excellent and much-easier-to-manage commercial offerings from the vendor community.

And third, introduction of machine learning (ML) as an underlying algorithmic enhancement to the detection and prevention process improved the accuracy of attack and indicator detection. The moniker 'artificial intelligence' produces a range of visceral reactions among experts, and is specifically avoided here. Rather, the effective use of supervised or unsupervised ML by the best security vendors has moved this area of cyber security forward.

It is interesting to note that the effectiveness of IDPS took a dip after its earliest promise – and this stemmed directly from the realization that keeping signatures current was not going to be feasible. Furthermore, the best hackers viewed IDPS signatures as little more than a speed bump. Luckily, improved signature deployment methods, behavioral algorithms, virtual detonation, machine learning, and advanced deception have improved matters considerably.

Amidst this progression to more effective intrusion detection, prevention, and deception, two trends can be observed: The first is that the technology has moved from more generalized processing at its inception to more domain-specific processing now and into the future. In addition, the overall accuracy of detecting relevant indicators has improved over the three generations of products. Both trends are welcome and make this a desirable security control.

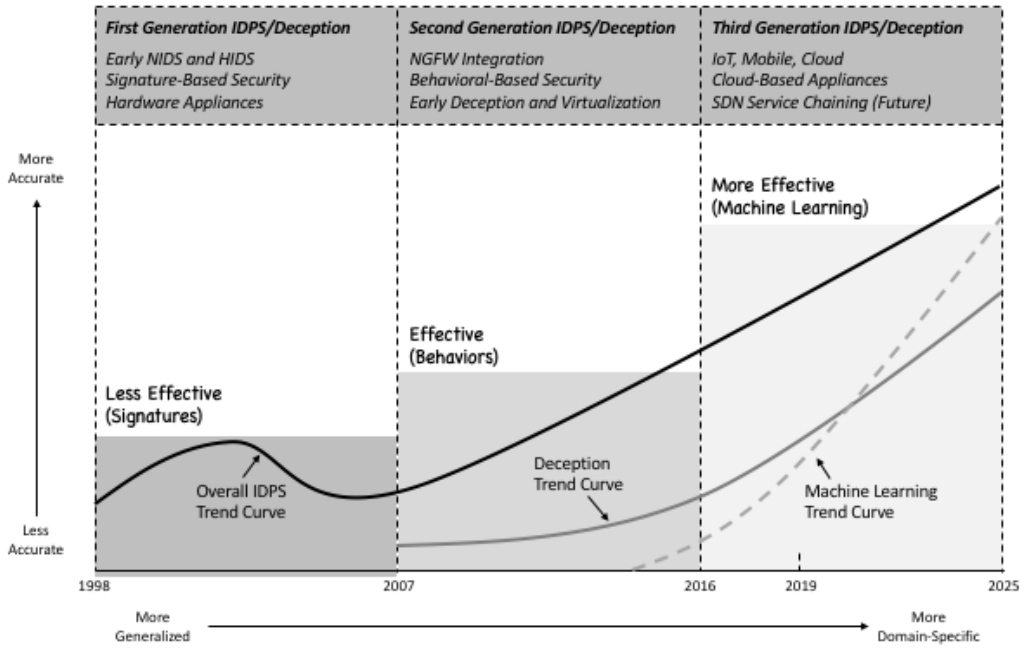


Figure 1-1. Intrusion Detection, Prevention, and Deception Trend Chart

The future of intrusion detection, prevention, and deception is bright, and will likely include continued advances in behavioral detonation of attacks in virtual environments, more accurate deception algorithms, and more extensive use of powerful ML technologies. All these advances will continue to use cloud assistance, but software defined networking (SDN) usage will grow in the latter portion of the 2010's as service providers embed these tools into SDN deployments.

2. DLP and UEBA

The design of *data leakage prevention (DLP)* systems was originally centered on detecting whether files with certain keywords were being transferred externally by insiders. This emphasis had the advantage of being easy to implement at gateways, but had the challenge that most of the structured and unstructured files in a typical enterprise are poorly marked. The result was a mixed initial attempt to keep corporate data inside the enterprise.

DLP systems – because they focus on insider leakage – were quickly extended to reside anywhere users might allow data to slip away. The endpoint is an obvious target, so most DLP systems include support for controlling how data is shared, copied, downloaded, and even backed-up to memory sticks. This one feature – restricted use of external storage media – brings both great security benefit and enormous inconvenience to enterprise users.

An issue with early DLP that remains relevant in all environments today is that sidestepping DLP systems through unsanctioned shadow IT or off-network tools is easier than it should be. Employees who would like to exfiltrate a document can easily snap images on their personal iPhone, or they can create and maintain the document using external systems such as from Google or Box. Shadow IT is the scourge of DLP and must not be ignored by security teams.

For these reasons, most existing DLP installations have been correctly advertised to senior leadership as effective controls against inadvertent, non-malicious transfer of data outside the enterprise. But even this requires that corporate data be properly marked to detect such leakage, either across a network or from an endpoint onto a separate storage device such as a portable memory stick. Unfortunately, proper marking is not commonly enforced.

The transition from static matching of strings and markings toward more behavior approaches suggests a great opportunity for integration of *user entity behavioral analytics* (UEBA) technology. Focused more broadly than DLP, UEBA solutions encompass both insider data leakage and more general suspicious insider behavior on endpoints, applications, and systems. While UEBA and DLP are separate functions, they are well-suited to integrated cooperation.

2019 Trends for DLP

Despite these challenges, DLP technology has progressed from a less effective first generation, to an effective second generation, to a more effective third generation (see Figure 1-2). This progress has been achieved through the following initiatives: First, companies have done a (somewhat) better job marking assets, especially structured, sensitive data. This allows DLP systems to more accurately detect potential leakages from a gateway, endpoint, or system.

Second, the algorithms for DLP from vendors the best security vendors have progressed from phrase-matching toward better use of regular expressions and machine learning. With this comes a greater ability to address malicious, intentional data exfiltration from compromised insiders. This coverage now extends to virtual computing on distributed hybrid cloud systems, which is important as most organizations depend less than ever on their perimeter.

It is worth mentioning that indirect methods for DLP have also been included in UEBA tools that focus on insider threats. That is, by observing the behaviors of insiders, effective determination can be made about whether that target might be inclined to cause a problem. In the better UEBA tools, direct observation can be made about suspicious activity that might lead to an information leak. UEBA is now a necessary function in enterprise.

The inclusion of DLP capability in present and future cloud-based systems and services, including SDN, represents a growth area in cyber security. Stated simply – your as-a-service provider will soon, if not already, begin to offer customers DLP-like functionality. It remains to be seen how much UEBA they can add, because cloud has less of an "insider threat" focus. Nevertheless, expect to see considerable adoption growth in these cloud-based DLP offerings.

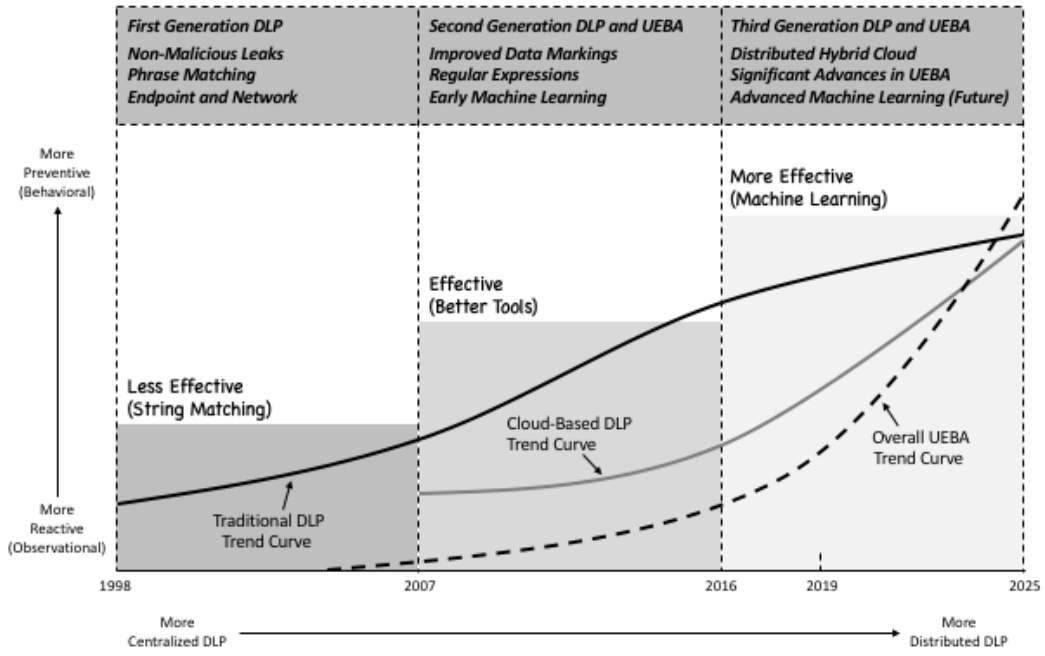


Figure 1-2. DLP and UEBA Trend Chart

The future of DLP – and its adjacent UEBA functionality – lies in advanced, embedded algorithmic controls that will recognize the indicators of potential future leakage in advance of an actual exfiltration. This will require management planning to minimize the temptation for employees to evade such detection via shadow IT services. A well-orchestrated balance between security and the freedom to use the best DLP and UEBA tools will emerge.

3. Firewall Platforms

The original purpose of a *firewall* was to protect enterprise networks from the lurking dangers of the emerging Internet. This evolved toward the more general notion of protecting one network from another, but the idea that this would be accomplished at a well-defined chokepoint remained central to the proper placement and operation of a firewall. This basic notion served as the basis for network security for nearly two decades.

The bad news is that the latter portion of that two-decade era of firewall usage was not a period of exemplary cyber security. Rather, with the accelerating dissolution of the perimeter in the mid-2000's, organizations began to realize that their overall network security architecture was ill-suited to how companies operated. Most of the major breaches that occurred during this era were not prevented by firewalls. In short, the firewalls were often almost useless.

The good news, however, is that commercially available firewall solutions have become progressively better since their initial inception. So-called *next generation firewalls (NGFW)* from the best security vendors are now incredibly powerful, feature-rich devices that provide the most advanced cyber security available today. The capabilities embedded in a modern NGFW are essential for proper assurance and security protection of a network.

All of this highlights the challenge for enterprise security teams regarding firewalls. That is, they must work with commercial vendors to ensure that the power and capability of NGFW technology continues to evolve, but in a way that is consistent with the mobility-enabled, cloud-based architectures that are emerging. This includes the migration of PCs and servers on a local area network (LAN) to a device-to-cloud scheme for accessing business apps.

An obvious advance with wonderful promise involves the use of distributed firewalls to create so-called *software-defined perimeters (SDP)*. This architectural approach requires coordination and orchestration of multiple policy engines deployed virtually to ensure a common enterprise policy enforcement approach. This is not easy – but it is not hyperbole to call this method the future of enterprise security. Virtual firewalls will be the drivers of this welcome shift.

2019 Trends for Firewalls

Firewall technology has progressed from an effective first generation, to a less effective second generation (due to perimeter issues), to a welcome and more effective third generation (see Figure 1-3). The obvious good news here is that existing users of firewalls should enjoy continued increases in capability, features, and effectiveness in the coming years. Trends toward virtual, distributed processing will complement improvements in firewall technology.

A key observation with respect to firewalls in the enterprise is that traditional firewall hardware appliances are being gradually replaced with virtual appliances embedded in software-based infrastructure. In addition, firewalls originally designed for single gateways are being gradually replaced with distributed appliances scattered across cloud workloads to support emerging SDP methods. Most companies work in a tentative hybrid arrangement today, but this will change.

The capacity for an individual firewall was originally smaller, given the thin connections most companies had to the Internet at its inception. This capacity expanded dramatically during the second generation of NGFW solutions, with gateways growing to support large wide-area connections. Interestingly, this capacity trend is reversing itself now for individual appliances with segmented workload protection, even though aggregate capacity is larger.

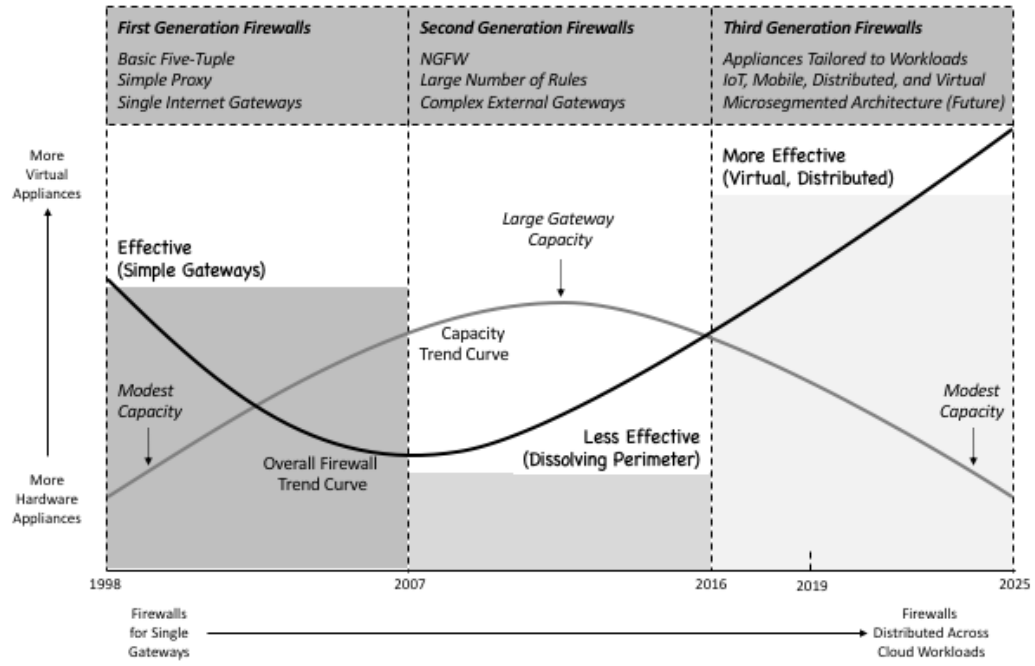


Figure 1-3. Firewall Trend Chart

The future of firewall technology and architecture can be summed up in one word: *Virtual*. Every sign points to increased software-based implementation with orchestration across distributed systems based on software-defined controls. SDP virtualization creates flexibility, and support for on-demand provisioning. Organizations of the future will automatically provision new firewalls based on situational awareness, and this will be a welcome advance.

SDN-based firewalls are also likely to provide an exciting new opportunity for firewall vendors to explore new means for cyber defense. With the power of dynamic service-chaining in SDN, enterprise security teams can begin to deploy firewalls that can automatically, and even autonomously, extend their capability based on live circumstances. New capabilities such as IPS or packet analysis will be deployed virtually in the future and orchestrated by SDN firewalls.

4. Network Access Control

The original goal of *network access control (NAC)* was to ensure some degree of policy and integrity enforcement before a device could join a local area network (LAN). Standards such as IEEE 802.1X were created to govern such functionality, and network technology vendors created generations of solutions that enterprise buyers tried for years to make work on their perimeter-protected environment. Some were successful; others not so much.

So, most NAC implementations in the first and second generation experienced uneven results with their customers. Certainly, the goal of NAC is clear, and the objective of ensuring high integrity for devices joining a network remains entirely rational. But so many complicating factors have made typical NAC a tough proposition for larger companies. Mid-sized and homogeneous firms have reported better results, often because their networks are simpler.

The current situation in NAC is that many organizations continue to rely on this control for their existing, legacy networks. This situation will gradually change, but for the foreseeable future, NAC vendors will continue to do considerable business, and enterprise teams will continue to install the control, with its associated quarantines and other functional measures designed to protect the LAN and minimize annoyance for visitors.

The primary business question for NAC vendors is whether they can easily transition their traditional LAN-hosted capabilities toward a more virtual, SDP-based architecture. There is no reason why they cannot make this shift, but it will introduce a new set of competitors. Cloud access security broker (CASB) or virtual private network (VPN) vendors, for example, might introduce NAC-like controls for SDPs. The NAC vendors will have to navigate this new terrain.

2019 Trends for NAC

Network Access Control (NAC) has progressed from a less effective first generation, through a continued less effective second generation, toward a more effective future (see Figure 1-4). This would seem counter-intuitive as LAN infrastructure continues to dissolve toward device-to-cloud enterprise computing solutions. But this shift creates new opportunities for NAC vendors to provide admission control and quarantine capabilities for these new network approaches.

One clear trend in delivery of commercial NAC solutions involves the evolution of early detection and quarantine solutions that relied on manual configuration, administration, and operation, toward more automated NAC solution delivery. In addition, NAC is experiencing a shift from its traditional role protecting LAN infrastructure toward a more integrated delivery across virtualized hybrid cloud, including mobility.

An interesting observation worth noting is that international enterprise security teams, especially in the Middle East, Asia, and Africa, continue to center their protection solutions around LAN-based NAC. One would expect this to provide additional runway for traditional NAC vendors targeting IEEE 802.1x needs to experience revenue growth while cloud-based SDPs begin to shift the functional requirements for NAC toward virtualization.

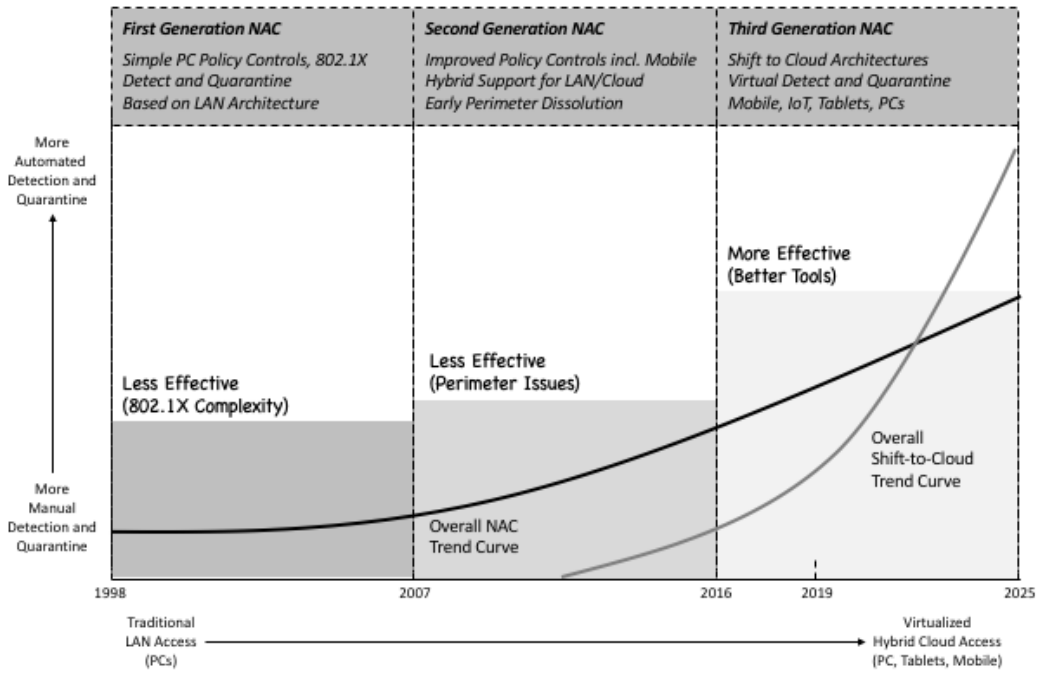


Figure 1-4. Network Access Control Trend Chart

The overall shift-to-cloud in the enterprise is accelerating in the current timeframe, and is having a clear impact on emerging SDP architectures for network access and security control. An inflection point is being approached where the effectiveness of new, virtualized NAC will exceed that of more traditional LAN-based solution offerings. This is good news for NAC vendors, as it creates excellent new business and revenue opportunities.

5. Unified Threat Management

A creative cyber security solution that emerged over the past decade for small and medium-sized businesses is known as *unified threat management (UTM)*. The idea in UTM is that a smaller enterprise would like its various cyber security-related functions to be integrated into a single, common appliance with a simple, consistent interface for managing and administering these various capabilities.

The resulting UTM devices included such familiar capabilities as firewall functionality, simple intrusion detection, VPN termination, and other commonly found security gateway functions. The simplicity of design and ease of operation made UTM solutions especially popular with these smaller entities, and allowed them to enjoy the advantage of next-generation features without having to go select and procure new products from a range of vendors.

The challenge with UTM is that smaller businesses are moving quickly to public cloud services, which dramatically reduces their local area network (LAN) footprint. Without a LAN gateway to the Internet, the role of a UTM solution becomes less clear. Nevertheless, the specific functions embedded in a UTM are still demanded, so the challenge for UTM vendors involves how to extend these capabilities to newer, more virtual architectures.

An additional challenge with UTM solutions is that they have tended to be implemented as hardware products. A clear trend in our industry involves some pause (or even a total halt, in some cases) by supply chain and procurement teams when hardware is being selected for purchase. The shift to software-defined-everything will find its way to UTM, and this represents both a challenge and a massive opportunity for UTM providers.

2019 Trends for UTM

Traditional, gateway-based UTM has progressed from an effective first generation, through an effective second generation, toward a less effective future third generation (see Figure 1-5). The justification for the 'less effective' view, is reduced need for hardware-based UTM appliances at the dissolving perimeter gateway. Such chokepoints are gradually diminishing in their frequency of use – hence the reduced need for hardware UTM appliances.

The good news, however, is the dramatically increased need to support the same basic gateway functions such as firewall and intrusion detection/prevention in the emerging, virtual small business enterprise. This need will drive a renaissance for UTM providers and will create demand for commonly provisioned, configured, and administered security along the same lines as traditional UTM, but rather for hybrid, and eventually complete public cloud usage.

The coverage of small and medium sized business (SMB) with UTM has progressed from a small initial footprint toward a greater deployment, and then toward a gradual trending downward for traditional hardware deployments. The trending for virtualized UTM is expected to increase dramatically in the coming years. Readers should note that this involves some prediction on the part of the analysts here, since virtualized UTM is not a big business today.

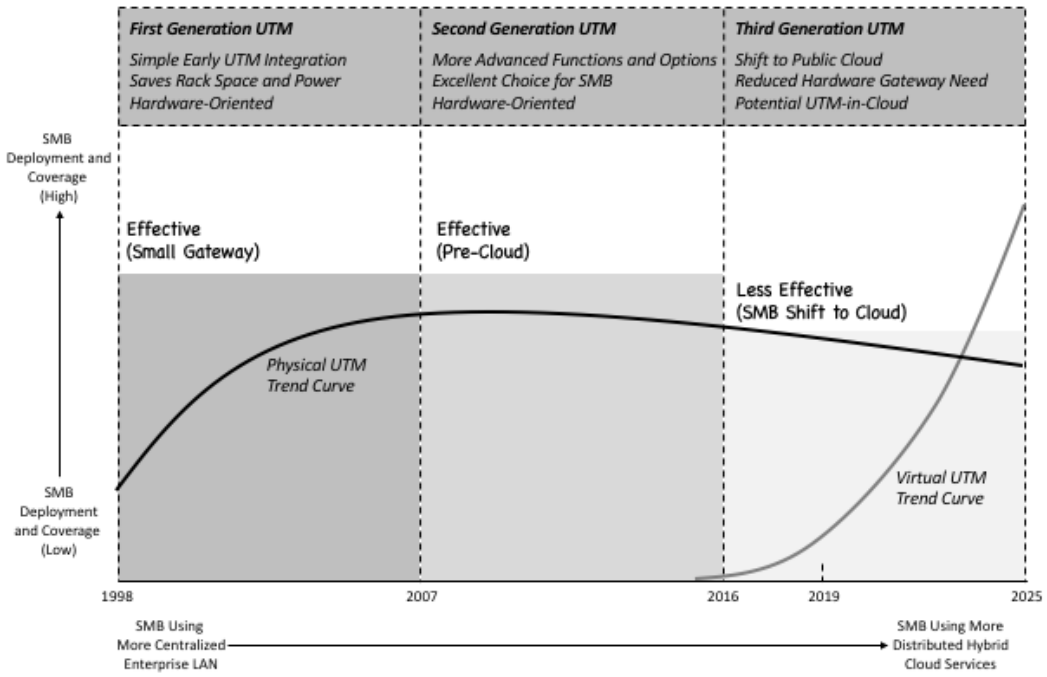


Figure 1-5. Unified Threat Management Trend Chart

The future of UTM is bright, so long as vendors recognize that SMB users will desire all the benefits of common UTM management, but in the context of a virtual infrastructure. This evolution will cause some competition with cloud access security brokers (CASBs) and microsegmented security solutions, but the UTM vendors will have the advantage of having served the SMB market for many years.

6. Web Application Firewalls

Web application firewalls (WAFs) originated as a means for tailoring policy controls to a specific application hosted on a website. This contrasts with the more general nature of intrusion detection and prevention systems, as well as conventional firewalls, which must include broad sets of rules that must address the policy needs for all the applications, systems, networks, and users that are being protected by that device. WAFs can be more specific.

The way a WAF works is that it sits in-line with the HTTP conversation that occurs between a client browser and a web server. Its main purpose is to reduce the risk of attacks on the server, and this includes prevention of commonly found web application exploits such as cross site scripting (XSS) attacks and SQL injection. Surprisingly, these two exploits continue to occur, despite their stubborn existence in the offensive arsenal for so many years.

Security architects often differentiate client and server protections in the context of a so-called *proxy*. That is, if some entity desires interaction with a resource, then a proxy can reside in-line and play the role of that targeted resource to ensure proper security. When this is done for clients, the proxy is maintained by the administrator of that client group. When this is done for servers, the function is called a *reverse proxy*, and WAFs generally fall into that category.

A challenge in deploying and maintaining any WAF is that as the HTTP application being protected is modified, the corresponding reverse proxy functionality must be adjusted accordingly. This complicates services such as managed WAF, because the policy and rules adjustments for a given application might occur frequently. One might view such adjustment as an acceptable burden for the tailored protection, but it certainly does increase workloads.

2019 Trends for WAFs

WAFs have progressed from less effective reverse proxy devices in the first generation, toward more full-featured HTTP security devices in the second generation, to more automated solutions for protecting web applications in DevOps environments in the third generation (see Figure 1-6). An obvious progression through this evolution is that the initial small attack exploit signature set has grown to include many more types of attacks.

As one would expect, it has been a challenge to keep up with the shift from less frequent changes in a typical application web application toward the present day (and future), where application changes are frequent and the norm. In a typical DevOps environment, for example, application changes might occur daily, which implies that any corresponding WAF must be integrated with this maintenance lifecycle, preferably using automation.

One would also expect to see application hosting providers offering WAF-like capabilities to their customers as an embedded service. This will be best done in partnership with the WAF provider marketplace, because most application hosting teams will likely underestimate the challenges of maintaining WAF accuracy with ever-changing app functionality. Nevertheless, this will be a growth area for the WAF ecosystem – and hence an opportunity for vendors.

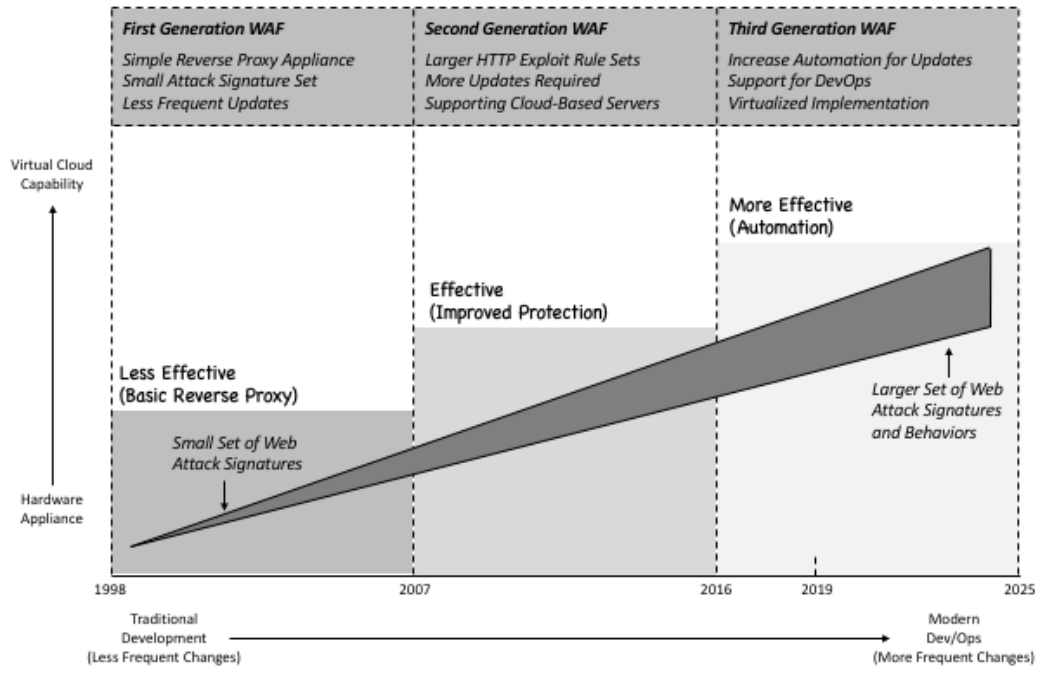


Figure 1-6. Web Application Firewall Trend Chart

The future for WAFs lies in several trending areas: First, WAFs must continue to improve the accuracy and coverage of the exploit detection for HTTP applications. This must continue to shift from simple detection of XSS attacks and SQL injection toward behavioral-based detection, perhaps using advanced heuristics, that can learn from observed client-server communications to recognize attacks that might be brewing.

Second, WAFs must continue to integrate into the DevOps lifecycle, so that as HTTP application owners making rapid, frequent changes to a given software application, can rely on the WAF to keep up. This is only possible in the context of automated controls that are integrated directly into the DevOps lifecycle. This constraint is consistent with other cyber security tools, but is particularly important for WAF evolution.

7. Web Fraud Prevention

Web fraud prevention tools emerged in direct response to an increase in malicious fraudulent activity aimed at websites, usually targeting eCommerce or financial applications, in the early 2000's. The goal of such fraudulent attacks almost always involves financial gain. The tactics used range from easily identified steps that can be codified into signatures, to more subtle tactics that exploit specific weaknesses in the targeted site.

Readers might be tempted to interpret "web fraud prevention" tools in the broadest sense, perhaps including the range of detection, response, and notification services offered by banks, credit card companies, and other large entities. A more acceptable interpretation for the work presented here involves an automated cyber security tool placed adjacent to, or in-line with, a given website to perform an intrusion detection-like function.

A typical heuristic involves watching a web session to determine if the initiating user is exhibiting behavior indicative of fraud. For example, if an eCommerce website includes a wizard that allows for some sort of account sign-up, then normal users might be expected to patiently click through the wizard steps. A fraudster, expecting to deal with many wizards, will more likely find a way to skip the interim clicks; web fraud prevention tools would watch for this.

2019 Trends for Web Fraud Prevention

Web fraud prevention has progressed from a less effective first generation based on the simplest early signatures, to an effective second generation with more behavioral analytics. The third generation promises to be a welcome era for web fraud prevention, as emerging machine learning and artificial intelligence-based processing appear to be well-suited to this type of cyber security challenge (see Figure 1-7).

The general strategy in web fraud prevention has evolved from a reactive control that watches for evidence that the fraudulent behavior has already begun, toward a more proactive control that focuses on detecting evidence that fraud might later occur. The architecture has shifted from a centralized gateway solution to a more distributed, virtualized function capable of becoming embedded in a software-defined network.

Perhaps a more fundamental question for web fraud prevention tools is how central web-based technologies will be to business activity in the future. The introduction of mobile applications and social network-based communities represent challenges to the status quo in eCommerce marketing and sales. One thing is for certain, however, and that is the inevitable attempts at fraud that will follow whatever means for commerce is in use in coming decades.

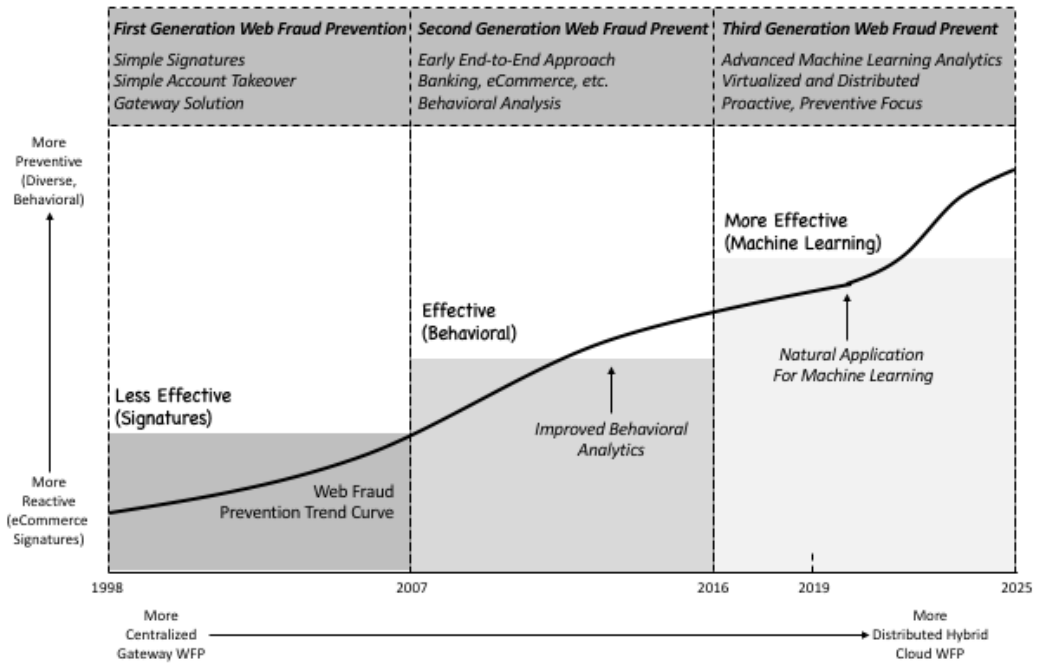


Figure 1-7. Web Fraud Prevention Trend Chart

The future of web fraud prevention appears to be centered on truly advanced predictive heuristics, which points, in turn, to machine learning and artificial intelligence. Since the nature of this control involves determining characteristics of the user (or automation) at the other end of a session, Turing tests and other forms of advanced processing are also well-suited to this security control.

8. Web Security Gateway

Web security gateways (WSG) emerged as critical cyber protections once enterprise teams recognized that any entity inside a perimeter might initiate outbound sessions with both known and unknown websites on the Internet. This included both appropriate and inappropriate sites (e.g., gambling), as well as benign and malicious sites. The malicious websites were ones preconfigured to accept information beaconing from an infected internal entity.

The resulting WSG proxy device soon became an essential filter for enterprise egress traffic, generally fed by a live threat intelligence feed from vendors with research teams watching for suspicious website URLs. Since this gateway filter was typically installed in-line with all Internet traffic, the performance was a key differentiator, and companies specializing in web acceleration were well-suited to developing early products in this area.

Most organizations today view their WSG as an essential safety net for endpoints and users – one that serves as a last-resort against policy violations and data exfiltration. That is, for an infected endpoint to beacon out sensitive data, it must have already been compromised and gone undetected. The WSG proxy will hopefully detect and block the exfiltration as a point of last protection. For this reason, the function will remain an essential one for all organizations.

2019 Trends for Web Security Gateway

Web security gateways began as effective proxy devices in their first generation, became more effective in the second generation, and should be expected to become even more effective in the third generation as algorithms and threat feeds continue to improve (see Figure 1-8). This trend is good news for enterprise security teams who rely on this important functionality to reduce their data exfiltration risk.

Additional trending involves WSG detection and prevention approaches moving from lists of URLs to more advanced behavioral capabilities designed to detect malware and other exploits. The architecture of the WSG will also shift considerably, as the perimeter dissolves. While the “functional need” for WSG continues to grow, the “traditional perimeter” set-up has already begun to wane.

The result of all this architectural evolution in the enterprise is that “virtualized WSG capability” will become an important functional component of emerging cloud-based software defined perimeter (SDP) enterprise set-ups. Expect to see such functional ability to provide both forward and reverse proxy-based protections for cloud workloads, virtual perimeters, application containers, and other virtual constructs.

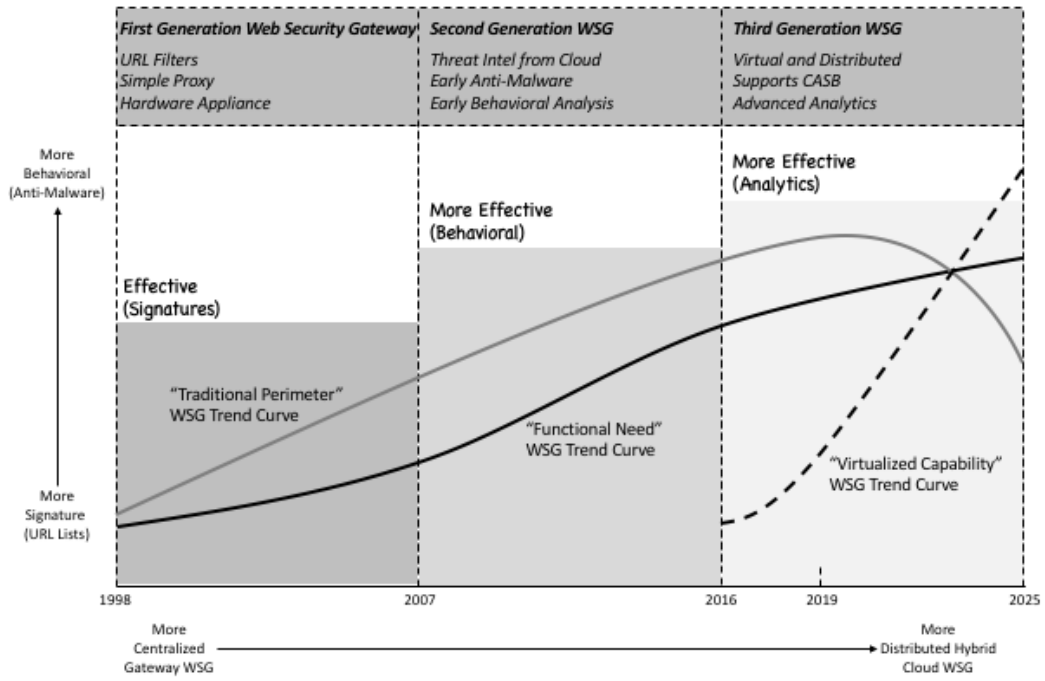


Figure 1-8. Web Security Gateway Trend Chart

WSG for enterprise cyber security has been one of the most successful functions over the past two decades, but massive de-perimeterization will prompt changes in this solution area. With fewer companies each day relying on a physical Internet perimeter, the web security gateway becomes more a functional requirement than a tangible device. The best vendors will recognize this and adjust, but security teams should keep a close watch on how this transition is handled.

9. Public Key Infrastructure/Certification Authority

Public key infrastructure (PKI)/certification authority (CA) solutions originated with great advances in cryptography half a decade ago, and have continued to be refined and improved by talented computer scientists, many of whom serve in academia. PKI-based technology maybe the most elegant, but also the most complex, technology employed in the enterprise security arsenal, and for this reason, has experienced varying levels of proper application and attention.

Surprisingly, few technology companies have found ways in the past few decades to make decent money selling pure PKI solutions. Instead, the capability has emerged as an essential embedded component of many other software and computing functions. It underlies all encryption support, all secure networking, and many other aspects of cyber security including software integrity checking, secure file transfer, and secure messaging.

One area where enterprise users and service providers should be more attentive, and likely will be more attentive in the future, involves the proper security protection of keys and certificates. Like privileges and passwords, these important elements of the security architecture are often handled either manually or via ad hoc procedures. This is getting better, but deserves more attention in the marketplace.

2019 Trends for PKI/CA

PKI/CA solutions have evolved from effective PKI/CA embedded in browsers for SSL in the first generation, through improved and more effective operations in the second generation, toward a current third generation, where the technology continues to be effective (see Figure 1-9). The number of CAs in business remains high, but their business success is mixed, with perhaps a Pareto chart of financial returns having a long tail of small CAs of dubious quality.

The trend from more ad hoc, manual operations began in the first generation of PKI/CA solutions with the admirable goal that multiple assurance levels would provide users with the ability to determine the proper fit for their application. CAs published statements of their certificate policies and assurance processes, and it was assumed that this would be viewed as valuable information for users.

What happened instead was that few users bothered to review the multiple assurance levels for certificate handling (not unlike users reading user licensing agreements for software), and instead, the process converged on assumed basic assurance levels. This has led to more uniform handling of PKI/CA at the service provider and enterprise levels. Most larger organizations have had their PKI operations audited in the past few years.

The trend from a smaller mix of supported services by PKI/CA solutions, to a much larger mix of supported services, follows the trend toward more devices needed cryptographic support. The explosive growth of Internet of Things (IoT) and operational technology (OT)-based devices and systems will require comprehensive PKI support for embedded secure communications, authentication, and other operations.

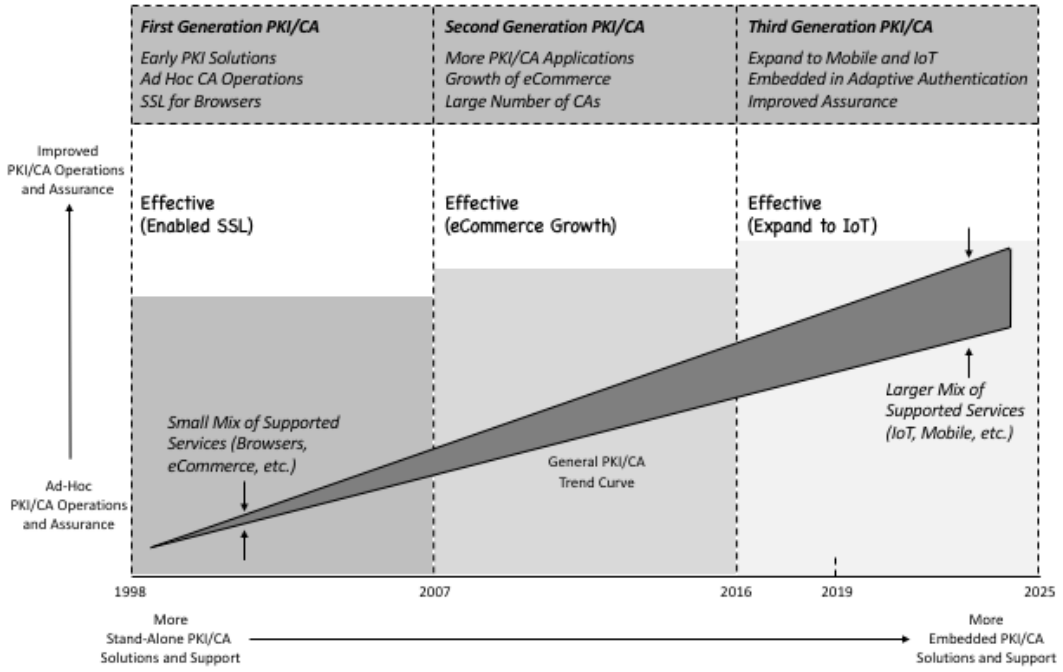


Figure 1-9. Public Key Infrastructure Trend Chart

The future of PKI/CA solutions is bright from a technology perspective, in that the underlying algorithms, tools, and protocols will serve as the basis for much emerging technology. Autonomous machines, for example, will require embedded cryptography for their communications. The business prospects, however, will remain muted, as PKI/CA solutions will continue to serve as embedded, rather than highlighted components of a security architecture.

10. Cloud Security/CASB

Cloud security has emerged as one of the most important areas of cyber security protection, both as a stand-alone category, and as a broad solution descriptor for a mix of sub-categories focused on cloud protection. Perhaps the most prominent offering of these categories, *cloud access security brokers (CASBs*) and cloud workload visibility software, have truly grown in recent years into components found in virtually all hybrid cloud architectures.

The drive to hybrid use of public cloud has been the obvious driver of these solutions. The great irony is that some more progressive security experts have come to recognize that cloud might be more in the solution-column than the problem-column for overall cyber security. Consider, for example, that by scattering workloads across public cloud as-a-service systems, the frightening lateral traversal risk for advanced persistent threats wanes considerably.

Every enterprise security team today includes some measure of cloud security, if only as a set of protection and data handling requirements for any third-party public cloud services in use. Managing and coalescing the plethora of scattered cloud accounts among individual employees using their work email address, into one master account is also popular to better control cloud access, as well as to ensure proper licensing support for enterprise use of cloud service.

It is worth mentioning that the compliance-oriented approach of early enterprise teams to cloud services has now shifted toward functional cyber security. This is good news, because it implies a more active role for CISO-led teams in determining how data and systems are secured in the cloud. The early checklist approach that just passively requested security data from cloud providers has thus been improved dramatically in most enterprise environments.

2019 Trends for Cloud Security

Cloud security solutions evolved from less effective initial offerings in the first generation of cloud usage, toward effective solutions in the form of CASB and micro-segmentation products in the second generation, toward a present and future generation of more effective solutions with heavy growth in the use of CASBs for cloud visibility and potentially software-defined perimeter support (see Figure 1-10).

The intensity of cloud usage for enterprise during this generational evolution has gone from low to high, and the attitudes of security and IT staff have shifted from security as-a-problem to cloud security as-a-solution. The importance and magnitude of this shift, especially on the part of senior managers, board members, and compliance auditors, cannot be under-estimated, because it has unlocked one of the most consequential shifts in the history of enterprise IT.

As a result, expect a shift downward in compliance concerns across enterprise for cloud systems supporting critical services. Compliance concerns have peaked in the 2018/2019 timeframe, but this will weaken as managers and security teams become more comfortable with cloud, and as providers continue to innovate. Commercial tools from the best cloud security vendors will also contribute toward this improved comfort zone.

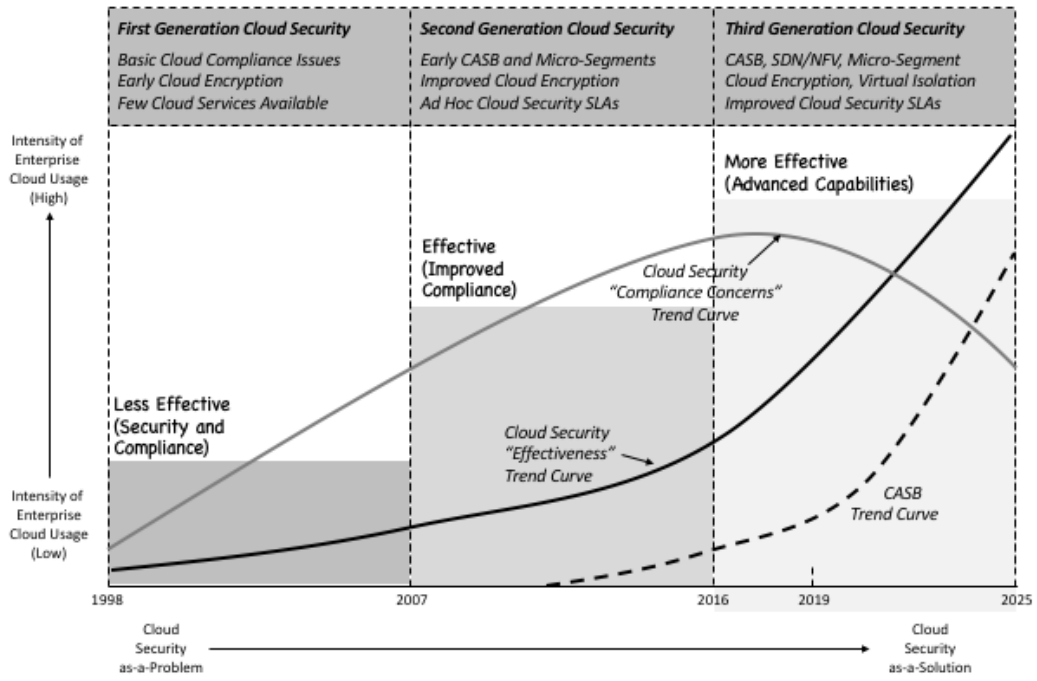


Figure 1-10. Cloud Security Trend Chart

The future of cloud security is about as bright as one will find in the cyber security industry. The need for world-class commercial tools will continue to increase across all segments of the enterprise, and vendors will see significant growth – so long as they continue to provide good solutions. CASBs will play an especially important role in redefining the corporate enterprise as they transition from passive visibility tools to more active mitigation components.

Expect to see SDN-powered solutions play a larger role for cloud security, including in the adjacent area of software-defined data centers (SDDCs). In addition, virtual management and orchestration of policies across distributed workloads will be a massive growth area for cloud and SDDC installations. Vendors who can successfully support orchestration in cloud will see considerable business success and growth in the coming years.

11. Distributed Denial of Service

Distributed denial of service (DDOS) Security solutions emerged purely in response to the growth of denial of service as a legitimate attack weapon against businesses with real potential consequence. In the earliest days of DOS and DDOS, the attacks were mostly for play and for show, and it was rare for a serious attack to cause much more than a bit of buzz and stir around the networking community (e.g., the early DDOS attacks of 2000 against eBay).

As the attacks grew from small single-digit Mbps capacities to the eye-popping, almost Tbps sizes of today, the DDOS solution space grew into an important consideration for every sector. Vendors in this space grew from a niche technologists to significant, and highly recognized brands in cyber security. This fact underscores how important it is for modern enterprise to ensure that their data can flow into and out of Internet-facing sites.

It is worth mentioning that many teams point to the use of content distribution network (CDN) as providing important protection against DDOS attacks. One cannot dispute that distribution of access points for websites and other on-line resources is a great way to reduce the exposure to a targeted, volume-based flood. It seems both prudent and imperative, however, that emergency procedures be established to deal with unexpected in-bound traffic waves.

Ultimately, the best DDOS security for enterprise will start with excellent scrubbing capability, including virtualized support, to protect the most important systems and services from significant, targeted attacks. But this capability will be enhanced by well-designed architectures using both CDN and distributed cloud workload approaches to ensure a high level of resilience against DDOS attacks, usually from botnets.

2019 Trends for DDOS Security

Distributed denial of service (DDOS) solutions evolved from less effective, ad hoc filters in the first generation, to effective solutions using automation in the second generation, toward more effective solutions including virtualization support in the present and future third generation (see Figure 1-11). Each of these solutions include designated scrubbers in special data centers, but future DDOS security will introduce virtual scrubbing, which reduces the need for hardware.

During this evolution, trending has moved from low deployment across the typical enterprise – perhaps even including little or no DDOS security for many Internet-facing services, to high deployment across all enterprise networks connected to public or external infrastructure (which implies all enterprise networks). Larger enterprise teams complement their DDOS security with a CDN to distribute ingress traffic to multiple gateways.

The algorithmic processing of DDOS security solutions has also progressed from simple Layer 3 procedures that rely on basic signatures of attack, including detection of increases volumes or packet rates, to more advanced means for dealing with complex, application Layer 7 attacks by searching for subtle evidence of a brewing attack. Application-level DDOS solutions are an essential modern control in our industry today.

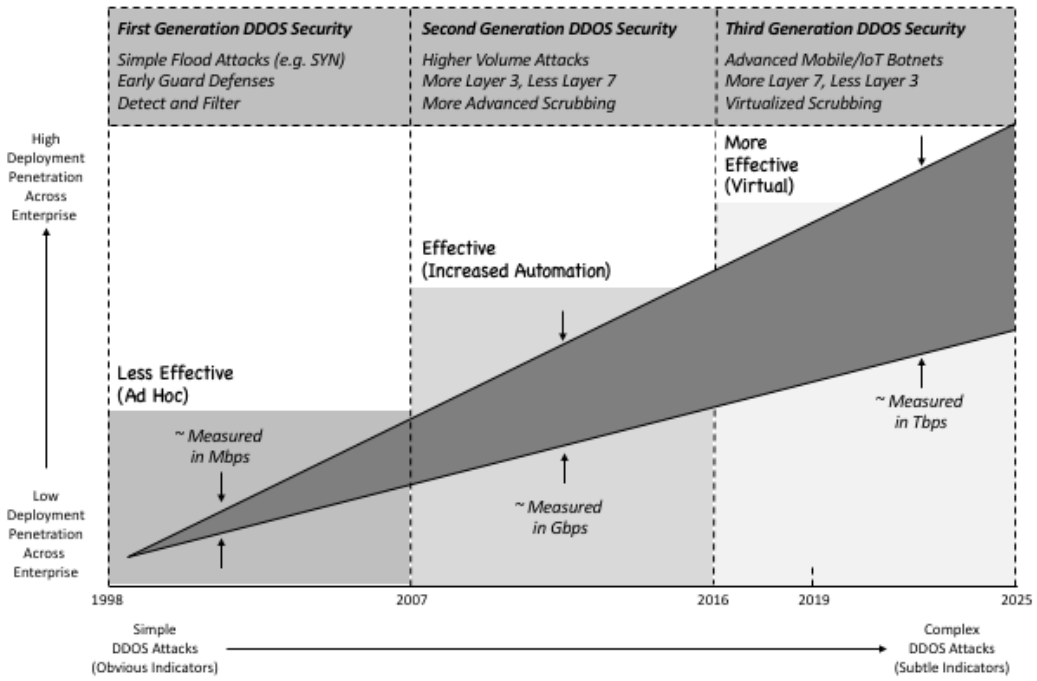


Figure 1-11. Distributed Denial of Service Trend Chart

The future of DDOS security lies in the introduction of advanced new controls for cloud infrastructure, mobility systems, and dynamic on-demand virtualized services such as software defined networks (SDNs). Virtualization allows for targeted infrastructure to expand (like a balloon) to absorb inbound attacks, and to contract when the volumes wane. This capability is especially exciting, because it can help address the almost limitless size of future attacks.

It is worth mentioning that Internet of Things (IoT) and industrial control system (ICS) devices connected to the Internet will offer a significant base for offensive actors to create massive botnets with great ability to perform DDOS attacks. One would expect DDOS solutions to include some attention to the unique challenges of IoT and ICS endpoints, including their use of often-proprietary protocols and technologies.

12. Email/DMARC Security

Email security is arguably the most important and essential control in the modern enterprise – if only because phishing has emerged as the most common and successful attack strategy amongst every type of offensive approach. This suggests that an extensive and coherent email security deployment would be the norm across enterprise, but the reality is that few enterprise teams have an optimal or even rational architecture for email security.

A great irony is that many security teams rely on awareness programs to deal with the phishing threat. Such education is certainly a reasonable complementary element of any program, but functional controls are more desirable to reduce risk. It is reasonable to expect that normal users would not have to carefully police their activities to ensure a primary control. This is much better automated as functional protections.

For example, excellent fraud protection of domains comes from *Domain Message Authentication Reporting and Conformance (DMARC)* implementations offered by the best email security vendors. Email encryption is also available from many different types of platforms. In addition, email filtering can be embedded into gateways for identifying potentially malicious content and taking appropriate steps toward proper removal.

2019 Trends for Email Security

Email security solutions were initially deployed in the first generation, but slipped in effectiveness as phishing became a more intense threat in the second generation, and is now evolving toward an effective control in the third generation. Improved algorithms and more accurate detection of malware are major contributors in this shift toward better solutions for protecting email.

DMARC deployment is also rising quickly from its inception in 2010, as well as its more modest roots in DomainKeys Identified Email (DKIM) and Sender Policy Framework (SPF) in the early 2000's. This shift is welcome, because fraudulent use of domains, especially in the context of financial services sector use, continues to be a significant attack vector. DMARC usage is an excellent means for reducing this threat.

Additional good news is that email encryption has become more mainstream in modern business, although ease of set-up remains somewhat uneven. It is not uncommon for two business partners in 2018 to have to get their IT teams together to agree on a reasonable means for sending secure email. Creative solutions such as from BotDoc are also commonly deployed to make encryption more commonly used.

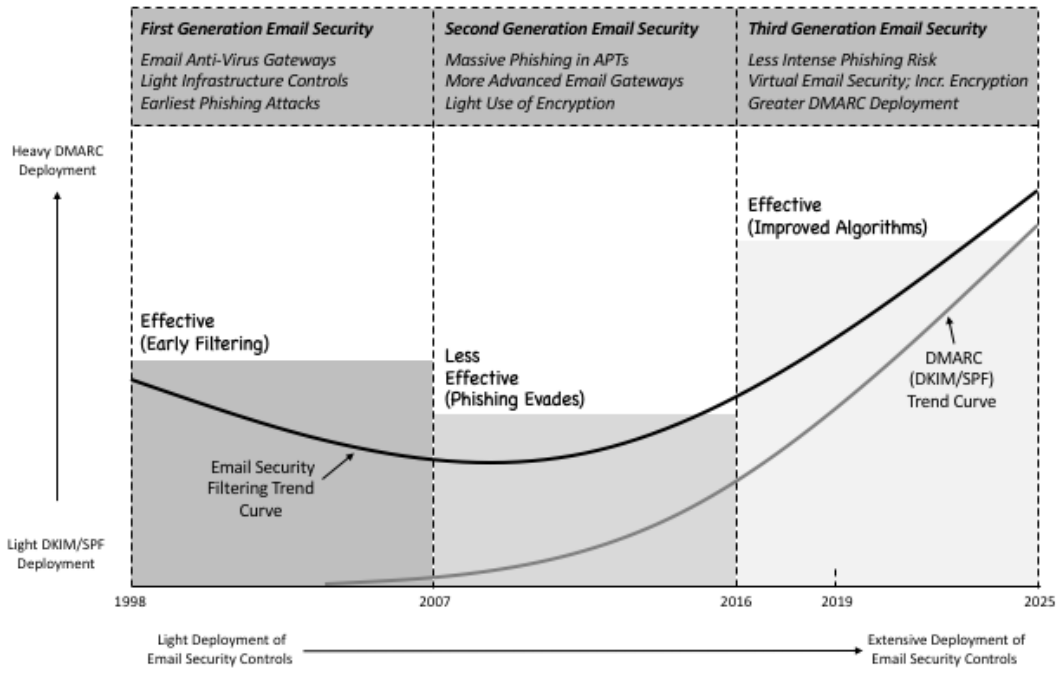


Figure 1-12. Email Security Trend Chart

Future email security solutions will need to expand their coverage from pure email use toward combined use of various over-the-top means of communication. Texting has already become a mainstay of modern business, but applications typically include means for individuals or groups to communicate. Security solutions for these new forms of connecting and communicating will be required – and email security vendors are best positioned for this.

13. BGP/DNS/SDN Security

The category of *infrastructure security* has always been challenging, because on the one hand, it includes the most intense threat vectors on the Internet today: *Routing* and *naming*. On the other hand, the category includes issues that are likely non-actionable by most enterprise security teams, especially ones with smaller teams or fewer experts involved in defining standards or providing cyber security thought-leadership.

The routing issue revolves around the challenges associated with the *Border Gateway Protocol (BGP)*, which can be considered the protocol and supporting infrastructure by which the administrators (and owners) of larger networks can direct and manage traffic flows. When this process is manipulated, and it often is, traffic can be rerouted to unusual mid-points, perhaps to collect intelligence or even sniff traffic content.

The naming issue revolves around the challenges associated with the *Domain Name Service (DNS)*, which can be considered the protocol and infrastructure by which many different individuals and groups around the world can connect names with Internet Protocol (IP) addresses. The types of attacks, tricks, exploits, floods, and other manipulations of DNS have become so voluminous as to be beyond the scope of this document.

The bottom line is that security teams must focus on three activities to reduce BGP and DNS risk: First, they must put pressure on infrastructure and telecommunications providers to manage BGP and DNS infrastructure securely. Second, they must follow best security practices for their own DNS usage and application. Third, they should be vocal wherever possible, such as in industry groups (e.g. Cloud Security Alliance) to keep awareness of these risks high.

A third significant infrastructure security issue arises with the introduction of *software defined networks (SDNs)* to the global network ecosystem. SDN has already pervaded the data center, resulting in software-defined infrastructure that requires proper protection; but its introduction to network fabric, including in emerging standards such as 5G for mobility, raises important obligations for providers to ensure sufficient virtual security protections.

2019 Trends for Infrastructure Security

BGP and DNS infrastructure security was less effective in the first generation as the risks to routing and naming were poorly understood and infrastructure providers had few solutions. The second generation produced slightly increased risk for BGP, but dramatically increased challenges for DNS, especially in supporting DDOS attack. The third generation has improved DNS security, given the enhanced procedural DNS controls across industry (see Figure 1-13).

Security incidents, especially for DNS, have trended generally upwards, but virtualized SDN infrastructure at the carrier and data center levels should have a beneficial impact on infrastructure threats, if done properly. Virtual security improvements should also be present for DNS, due to the architectural shifts that occur with SDN. Data center workloads, for example, will rely on SDN controllers for east-west traffic management.

In general, the security community has come to gradually increase its collective emphasis on infrastructure security concerns across the three generations of usage. This is a welcome trend, but has also been characterized by mostly disappointing controls for both BGP and DNS. Adding PKI-based technology to both protocols has done little to reduce risk; in fact, PKI-enablement for DNSSEC could be viewed as increasing DDOS risk due to larger payloads.

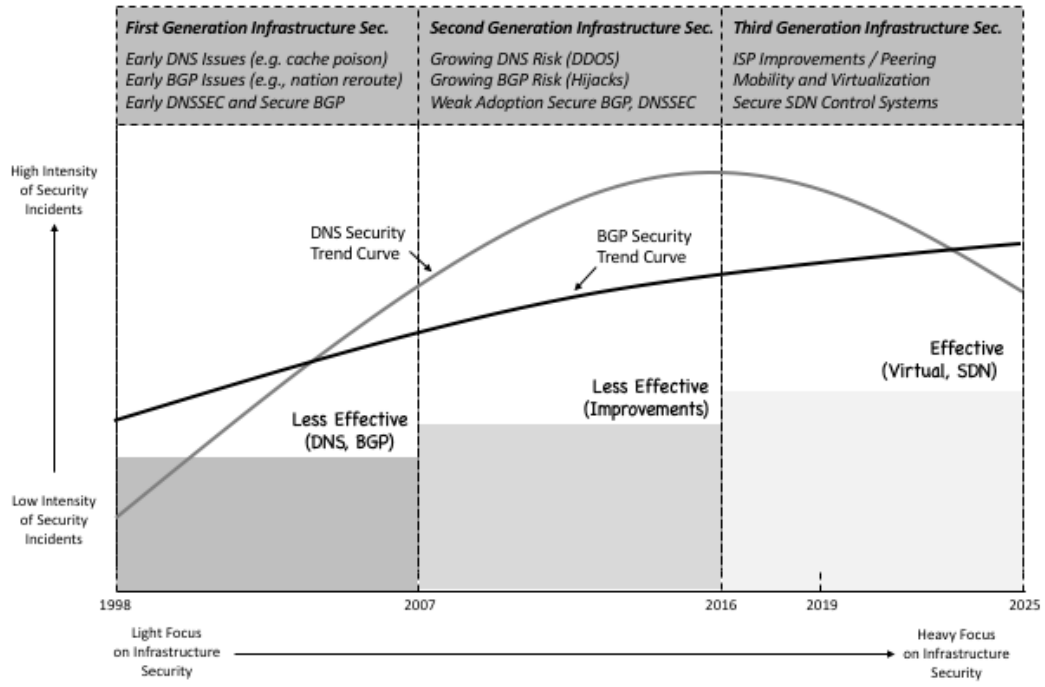


Figure 1-13. BGP/DNS/SDN Security Trend Chart

Sadly, future infrastructure security solutions for BGP and DNS are likely to continue to play a more negative than positive role in overall global cyber risk. Organizations with research and development (R&D) responsibility such as in academia and government are encouraged to continue their investigations into making both types of infrastructure security controls more effective in future applications.

The biggest challenge here is that enterprise security teams do not directly control the management and mitigation of this infrastructure risk. Instead, they are mostly dependent on carriers and major service companies including cloud vendors to ensure sufficient risk management. The best approach for CISOs and their teams is to maintain pressure and to demand that security – especially for BGP and DNS – be attended to carefully and diligently.

14. Network Monitoring

Network monitoring has always been an important component of cyber security architectures, but the specific methods for collecting and processing data have evolved as network systems in enterprise and carrier infrastructure have also evolved. Larger networks have been the prime focus of most network monitoring solutions to date, but with virtualization has come the ability to introduce this capability in a software-based environment.

The primary functional requirements for network monitoring in cyber security have centered on the capability to (1) collect data at large capacities in the 10 Gbps to 100 Gbps range, and (2) process this collected data at line speed using analytic tools and algorithms designed to detect evidence of the desired properties of interest. For cyber security, this means indicators of compromise. Other areas of focus include law enforcement and network management.

Privacy has always been an important consideration in network monitoring from two different perspectives: First, citizens in many nations are unhappy with the idea of their personal data being collected and processed, even if algorithms are used to filter unwanted information. Second, with privacy-concerns driving increased encryption of network traffic, many monitoring solutions become challenged to detect the desired properties.

Nevertheless, world-class tools and supporting infrastructure for collecting data from a network, making sense of that data – including dealing with any encryption of relevant indicators, and then taking mitigation action based on the network analysis, will remain a staple of large-scale cyber security protection. This cadence also provides a foundation for much of the day-to-day work that occurs in a typical security operations center (SOC).

2019 Trends for Network Monitoring

Network monitoring evolved from effective hardware platform solutions in the first generation, to continued effective, higher capacity platforms in the second generation, to continued effective solutions with more advanced algorithmic processing in the third generation (see Figure 1-14). The trend curve for capacity has evolved from collection in the Mbps range, with maximums in the low single-digit Gbps range, up to modern solutions in the Tbps range.

This evolution has been characterized by hardware appliances being used exclusively toward a more eclectic mix of offerings, although the highest capacity collection and processing continues to require specialized hardware. Algorithms have also gone from simple pattern matches and searches for obvious signatures and indicators to more subtle methods that are beginning to rely on advanced heuristics and even machine learning.

One would expect that with the advance of software defined networks (SDNs) in the provision of network infrastructure that network collection techniques would quickly gravitate toward control by SDN applications. Thus, the northbound SDN controller interface would connect to apps that would manage and orchestrate collection from devices across the southbound interface of the SDN controller.

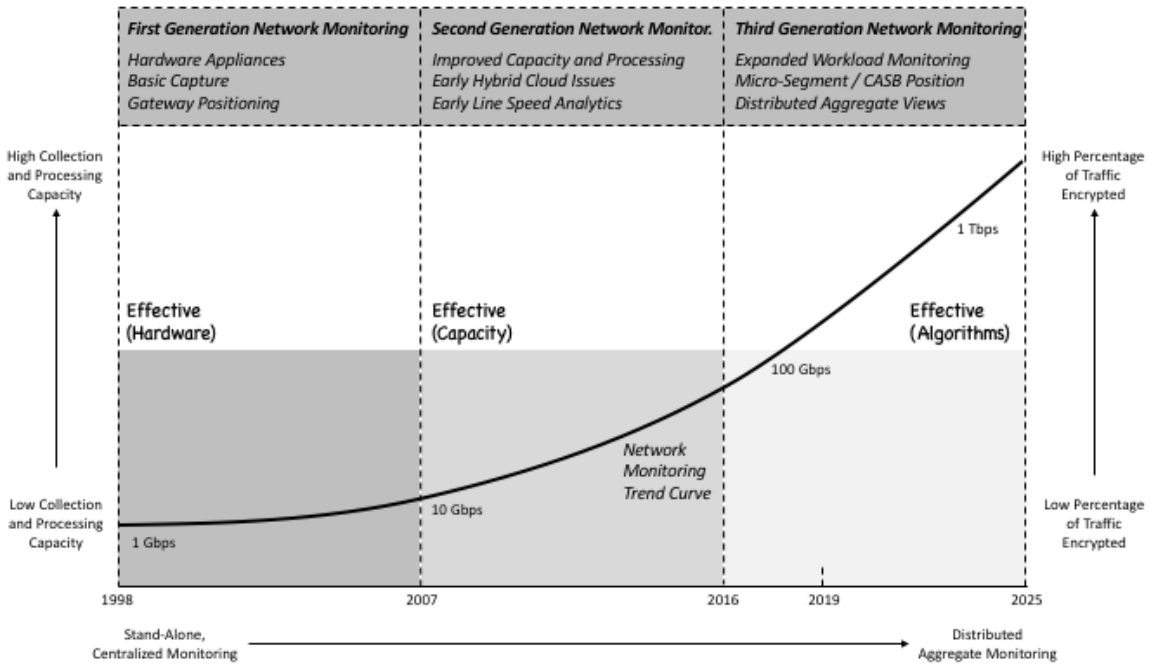


Figure 1-14. Network Monitoring Trend Chart

The future of network monitoring will include two basic tracks: As network capacity continues to increase, network monitoring solutions will continue to drive to the maximum size and speed of the infrastructure of interest – often from carriers and larger organizations such as military groups and banks. But in addition, AI-based methods will begin to take hold in network monitoring platforms, offering significant new opportunities to detect indicators quickly.

15. Secure File Sharing/Sending

Secure file sharing is a common name used in the industry to support general collaborative data interactions between consumers, business partners, colleagues, customers, suppliers, and on and on. One subtle issue, however, is that more direct operations such as *secure file sending* and *secure file receiving*, are separate from the more general secure file sharing category. The security issues that result from the various cases will in fact be different.

A common goal, however, for both secure file sharing and sending is to support the desired interaction without introducing vulnerabilities or exposures. This generally requires attention to three basic functional requirements: First, the interaction must be authenticated – preferably in a mutual manner. Second, the interaction must include encryption of any transmitted data. Third, the data transfer should include evidence that integrity has been preserved.

Surprisingly, the secure file sharing community has included a plethora of confusing, complicated, and often tough-to-use tools that have been poorly integrated into familiar enterprise tools such as the Microsoft Exchange and Office suites. This is beginning to change, as vendors, including large providers such as Microsoft, have come to realize how important support for secure file sharing and sending has become.

In addition, excellent and easy-to-use utilities have emerged that allow for fast, convenient, and secure file sending and receiving between participants who might not have interacted previously. This is a welcome advance, because it supports business practices that go back many centuries or longer – namely, the routine back-and-forth cadence between buyers and sellers who have not previously interacted. This is the basis for most commerce.

2019 Trends for Secure File Sharing/Sending

Secure file sharing and sending have evolved from less effective first generation solutions based on File Transfer Protocol (FTP) and email, to effective second generation solutions that were more securely designed (although not as widely deployed as they should have been). Third generation secure file sharing and sending solutions are now more effective from both a security and wide deployment perspective (see Figure 1-15).

One of the key aspects of this evolution has been the shift in emphasis from light, exception-based use of encryption or other security enhancements for file transfer and collaboration, to more routine use of security capabilities. Today, it is no longer considered an unusual request for a business partner to demand or expect that files be transferred in a manner that avoids cyber risk. This is a welcome change.

Additionally, cloud-based shared services have lent well to more secure remote collaboration, interaction, sharing, and sending of files and other data in a manner that respects security considerations. The concept of a secure cloud-based service involves protections that do not rely on network locality or trust to ensure controls. Instead, cloud services treat all requests as untrusted, which is consistent with secure file handling solutions.

It is worth highlighting that embedded support for secure file sharing, transfer, and sending within popular public cloud-based services is not only inevitable, but has already begun to occur at scale. The industry should expect to see exponential growth in security features for users of public clouds, especially ones that already support data storage, handling, and collaboration by different untrusted entities.

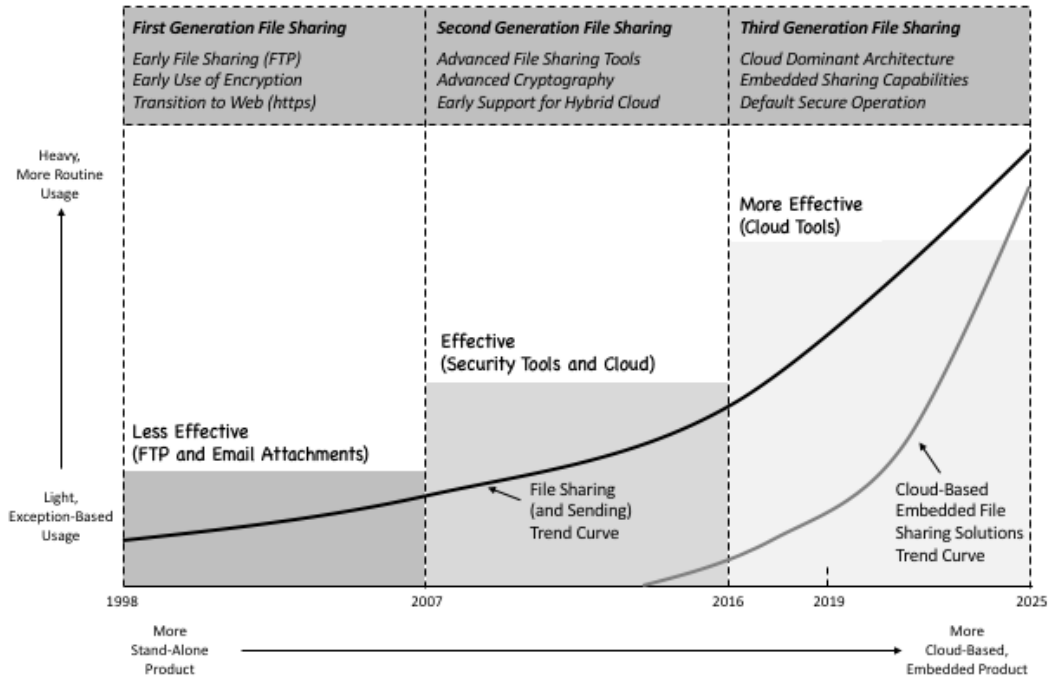


Figure 1-15. Secure File Sharing Trend Chart

The future of secure file sharing and sending lies in cloud. It seems inconceivable in the coming years that major public cloud providers will not aggressively pursue this business area. They'll certainly need to work with (or acquire) specialized firms that offer best-in-class tools, including secure sending capabilities. But in the end, one should expect that most consumer and business secure file interactions and handling will be done in the context of cloud services.

16. Secure Remote Access

Secure remote access began in the 1990's as a clever means for enterprise workers to gain remote login to the corporate LAN to work on weekends and evenings (or during snow storms). Gateways were established that allowed for such remote access, often with just a password for validation, and many of these mechanisms reside on corporate LANs today, albeit often with enhanced two-factor authentication.

The first challenge that occurred for secure remote access involved mobiles, which required slightly different handling than home PCs for gaining admission to the corporate LAN. Various solutions such as container-based tunnels and per-app VPNs to enterprise-hosted applications found their way into the enterprise in the 2000's and this created a bifurcated secure remote access environment for PCs and mobiles.

The second challenge for secure remote access involved public cloud-based services. Where the initial presumption in the design of remote work solutions was that enterprise apps were hosted on the corporate LAN, the modern evolution saw such apps find their way to public cloud-hosted systems, located outside the corporate firewall, and thus outside the location where secure remote access gateways had been installed.

The result was a hybrid arrangement, which exists to this day, where users with their mobiles and PCs use a variety of techniques to access on-premise and cloud-hosted applications. Some would call this the essence of a hybrid arrangement, where others might simply call such set-up a total mess. Regardless of the moniker used, the hybrid approach does not lend well to orchestrating common, uniform procedures or policy enforcement.

2019 Trends for Secure Remote Access

First generation secure remote access supported the growing need for telework, and the typical security scheme was less effective regarding threat. Second generation secure remote access improved matters with the introduction of two-factor authentication. Third generation secure remote access, present and future, is moving in the direction of highly-effective, highly-secure solutions that are integrated with modern cloud and mobility (see Figure 1-16).

Weak authentication using one-factor for early secure remote access from home PCs and laptops to the corporate LAN, has been replaced with more factors – up to and including three-factor authentication in some cases (e.g., mobile device biometrics, MDM-managed certificate, and user supplied password). This is excellent news for enterprise security teams, since many attacks traditionally included unauthorized remote access to the LAN.

The biggest debate regarding secure remote access involves the degree to which the user experience integrates with existing procedures. The best modern cyber security vendors specializing in secure access solutions understand that without careful attention to minimizing the number of steps (preferably down to zero) required to establish secure connectivity, the associated solution will not be welcomed by users.

This implies that the establishment of VPN connectivity through a designated application, as well as the early and existing focus on virtual desktop initiatives (VDI), will have the great disadvantage of not minimizing the number of steps to establish secure access. The most successful solutions in the coming years will have to be largely invisible to users, and the resulting risk reductions will be well-worth the additional design time and effort.

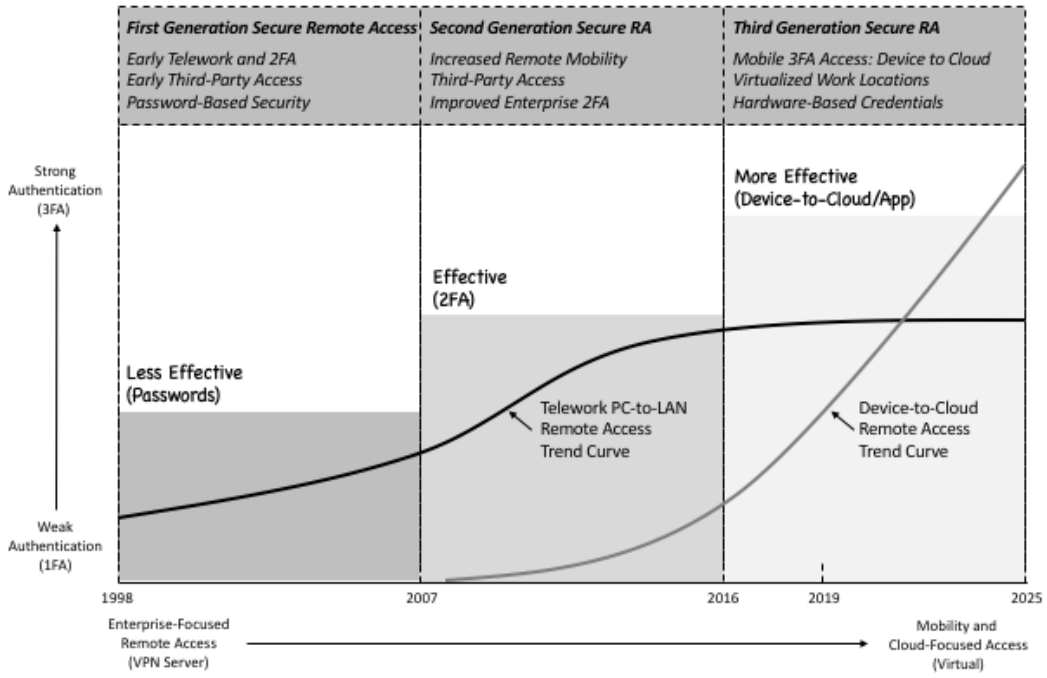


Figure 1-16. Secure Remote Access Trend Chart

The future of secure remote access lies in device-to-cloud, where mobility and embedded controls ensure that authentication, encryption, and integrity are in place. The use of public clouds to host enterprise applications will eventually remove the need for telework-based access to the corporate LAN. This function will remain in hybrid mode for several years, so traditional PC and laptop solution needs will remain in place during that transition period.

17. Anti-Malware Software

Perhaps the earliest successfully commercial computer security control was traditional *anti-virus software* loaded onto the Windows PC. Since its inception in the Nineties, this control has experienced uneven success detecting increasingly subtle malware, but has never wavered from its ubiquitous presence on endpoints. This stubborn application stems partly from compliance requirements, but also reflects advances made by security vendors in this area.

The original concept of anti-virus, now more commonly and more accurately referred to as *anti-malware software*, involved matching up known signatures with a scan of the operating system. Because these signatures were based on trivially side-stepped algorithms such as file names, variants became the scourge of the control. Vendors tried for many years to keep up through amazing diligence with malware samples, but this has not been an optimal strategy.

The good news is that the incredible experience and capability of the larger, legacy solution providers, combined with creative enhancements from start-ups and other security vendors, have resulted in much more impressive means to detect malware than the community might recognize. Behavioral heuristics and other powerful techniques have been used to expand the aperture for anti-malware software.

An additional powerful control has been the interactions anti-malware vendors establish between their deployed software base, and cloud security analytics used by their research teams. Samples can thus be sent to cloud for rapid analysis or even expert human review to determine a verdict on the file. This process has been streamlined to pseudo-real time in many cases, which is a welcome advance for enterprise security teams.

2019 Trends for Anti-Malware Software

First generation anti-malware solutions were effective in their early task of detecting viruses on PCs. Second generation anti-malware solutions were clearly less effective as variants abounded across the security community. Third generation anti-malware software solutions are demonstrating much more effective success at detecting exploits through a combination of better algorithms, cloud assistance, machine learning, and other techniques (see Figure 1-17).

The algorithmic trending for anti-malware has clearly shifted from traditional signature-based anti-virus to behavioral and more advanced machine learning analytics. Machine learning is particularly well-suited to training processes, including by humans, where examples of previous variants are used to help identify new variants (e.g., a simple prepend or post-pend of a single character to a known bad file name).

Virtualization also introduces new challenges and opportunities for anti-malware software. As cloud-hosted workloads require malware detection and mitigation capabilities, such protections are likely to begin to emerge in cloud security controls such as CASBs and micro-segmentation security systems. Cloud security compliance controls will increasingly drive specific anti-malware objectives for workloads and virtually hosted systems.

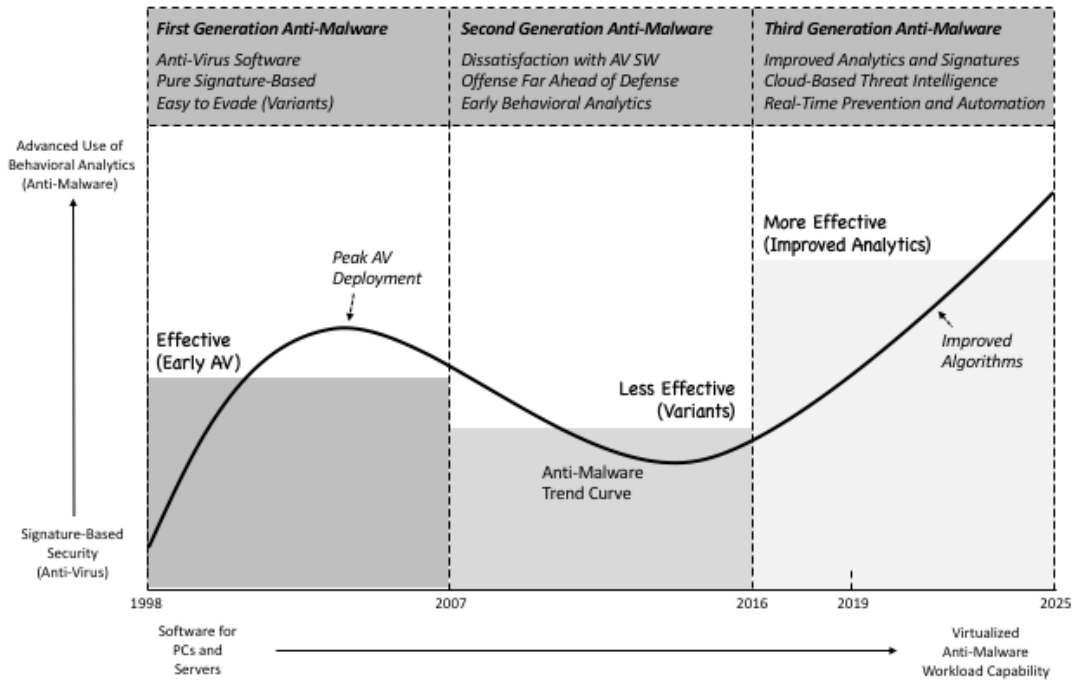


Figure 1-17. Anti-Malware Software

The future of anti-malware software lies in dramatically expanded use of AI and machine learning. In addition, more intimate real-time correspondence between anti-malware software located adjacent to an asset, and powerful cloud-based processing, perhaps crowd-sourced, will render immediate verdicts on detected samples. These advances will combine to continue the improvements in anti-malware software that have occurred.

One aspect of the anti-malware ecosystem that remains up for debate is the degree to which AI and machine learning techniques can remove the human being from the judgment equation – for both file-based and fileless malware detection. One would hope that at minimum, the automation would make this process mostly real-time, and thus minimize the likelihood that malware is causing damage while security teams are trying to perform human-time analysis.

18. Endpoint Security

The most complex, and arguably crowded, vendor space for cyber security involves the protection of *endpoints*. While such reference to endpoints is often generalized to include a variety of different devices, the sweet spot for cyber security vendors involves desktop and laptop computers that are issued and managed by enterprise teams for employees to use on the corporate LAN.

Endpoint PCs and laptops have traditionally been primarily Windows PCs, which have tended to be quite vulnerable to a variety of security exploits. Opening a malicious link via an email phish is generally viewed to be most dangerous when done on a corporate Windows PC connected to the enterprise LAN. In contrast, opening the same link on your personal iPad or iPhone is viewed as considerably less dangerous from a security perspective.

As such, most endpoint security solutions tend to target this general threat to PCs and laptops, with servers protected using other means. The commonality of methods stops there, however, as the field of endpoint security includes a complex, varied, and often confusing assortment of techniques, methods, agents, management systems, algorithms, and on and on. Enterprise security teams regularly express concern that endpoint security is tough to get right.

For most teams, the endpoints strategy can be viewed in three separate contexts: First, there is usually an installed baseline anti-malware tool, often from a major vendor such as Symantec, McAfee, or Kaspersky. Second, there is often an advanced, analytic-based security agent that is designed to either complement or eventually subsume the existing baseline tool. Third, there is the management system that supports installation, update, support, and the like.

2019 Trends for Endpoint Security

In general, endpoint security has evolved from less effective, first generation anti-virus solutions, through effective endpoint solutions in the second generation, toward more effective third generation solutions with many different advanced, integrated options (see Figure 1-18). The various evolutionary tracks include (but are not limited to) anti-virus (now anti-malware), data leakage prevention, user entity behavioral analytics, security containers, and isolation.

Across the board, these endpoint security techniques all benefit from the use of advanced heuristics including machine learning and AI techniques from the best security vendors. In addition, the assistance of cloud methods and automated tools for rendering rapid verdicts for potential malware samples, has dramatically improved currently-available solutions for keeping endpoints clear of exploit software.

The evolution of endpoint security has shifted during the three generations from simple security software point solutions toward comprehensive, integrated solutions. In addition, the basic support for early PCs running Windows operating systems has expanded to include more comprehensive support for a wide range of endpoint types including Mac OS, servers, mobile devices, IoT, and other endpoints.

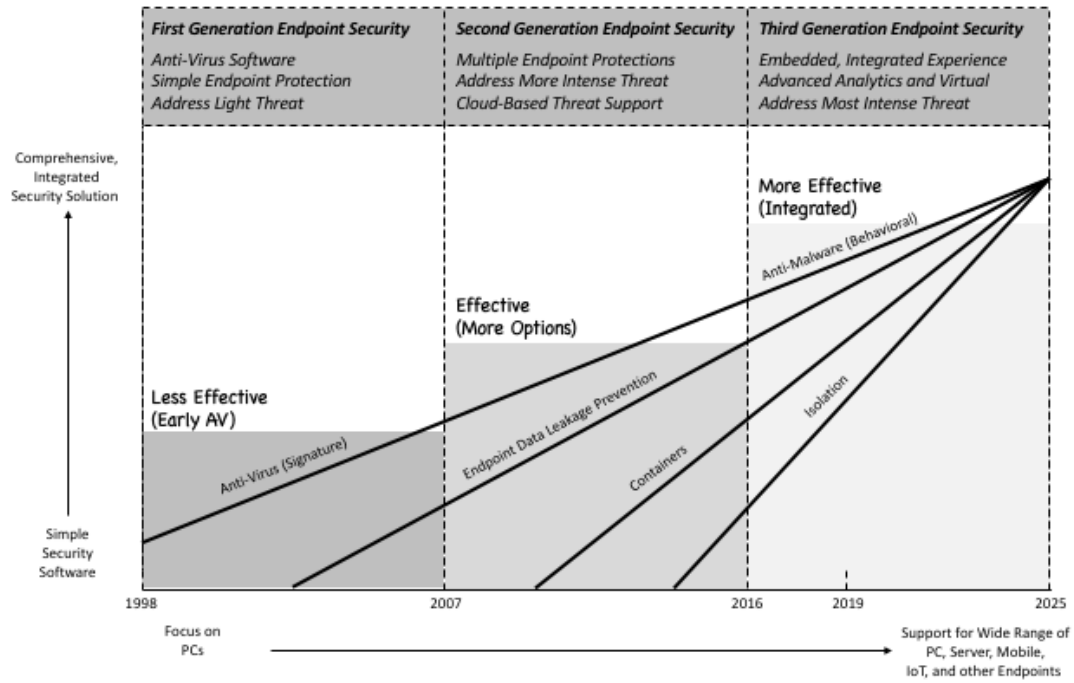


Figure 1-18. Endpoint Security Trend Chart

The future of endpoint security involves more intense use of AI and machine learning, simply because these technologies fit the problem of malware identification quite well. The essence of automated learning involves the use of live or test samples as the basis for detecting future instances of the same thing, albeit slightly modified (like different pictures of cats). This will substantially reduce the risk associated with endpoints.

An additional future trend will be massive consolidation of the disparate means for protecting endpoints. One should expect a continuing flurry of mergers, acquisitions, and partnerships that will result in more embedded, user-invisible endpoint security solutions that will be cost-effective, easy to use, and much more suited to the progression of enterprise computing toward mobility-enabled hybrid cloud usage.

19. Hardware/Embedded Security

It is fashionable in this era of virtualization and software-defined everything, to say that *hardware and embedded systems* are no longer relevant in modern computing – and that if any desired function can be implemented in software, then it should be done in that manner. What this view misses, however, is the optimal design balance that seems a more reasonable goal between hardware and software.

Security experts *should* be explaining that hardware is best deployed when high levels of *performance* and *assurance* are desired, and these are not uncommon requirements in most settings. The use of hardware should this be viewed in terms of optimal usage, rather than as being supplanted by software running solely on generic CPUs, arranged row-like and ready to be replaced with new appliances when they need update or show signs of wear.

The security community benefits from hardware in the following areas: (1) Embedded endpoint and mobile device hardware such as Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) for high assurance; (2) optimized hardware for specialized applications such as browser or IoT isolation; and (3) hardware appliances for ultra-high performance requirements. In each case, the hardware plays an important role in achieving desired security objectives.

It is also worth mentioning that various creative solutions in cyber security have tended to utilize an attractive balance of hardware and software in their implementation. Everything from DDOS mitigation to high-assurance remote browsing can benefit from the judicious and careful integration of hardware into the design. The clear advantages of using software for most cases does not preclude hardware being a great choice in certain instances.

2019 Trends for Hardware/Embedded Security

First generation use of embedded hardware for security was effective and consistent with the threats and technology of the time. Second generation cyber security saw a clear shift and bias away from hardware toward software, but the result was less effective for many reasons – most unrelated to the shift away from hardware. Most of the shortcomings stemmed from significantly increased attack methods with increasingly reliance on perimeter.

Stated another way – the speed with which cyber threats began to progress in the late 90's and early 00's, made it clear that the rigor and capacity associated with hardware might not be sufficiently vital to justify the relative inflexibility of making changes quickly. As a result, software – even with its myriad of familiar exploitable bugs – became a more attractive option for most security controls. This accounts for the effectiveness dip experienced during this era.

Present third generation use of hardware and embedded means for reducing cyber risk generally includes a more effective and balanced mix of hardware and software – taking full advantage of the primary strengths of both (see Figure 1-19). Higher assurance and performance requirements have gradually shifted as the main motivations for selecting hardware security implementations over corresponding software-based designs.

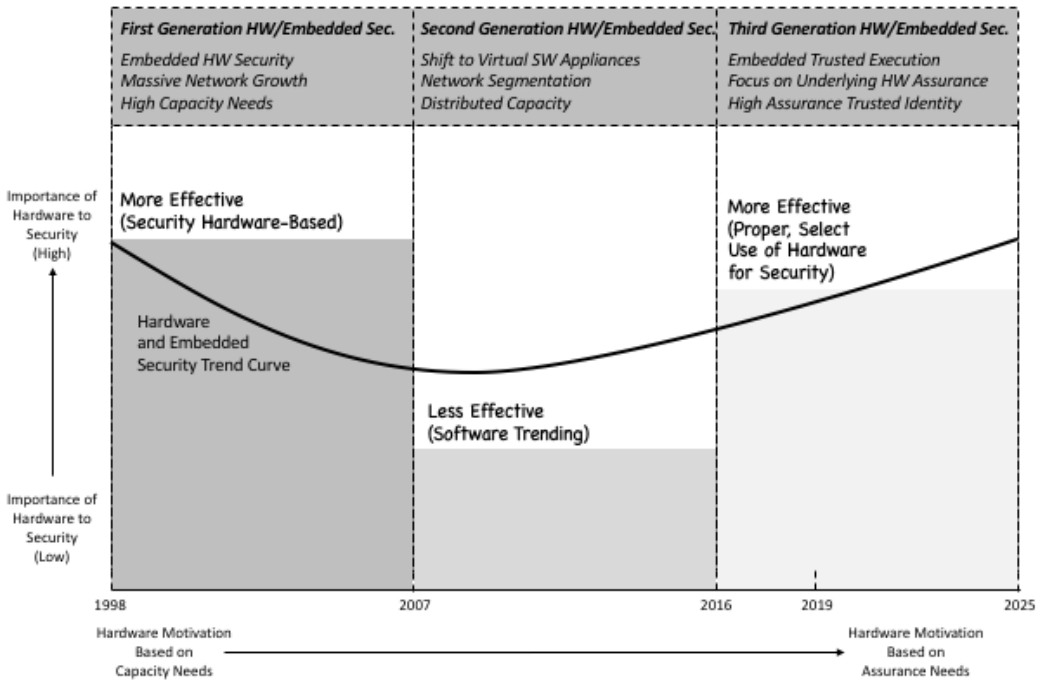


Figure 1-19. Hardware/Embedded Security Trend Chart

The future of hardware/embedded security will continue to involve optimal design and implementation balance with software. The growth of operational technology (OT) and Internet of Things (IoT) will also drive this balance of software with embedded security. New IoT devices, for instance, should include functional protections at manufacturing time, and this will often involve embedded hardware implementations that coordinate with software controls.

20. ICS/IoT Security

The distinction made here between *industrial control system (ICS)* and *Internet of Things (IoT)* is that ICS includes devices associated with highly consequential impact upon breach, including life and safety-critical implications. IoT devices, in contrast, are essentially in-band IT devices that support innovative new functions such as recognizing voice commands, controlling consumer items, and providing entertainment and fun for citizens.

While it might seem controversial to some, we choose to focus our main emphasis here on ICS security as a unique situation – and to treat IoT devices as endpoints that require the same types of IT protections as other endpoints, including mobile devices. This follows the observation that ICS has its own unique technologies and support systems, and the security consequences are typically enormous.

In fact, technology experts will agree that ICS security (and select IoT) represents one of the greatest new challenges for data and system protection. The security obligation here focuses specifically on operational environments such as factory floors, manufacturing plants, embedded systems, machine designs, robots, drones, mart weapons, connected cars, wind turbines, and many other aspects of societal and national critical infrastructure.

ICS security has been challenged for a couple of reasons: First, legacy ICS infrastructure barely took cyber threats into consideration at design time – a decision reinforced by many years of quiet time in terms of cyber threats. (Note that almost all IoT is non-legacy.) And second, the various ICS technologies and protocols employed are inconsistent with standard IT methods, which made generally available commercial tools largely unusable for ICS in OT environments.

Neither of these conditions have changed, but the attention placed by both malicious offenders and industrial defenders has increased considerably. This is mostly because the offense became more active, largely due to the high consequence and enormous gain achieved by successfully breaching an ICS system. In the gravest cases, OT exploits can lead to significant loss of life, which might be the objective for a truly evil actor involved in a diabolical cyber initiative.

2019 Trends for ICS/IoT Security

First generation ICS security from 1998 to 2007 was arguably non-existent in almost all OT environments, with some larger early adopters as exceptions. Second generation ICS security from 2007 to 2016 introduced some effective early solutions, albeit with uneven adoption and deployment. Third generation ICS and IoT security from 2016 to 2025 will involve more effective solutions deployed uniformly across industrial and IoT environments (see Figure 1-20).

A major trend in this evolution involves stand-alone, hardware-based ICS and IoT security solutions shifting toward more virtual, cloud-based protections for both ICS and IoT. In addition, proprietary ICS and IoT protocols and systems are being gradually replaced with open, standard-based protocols and systems for cyber security. The convergence of IT and OT will drive greater deployment of common, standard security solutions.

Security solutions for ICS and IoT have tended to fall into several different categories: Some systems focus on managing direction of flow between IT and OT; others focus on enforcing policy at gateways between IT and OT; and still others embed their controls directly into OT devices and systems at the lower layers of the familiar Purdue model. These methods are complementary but have not been typically well-integrated in OT environments.

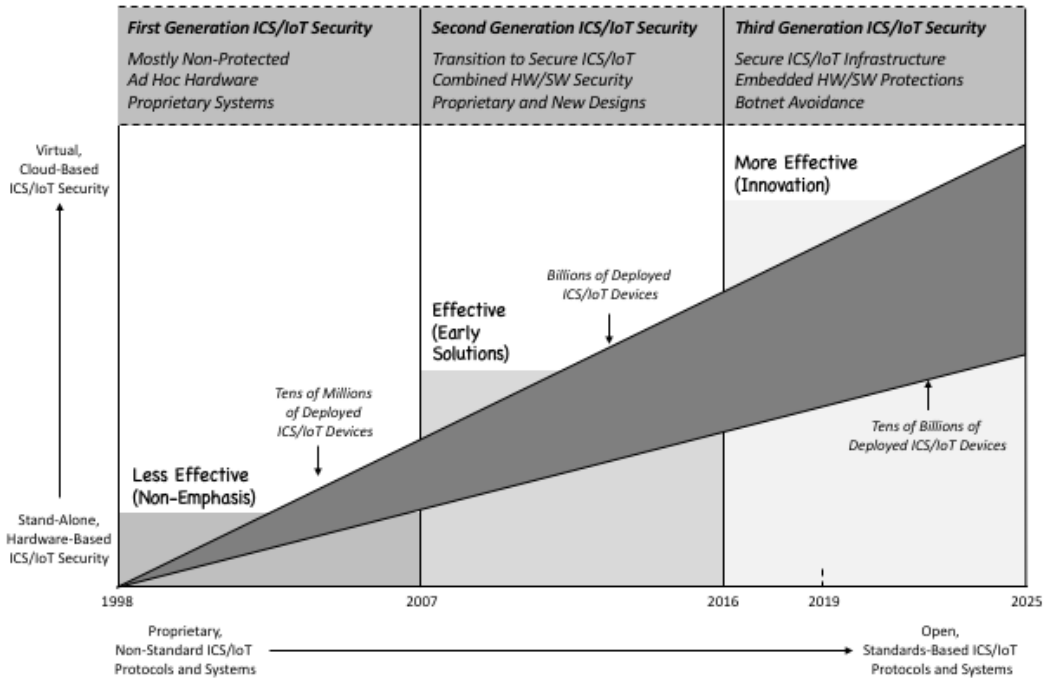


Figure 1-20. Industrial Control System Security Trend Chart

The future of both ICS and IoT security lies in the convergence of IT and OT. That is, increasingly cyber security protections will not require redesign for non-IT usage, but will rather operate natively. This implies that OT infrastructure will shrink around the devices they currently manage, and most of the computing and networking supporting ICS and IoT devices will be based on standard IP protocols and technology.

21. Mainframe Security

It is tempting to ignore mainframe security as being long gone, but the reality is that many companies and agencies continue to rely on mainframes and their applications. Reasons vary, but the core issue is that inertia is a powerful driver of infrastructure support, and many IT, software, and network teams have decided that it is simply easier to just leave the mainframes in place, than to swap them out. This will shift with time, but it remains true today.

The resulting challenge is that traditional mainframe security protections, including tools for data governance, encryption, transfer, and audit, remain in place and require time and attention. The experience and skills of people trained to perform such mainframe-based protection are beginning to seriously wane – and it is conceivable that the skills shortage (through attrition and retirement) will be the final driver to shut down mainframes.

One great irony with respect to *mainframe security* is that the associated centralized concept of amortizing the best available mainframe administration and protection talent into one place is closely related to modern cloud security processes. In fact, it is not uncommon for pundits and observers to draw direct comparison between cloud security and the earliest efforts at mainframe security.

An additional irony is that during the heyday of mainframe security – perhaps during the mid-1970's through the mid-1990's, one could easily make the case that the associated cyber threat was far less intense than it is today. Now, most experts would (correctly) view this as primarily driven by the relative immaturity of offensive techniques; but one should not ignore or even discount the fact that when mainframes ruled, security problems were less intense.

2019 Trends for Mainframe Security

The effectiveness of mainframe security has been high from its inception to the present. Few would argue that mainframe controls have been weak, although the processes and policies of early enterprise were, in fact, poorly done (see Figure 1-21). The percentage of security infrastructure focused on using mainframe security tools has gone from moderate/high to very low, and many would refer to mainframe protection as a "dying art."

The corresponding consulting fees that can be obtained from the remaining mainframe experts should be expected to rise dramatically, as companies continue to rely on these systems without the abundant availability of administrators who know IBM z/OS and the like. Enterprise teams are thus advised to accelerate retirement of their mainframes to avoid the need for costly consulting fees.

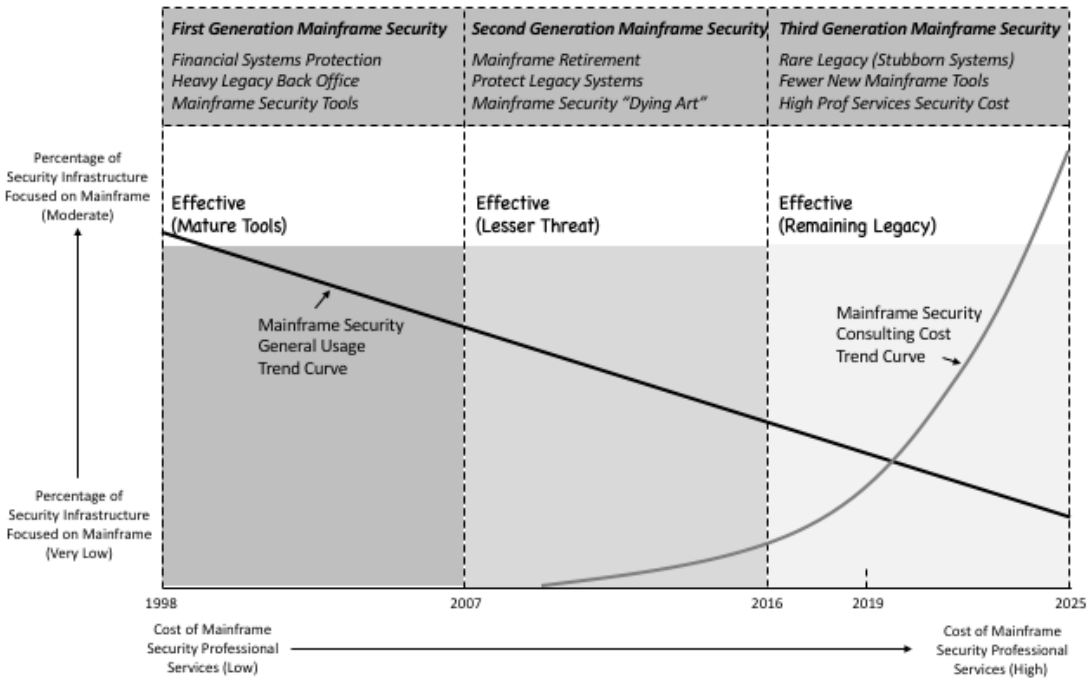


Figure 1-21. Mainframe Security Trend Chart

The future of mainframe security lies mostly in some technology museum. Future versions of the TAG Cyber Security Annual will likely drop this control from the fifty, but it remains today, simply because so many larger companies continue to run mainframes. Government agencies apparently have quite a few mainframes as well, and presumably IBM and others will continue to support this business, which is likely to be quite high margin.

22. Mobile Security

Mobile security has shifted from an optional consideration for smart devices that provide conveniences for workers, to a mandatory requirement for all mobile devices, systems, and infrastructure that support essential business operations. This is a dramatic shift – one that is mostly accepted by business and government teams around the work. Vendors have obviously noticed this shifted emphasis on mobile protection, and are offering a portfolio of solutions.

A curious and somewhat nagging issue, however, is that far too many businesses, especially smaller ones, still opt to manage their mobile devices through services such as Apple iTunes, with little or no consideration to additional cyber security. Biometric unlocking becomes a primary control in such environments, which is fine to reduce the risk of lost devices, but insufficient to deal with post-login exploits such as embedded malware.

The history of cyber security strongly suggests that with all the emphasis on mobility, and its central role in access to cloud-hosted enterprise applications (e.g., Google's BeyondCorp model), that the associated risk will increase as malicious intruders find creative ways to exploit even the best designed software from companies like Apple. Enterprise teams who do not recognize this inevitable fact operate at their own peril.

It is also imperative to observe that the walled-garden approach taken at Apple, which ensures that all downloaded apps are passed through and vetted by Apple, has resulted in a relatively secure processing environment. It is not uncommon, for example, to hear security teams recommend that executives open their email (which might include dangerous attachments) on their iPhones versus on their LAN-connected Windows PCs.

2019 Trends for Mobile Security

Mobile security has transitioned from weak controls in the first generation of use from 1998 to 2007, to effective controls in the second generation from 2007 to 2016, to more effective and integrated controls in the third and present generation (see Figure 1-22). This evolution has been characterized by a shift from weak device and system protections to much stronger protections based on more solid foundational components.

Early mobility security was viewed largely as a complement to the traditional PC/LAN enterprise infrastructure. That is, most business users in the early days of mobility viewed their flip phones and early Blackberry devices as a nice-to-have convenience, but certainly not as a critically essential component of their day-to-day work experience. This is reflected by the largely fixed, stationary, non-mobile nature (with cubicles) of the typical office environment of the time.

Modern mobility security, in contrast, is viewed as an essential basis for the emerging cloud-based virtual work environment. What used to be called telework is now simply called work; hence, the threats to any enterprise team will now increasingly encompass traditional PC and computing assets, as well as mobile devices – whether bring-your-own-device (BYOD)-managed or company issued. It should come as no surprise that threats will continue to shift accordingly.

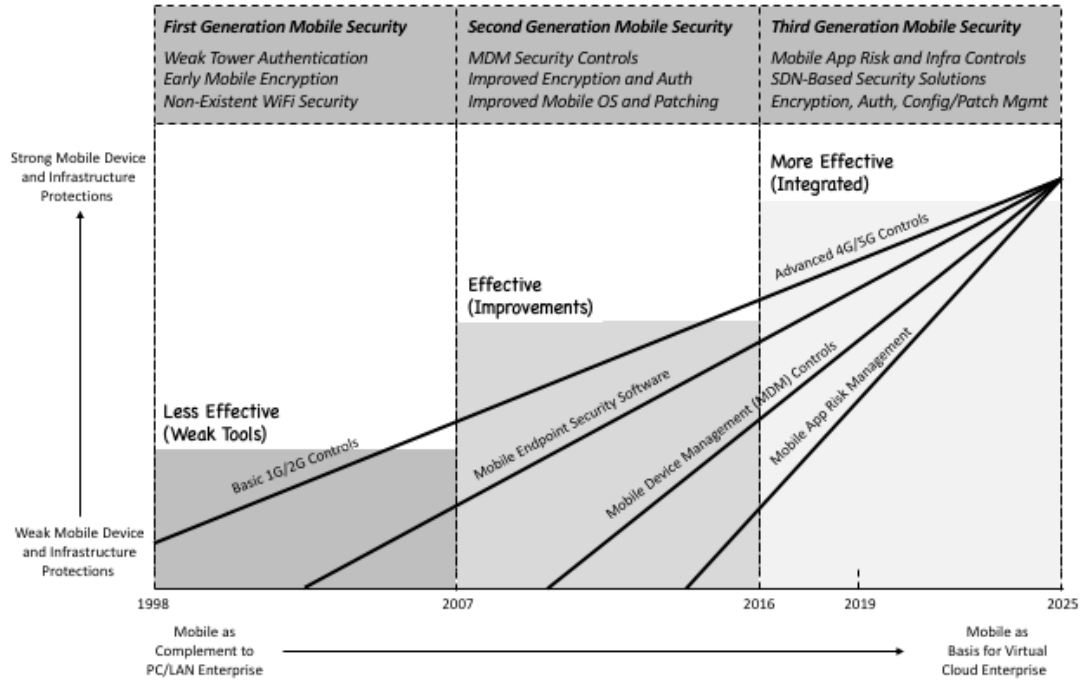


Figure 1-22. Mobile Security Trend Chart

The future of mobility security is an integration with traditional enterprise security. That is, one should expect that mobility will become an assumed component of every enterprise, regardless of size, scope, or mission. This is good news, because teams will soon no longer view mobility security as an add-on to their protection scheme, but rather as an integrated, embedded element in their security approach.

23. Privilege/Password Management

Decisions about passwords have traditionally been left in the hands end-users who often make colossal errors in judgment in their selection, use, and sharing. When this involves passwords for critically essential resources in an enterprise, we often refer to the authentication information as a privilege. As one might expect, mishandling or poor decision-making with privileges can lead to more serious consequences.

To deal with both problems, *password management* and *privilege management* tools have emerged that simplify the corresponding tasks. (Commercial vendors often market tools for one or the other tasks, but quite often not both.) Whether for consumers or enterprise users, and whether for passwords or privileges, the general idea is that an automated tool simplifies the interface to the user, and then securely manages back-end authentication usage and handling.

Both privilege and password management tools are getting easier to use, more commonly accepted, and better integrated into the usage patterns of consumer and enterprise users. Secure constructs such as password and privilege vaults, for example, are becoming more frequently cited in enterprise security policy requirements, and even showing up in security compliance frameworks.

One challenge to the use of secure vaults involves the complexity and challenge of ensuring proper coverage across all privileged passwords for all relevant applications. To that end, vendors have begun to build solutions that focus on the process of privilege management without need for a vault. Generally, two-factor authentication is an important element of this and all password and privilege management schemes.

2019 Trends for Privilege/Password Management

First generation privilege and password management involved early tools that were not as well-understood by customers as they are today (e.g., CyberArk was founded in 1999). Second generation from 2007 to today saw considerable usage and security improvements; and third generation tools will become even more effective, as machine learning and advanced analytics find their way into the algorithms and utilities (see Figure 1-23).

The trend for both password and privilege management can be summed up pretty-well by the transition from simple, stand-alone administrative tools to more advanced, analytic controls, especially in the context of enterprise use. The capabilities are becoming more embedded into identity and access management (IAM) infrastructure, and even emerging Internet of Things (IoT) authentication and authorization.

Both capabilities will also benefit from increased use of cloud and virtualized as-a-service computing, if only because these emerging services increase the demand for non-homogeneous authentication and authorization for consumers and enterprise users. One might thus expect to see password and privilege management support integrate with cloud security solutions such as cloud access security brokers (CASBs).

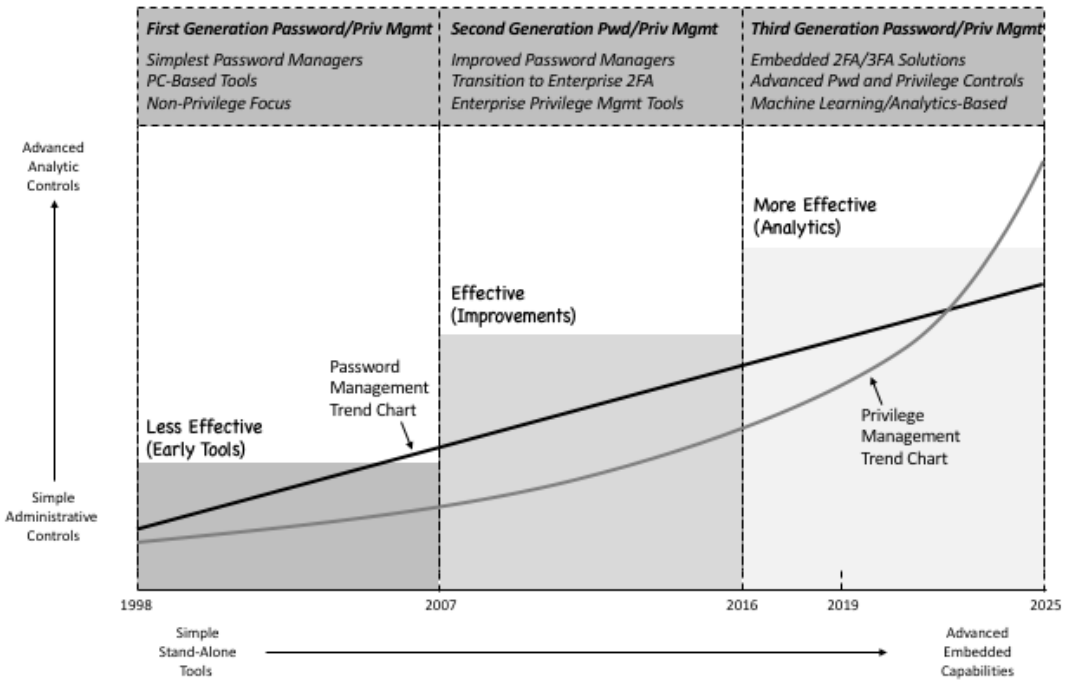


Figure 1-23. Privilege/Password Management

The future for privilege and password management continues to be positive, with privilege management tools in the enterprise likely seeing exponential growth due to increased demands from a compliance perspective. Password management is likely to see continued linear growth, as the typical consumer will remain somewhat uncertain about the best way to manage passwords, often just utilizing federated authentication between social media sites.

It is worth mentioning here that a great debate exists within the security community about whether a true password-less experience is a reasonable and attainable goal. This debate is somewhat orthogonal to the password and privilege management functions, as these capabilities will travel with whatever contextual or adaptive credential validation is in use by enterprise and consumers in the coming years.

24. Multi-Factor Authentication

The use of *multi-factor authentication* for the validation of a reported identity is now accepted as a basic tenet of cyber security. Most enterprise applications now require at least two factors for access, but the selection of such factors involves every combination of proof methods one can imagine. Some users might need a password and biometric; others might use a password and mobile text code; others might use a certificate and device identifier; and so on.

Such diversity of factors is a defensive advantage from the perspective of complicating matters for offensive actors, and most users will tend to settle into whatever authentication cadence they've been asked to learn. Furthermore, most proof factors have become surprisingly easy to provide (or derive); thumbprint biometric use on the mobile, for example, is trivial for anyone to use and offers a valuable initial proof factor.

Most development teams and solution vendors would prefer to see a standard-based approach to authentication. Groups such as FIDO (Fast Identity Online) are developing globally and supporting a common framework to address this interoperability for stronger forms of user authentication. The FIDO group, specifically, has gained traction and has the support of many heavy-hitting organizations.

It is also generally accepted in the community that *contextual authentication* that senses relevant environmental attributes is a valuable goal. Furthermore, *adaptive authentication* that dynamically adjusts to these sensed attributes offers a more dynamic means for users to be authenticated, and holds promise that eventually, multi-factor authentication might require zero action on the part of the user.

2019 Trends for Multi-Factor Authentication

The use of multi-factor authentication has been effective through all generations of usage, but has become even more effective in this third and present generation. The emerging adaptive, contextual solutions that are more standards-based have come a long way from the early hand-held tokens that emerged in the industry decades ago, and that were so dominant in the industry for many years (see Figure 1-24).

The most obvious transition has been from a single, add-on, second factor – such as handheld tokens – to the use of advanced, adaptive, contextual authentication. Adaptive authentication deals with the dynamic nature of behavioral activity, whereas contextual authentication provides complementary use of the specifics of a given authentication challenge, including attributes such as location, device type, and user behaviors.

The ease-of-use for strong, multi-factor authentication has come a long way, with clumsy fumbling around with often-lost physical tokens to cleverly integrated solutions that do not cause great additional work for users. Ease of administration is also a clear trend, especially as standards-based solutions begin to emerge. More recently, the best vendors have also included decentralized storage to reduce the risk of credential compromise against central stores.

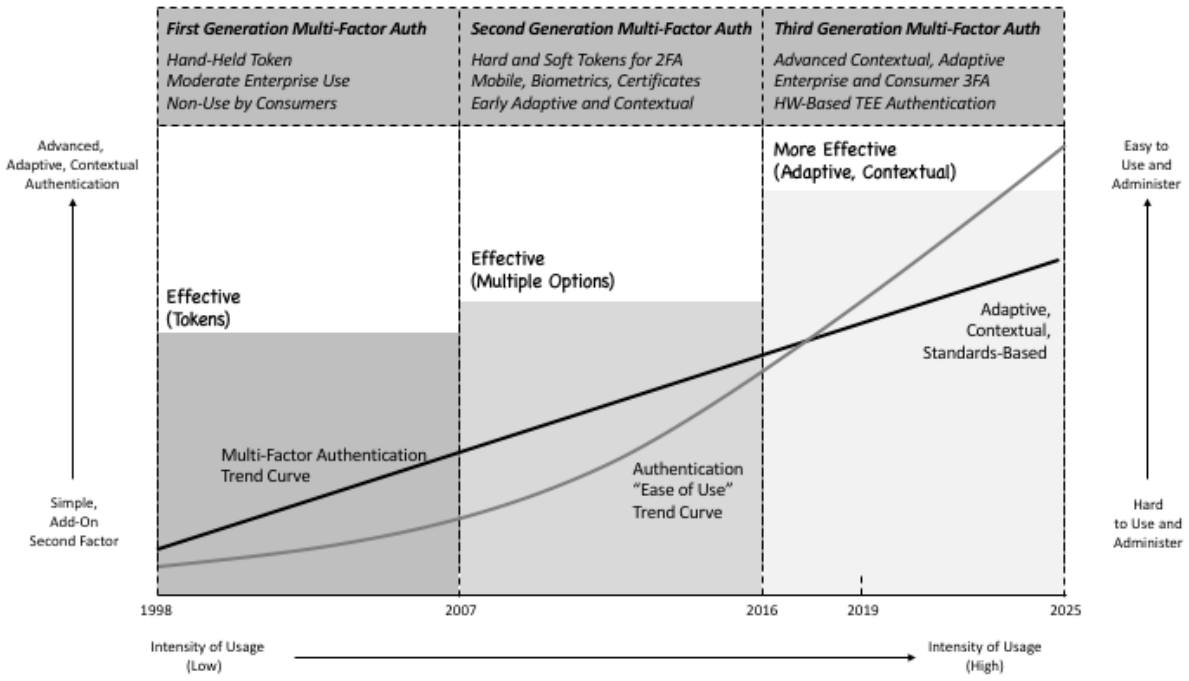


Figure 1-24. Multi-Factor Authentication Trend Chart

The future of multi-factor authentication involves improved security through decentralization (including for authorization), as even greater introduction of embedded contextual and adaptive proof. The extension of stronger authentication to Internet of Things (IoT) and operational technology (OT) has also begun and will accelerate as these initiatives continue to develop.

One should also expect in the coming years a more intense effort to integrate artificial intelligence and machine learning into the adaptive, contextual process. This will naturally complement more decentralized methods for handling authentication and credential information, and should result in highly secure, highly accurate authentication with a minimum of obligation for users.

25. Voice Security

Most enterprise security teams have tended to forget that, over the past few years, voice communications have become increasingly mobility-based, and increasingly vulnerable to a range of new cyber threats. While it is true that the conventional public switched telephone network (PSTN) was less directly vulnerable to modern IP-based attacks, this claim simply cannot be made about modern voice services, especially when using mobiles.

The good news is that mobile service providers have tended to do a good job improving their underlying communications infrastructure protections toward enhanced *voice security*. Encryption algorithms have improved, as have the basic voice service infrastructure elements, often due to compliance pressures. So, the challenges to voice security are not as severe as they might be – but enterprise teams should recognize the risk and take immediate action.

Voice security tends to fall into three categories of concern: (1) Encrypting traditional and mobile voice communications when the threat has great potential consequence (e.g., when senior executives travel); (2) Protecting voice communications from eavesdropping at the infrastructure level (e.g., SS7 vulnerabilities in traditional infrastructure); and (3) Ensuring robust, highly-available services for critical applications including first responders.

References above to voice security can and should include adjacent references to texting, messaging, and other forms of over-the-top (OTT) communications. Increasingly, voice-over-IP (VOIP) and related means for speaking with friends and business associates using Internet connectivity (most often involving open WiFi service somewhere in the communication) has become the norm. Voice security for OTT is thus more imperative than ever.

2019 Trends for Voice Security

Through the three most recent generations of voice security, the associated controls started with mostly effective PSTN controls, through less effective early security for Voice-over-IP (VoIP) and mobility, toward the current generation, where excellent over-the-top (OTT) encrypted voice solutions and improved underlying infrastructure controls give enterprise teams good options (see Figure 1-25).

While the intensity of voice attacks is becoming ever more intense, many CISO teams have been surprisingly passive (or ignorant) regarding this threat. The transition from landline PSTN toward emerging 5G mobile services with its largely SDN-powered infrastructure offers greater flexibility for introducing new security for voice. But this is only true if security teams select the best OTT solution for mobiles, especially for traveling executives.

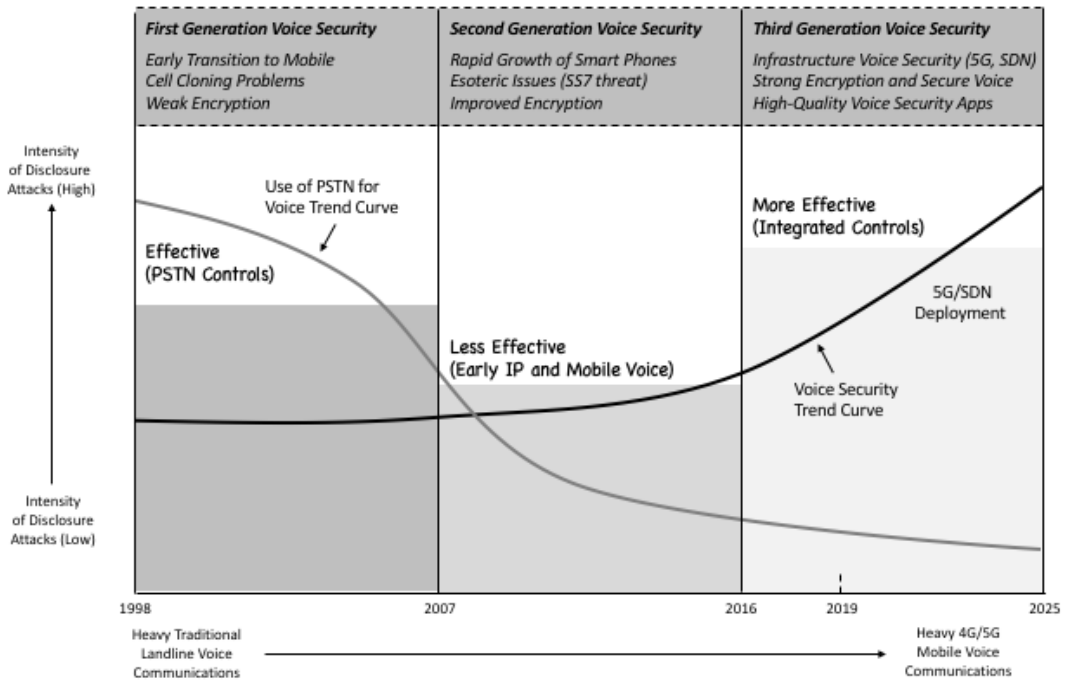


Figure 1-25. Voice Security Trend Chart

The future of voice security will be heavily focused at the application OTT level with end-to-end encryption providing round trip protection between endpoints. This will be true for mobile, VoIP, and application-based communications such as conference bridge and video conferencing utilities, which are generally non-encrypted today. Compliance controls for secure voice are likely to increase in their intensity as well.

It is worth saying that in the coming years, voice leaks are likely to play an important role in the transition of voice security from an add-on to an essential strategic component of every CISO's operational playbook. When senior executives start to see their voice communications on WikiLeaks and other Internet-facing sites, the demand for encrypted OTT applications for voice will grow accordingly.

26. Digital Risk Management

Digital Risk Management might be the greatest control in the enterprise that is *not* properly addressed directly by most enterprise security teams. This lack of security attention – and an exception could be argued larger organizations such as banks and telecommunications firms – is surprising, because fraudulent activity affecting and negatively influencing brand have increased considerably.

The most common digital risk and brand-related attacks involve domain misuse, hijacking, and other business identity-related breaches and fraudulent actions. This can involve the use of adjacent domains to spoof identity for phishing, or even domain squatting for illegal impersonation of a business – but in all cases, the attack techniques used range from subtle action to blatant use of obviously spoofed domains.

Two reasons such brand and reputation protection functionality have been less prominent with security teams to date include: First, a brand is an intangible asset – one that cannot be easily embraced, catalogued, and financially valued (unless you are Coca-Cola or Google). Second, recent data breaches suggest to some observers that even after a major breach, brand reputation rarely suffers and companies tend to bounce back (e.g., Home Depot, Target).

These arguments should hopefully ring hollow to the cyber expert, simply because a stronger case can be made that attackers have only scratched the surface of the negative reputational impact that can be brought about by successful breaches. The Democratic National Committee is an example of an organization deeply wounded by their attacks – many of which involved brand-related attacks.

The most common solution for protecting brand involves this new discipline now known as *digital risk monitoring*. In short, the approach relies on a comprehensive, all-source gathering of past and real-time information about an organization. This can include deep investigative collection across the surface, deep, and dark web infrastructure. The goal is to detect evidence of fraudulent activity, and the industry has produced some excellent tools and offerings.

2019 Trends for Brand Protection

The effectiveness of brand protections has evolved through three generations of use from less effective early techniques, including trying to deal with early screen scraping, to more effective techniques that use advanced analytics in the context of digital risk monitoring solutions. The maturity of digital risk monitoring, including user interfaces and skill-sets of risk researchers on the surface, deep, and dark web, has increased commensurately.

In addition, the focus brand protection has shifted from a sole focus among marketing and brand management teams who were concerned with brand degradation from non-cyber origins, to now include focus from security teams who worry about brand degradation by malicious adversaries engaged in deliberate acts. Such combined focus has yet to include full merging of marketing and security budgets, but this might happen in the future.

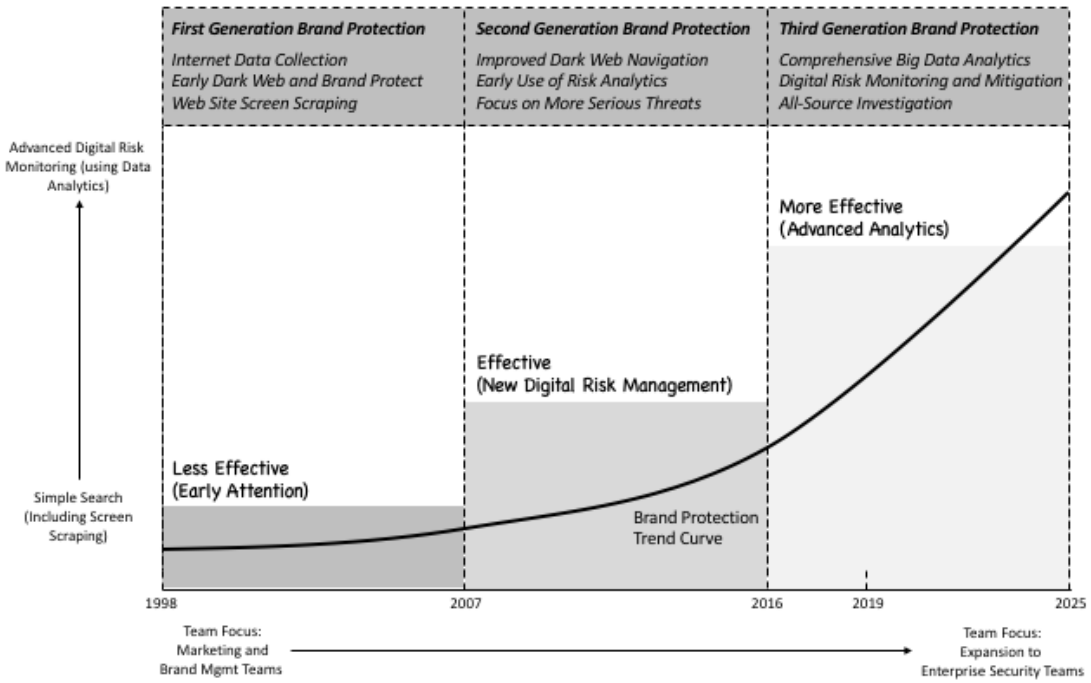


Figure 1-26. Brand Protection Trend Curve

The future of digital risk management lies in the convergence of interests between corporate brand and marketing teams, with zero understanding of security, and the cyber security teams, with less understanding of marketing interests, but who certainly understand cyber threats. The resulting interdisciplinary approach to digital risk will be one of the more effective controls in the future enterprise.

27. Bug Bounty Services

The use of *bug bounty* programs began with the largest companies in the world – Google, Microsoft, AT&T, and so on – deciding that it was in their best interests to work with, and reimburse security researchers targeting their corporate infrastructure. It was a good example of practical and reasonable *if-you-can't-beat-'em* then *join-'em* thinking amongst these corporate security groups.

The original bug bounty programs were mostly in-house, but the security community quickly made available a collection of excellent options for a managed, outsourced, or crowd-sourced bug bounty and vulnerability management services from vendors. One attractive approach involves the use of a vetted community of hackers who carefully and appropriately probe and scan target infrastructure. The results are useful and cost-effective.

For buyers looking at vetted research communities, it makes sense to carefully review the steps followed to determine who can be part of the testing crowd and who cannot. This is an important differentiator, because if you can locate a great crowd that is capable, vetted, trustworthy, and also well-trained to find exploits, then you will have an excellent resource for your security program.

Increasingly, mid and even smaller-sized companies are putting bug bounty and vulnerability management programs in place with vendors. The result is that more exploitable holes are being detected sooner by white hat hackers than would have previously been quickly identified by black hats. Obviously, all bug bounty and other testing programs cannot find every problem, but the approach pays off well in most cases.

2019 Trends for Bug Bounty Services

Bug Bounty programs in the first generation were mostly ad hoc, in-house programs with uneven results and unclear reimbursement economics; second generation bug bounty services improved the overall effectiveness, and modern, third-generation solutions are more effective, mature, and attractive to a variety of different companies in all sectors (see Figure 1-27). Even government agencies are using bug bounty services as a risk reduction measure.

The general trend has been from reactive responses to issues through researcher detection toward more proactive testing to prevent problems from occurring. This requires that staging and pre-deployment systems be subjected to bug bounty and vulnerability testing. An additional trend has been from simple reimbursement of researchers for bugs found to a more relationship-oriented program of cooperative trust.

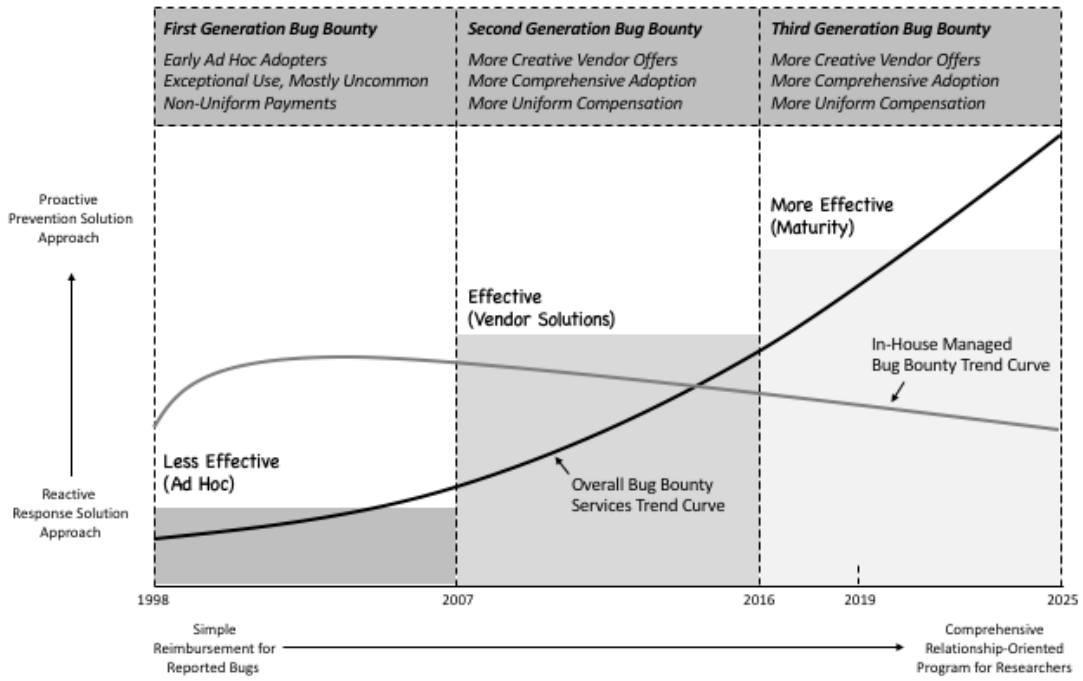


Figure 1-27. Bug Bounty Services Trend Chart

The future of bug bounty services lies in more trusted relationships with vetted groups. To date, much of the work delegated to crowd-sourced testing has tended to be the Internet-facing infrastructure, simply because the external trust model need not be adjusted. In the future, however, bug bounty service providers will be given special, trusted access to more sensitive applications and systems, in many cases, prior to their production deployment.

28. Cyber Insurance

The *cyber insurance* marketplace has been an obviously vibrant aspect of our industry, with growth, excitement, and buzz surrounding the emergence of significant new business in this area. Board members and executives like the idea of risk transferal via an insurance policy, and CISO teams have tended to be fine with the purchase of a policy – so long as the premium payments do not come from the enterprise security operating budget.

This budgetary issue is a major consideration, of course, because CISOs would never select a policy over the purchase of a functional solution – and this should be obvious: Ask any CISO if they would prefer budget for ten new staff or for a cyber insurance policy – and I think you can guess the answer. Once (or perhaps, *if*) financial responsibility for insurance premiums shifts to the operational security teams, then expect growth in this area to subside quickly.

That said, the bottom line in cyber insurance is that no one – and that means *no one* – has much grasp on the correct financial risk equation to determine the optimal premium/coverage ratio. Instead, what tends to happen in 2018 and into 2019 is that insurance companies cover as little as they can, with premiums that are as high as they can sell. This is obviously how all insurance works, but buyers of traditional policies have more data to help them negotiate.

Here is an example of the challenge to writing cyber insurance: We all know that it would be highly unlikely (except in the Biblical circumstances) for a severe hurricane to hit on the same day in every US city with an NFL football team. So, writing hurricane insurance does not need to account for this impossible scenario. In contrast, any cyber expert can attest that a cyber attack can easily hit every NFL city in the same *instant* – and this influences the details of policies.

2019 Trends in Cyber Insurance

The effectiveness of cyber insurance is best measured in its ability to properly transfer risk in a meaningful way from the team being insured to the insurance company. First generation policies were less effective because premiums were too high and coverage too low. Second generation policies were better, and third generation cyber insurance is already beginning to show signs of more effective risk transferal (see Figure 1-28).

Trends include a shift from varying policy specifics across different insurance companies toward more converged insurance offerings with a common, predictable equation for calculating premiums and coverage. Buyers will shift from making ad hoc decisions about cyber insurance, toward making more informed and mature decisions about what to buy. This maturity will hopefully extend to the executive team and corporate board.

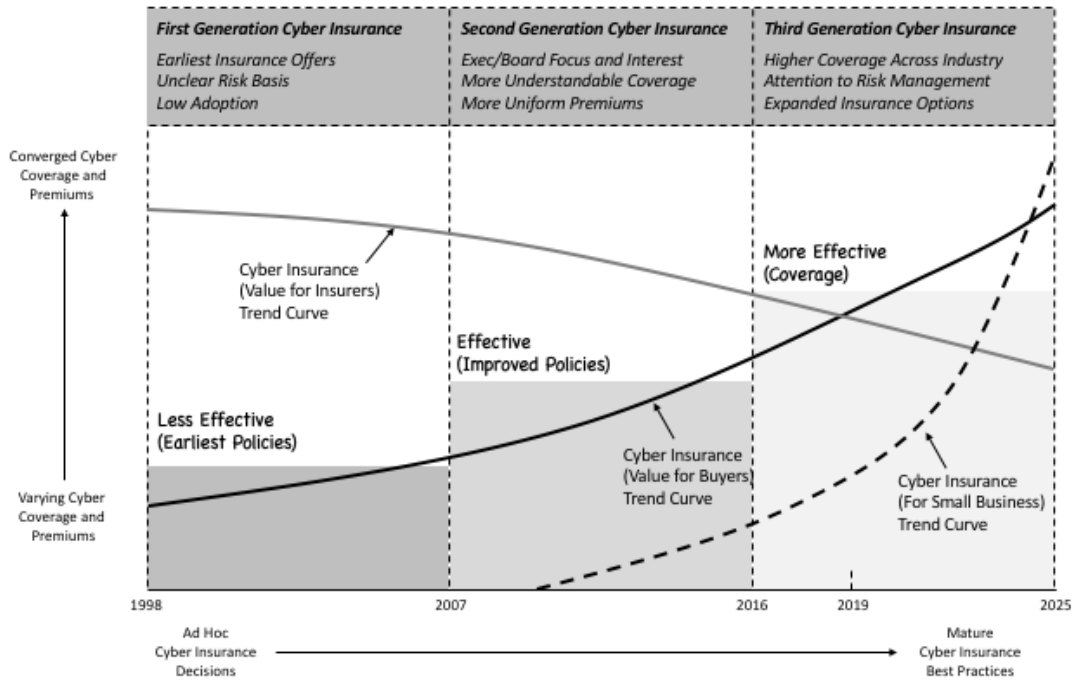


Figure 1-28. Cyber Insurance Trend Chart

The future of cyber insurance can be summed in three basic themes: First, the buyer will gain increasing value in both risk transferal and improved coverage for lower premiums; second, the insurers will see decreasing value, but will see increased business volumes; and third, small businesses will begin to buy cyber insurance policies at increasing levels, potentially becoming the bulk of the insurance industry growth.

29. GRC and Risk Management Platforms

A promising development in cyber security in recent years is the improved and more frequent use of automation in the establishment, maintenance, and support of *governance, risk, and compliance (GRC)* objectives. To support this desire for automation, commercial GRC platform usage has exploded well beyond use by the pioneering adopters of crude, early tools. This is good news for the cyber industry, as it results in dramatically improved GRC processes.

Some excellent advances in GRC and risk management platform support include more integrated and embedded collection of data from business unit processes, more extensive coverage of DevOps software processes, and improved reporting of GRC issues to senior executives and boards. Each of these platform advances has come from practical usage-based requirements, so this is additional evidence that GRC is a mainstream tool in business.

Mid-market and SMB organizations have tended to not utilize GRC and risk management platform solutions at the same rate, however, presumably because their governance issues are less intense. With compliance demands increasing, however, one would expect to see GRC platforms moving down-market and more into as-a-service environments. This trend should be present across all sectors and will include government and academia as well.

An additional trend one would hope to see involves less emphasis on introduction of new compliance frameworks in response to political or public pressure after an incident. The idea that cyber incidents are best handled by some state, or interest group, or nation, or even company – introducing a new set of compliance requirements is gradually becoming extinct. This is good, because existing frameworks are sufficient; it's the execution that matters.

2019 Trends for GRC Platforms

The effectiveness of GRC platforms has grown from highly complex and tough-to-use early platforms in the first generation, through effective platforms in the second generation that relied on improved automation of workflow, into more effective solutions in the present, third generation that have expanded scope and are offered with a cloud-based as-a-service option for customers (see Figure 1-29).

Trends include a shift from stand-alone platforms hosted on-premise, toward virtualized, cloud hosted (or even hybrid cloud supporting) solutions that serve the governance, risk, and compliance needs of evolving organizations. A clear trend has been the shift from non-embedded compliance overlay data collection to fully-embedded GRC data collection and management within business unit processes.

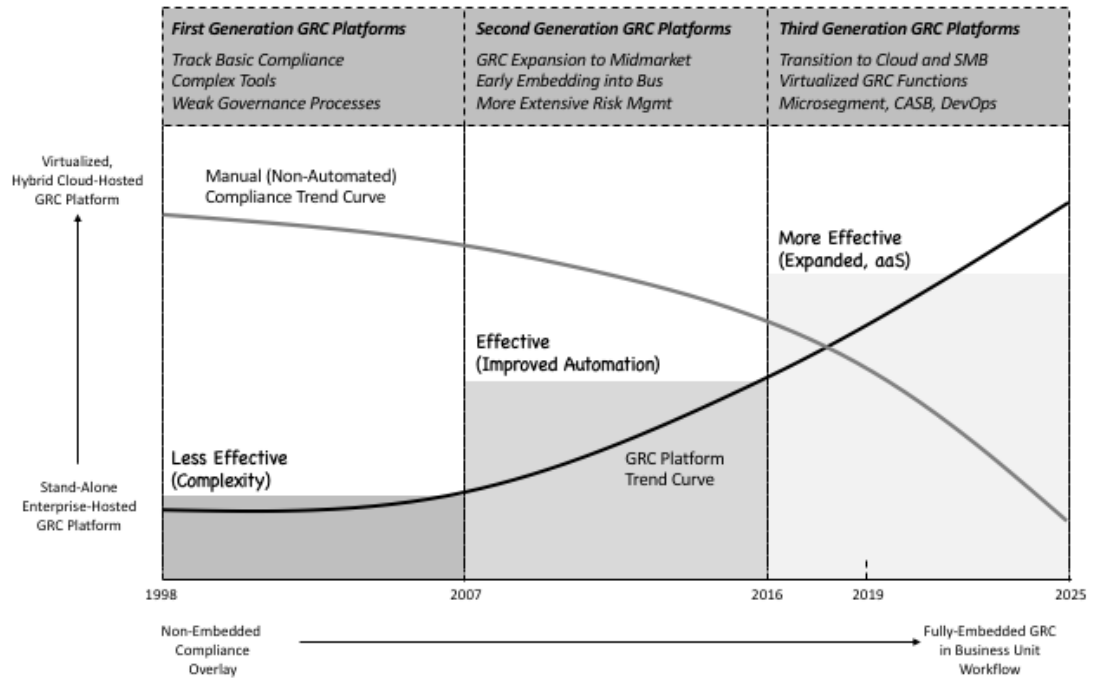


Figure 1-29. Governance, Risk, and Compliance Platform Trend Curve

The future of GRC continues to be bright, as organizations of all sizes will continue to rely on platform automation for all GRC-related activities. The market will see growth in GRC solutions for down-market, as-a-service offerings. Even the smallest companies will likely begin to use GRC to support compliance in their day-to-day activities. International use, perhaps driven by more severe privacy requirements, will be even more intense than in the United States.

The impact of super-intense privacy requirements as evidence in the General Data Protection Regulation (GDPR) arising from the European Union will gradually find a balancing point across international standards and norms. Certainly, privacy controls are essential and the GDPR has done much to advance awareness and attentiveness; but some aspects of the GDPR, such as the high fines to be levied post-breach, might require some adjustment downward over time.

30. Incident Response

Incident response involves the processes, tools, and procedures required to deal with on-going or previous cyber attacks on an organization. Traditionally, incident response has been more about cleaning up a disaster, forensically analyzing a prior cyber attack, and reconstituting hacked systems. More recently, however, incident response includes dealing with analysis of indicators, which introduces the possibility that incident response can be preventive.

A common visual descriptor used in our industry to describe cyber security emphasis is the so-called "shift-left" and "shift-right" designation. The underlying basis for this view is the attack lifecycle, which spans early indicators (on the left), across to an accomplished cyber attack mission with consequences (on the right). As such, shifting left implies being more proactive, and shifting right means being more reactive.

Incident response references the work done on the right of that underlying lifecycle. It includes the workflow, tools, databases, automation, analytics, forensics, and other resources to support all reactive work done after an attack has commenced or completed. Many of the larger commercial and government organizations today have an incident response vendor partner, but a surprisingly high percentage of mid-market and smaller firms do not.

2019 Trends for Incident Response

The effectiveness of incident response has evolved from most manual, less effective procedures in the first generation, through effective incident response advances that introduced automation in the second generation. Today's modern, third generation incident response frameworks are coordinated with hunt teams, automated into the SOC, and much more effective at dealing with incidents (see Figure 1-30).

One of the more interesting trends in cyber security is the seemingly cross-wise views that security teams should essentially just accept that attacks are inevitable, and agree to shift right on their emphasis. This is a hard concept to dispute, because just about every industry expert or pundit has explained that stopping capable cyber actors is not possible today, and that if a nation-state wants to break into your systems, then they can do so with impunity.

Despite this observation, just as many cyber experts will agree that incident response tools can be deployed and used to deal with early indicators, rather than with emerging evidence of a completed attack. By pointing the incident response team at indicators, the security team is essentially shifting left in their emphasis – and this would seem to contradict the earlier advice. The bottom line is that incident response teams will have to cover the entire lifecycle.

Everyone agrees, however, that the clearest trend is from manual incident response toward highly automated tools that guide workflow and manage artifacts. This is good news, because as cyber campaigns by adversaries continue to grow more advanced and complex, no enterprise security team can possibly defend using manual processes. The speed and scale of attacks require automated support, if only to keep up with volumes of data for analysis.

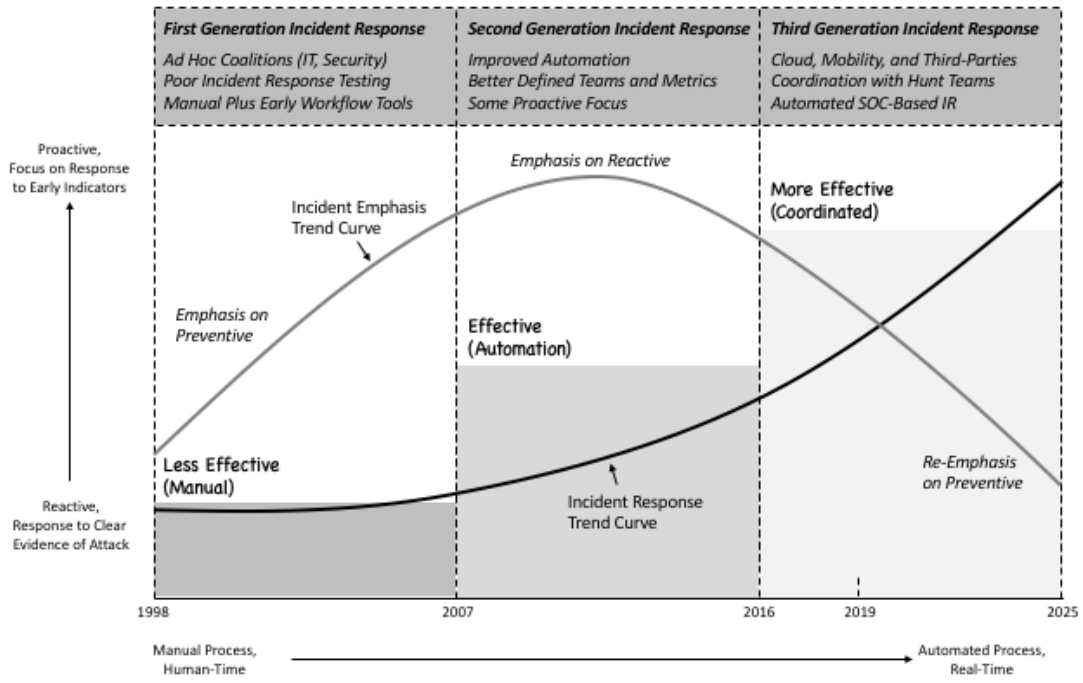


Figure 1-30. Incident Response Trend Curve

The future of incident response is toward expansion into mid-market and SMB team processes, likely through as-a-service, cloud-based offerings. This is a natural evolution because cyber attacks to these segments are becoming more intense, and the automation associated with modern incident response platforms does not require large, highly trained teams to operate. This greatly expands their applicability and potential use.

31. Penetration Testing

Penetrating testing has always been a staple in the enterprise security team's arsenal against continually expanding cyber risk. Few would argue the obvious benefits of unleashing the power and capability of vetted, trusted white hats against some target system, before non-vetted, untrustworthy hackers find their way to the same systems. This is particularly true for any asset or resource that is publicly accessible directly via the Internet.

Now, any form of testing will always have limitations. In fact, where testing is an excellent means for demonstrating the presence of exploitable vulnerabilities, it is not a great means for convincing an observer of their absence. In this way, penetration testing serves to illustrate and highlight problems, often in an environment where management or other decision-makers refuse to accept that serious issues might be present.

Finding good penetration testing talent for hire is non-trivial, so many enterprise teams have opted to create working relationships with companies specializing in this skill. Past experience suggests that many penetration testing teams have been somewhat transient, since it is easy for a highly-trained expert to spin off into a new start-up. Acquisitions of small penetration testing teams has also been a popular means for larger consulting firms to grow.

Nevertheless, every enterprise security team is wise to ensure a close working relationship with either in-house or contracted penetration testing talent. This is often best used to demonstrate, often in a shockingly visual manner, the existence of exploitable flaws in some portion of the business infrastructure. When a business unit leader refuses to cooperate with security, for instance, good penetration test results often shift such attitudes.

2019 Trends for Penetration Testing

Penetration testing has evolved from less effective engagements in the first generation, through effective usage in the second generation, into a more effective third generation. Advances that propelled this gradual and steady improvement included improved tester, better tools, more predictable pricing, and now greater attention to continuous penetration testing using automation (see Figure 1-31).

A clear trend has been from broad, general penetration tests toward more focused, domain-specific tests. This is good news for teams that manage specialized infrastructure or technology such as with IoT or ICS. An additional transition has occurred from ad hoc manual testing toward the use of automated platforms – and this includes attack simulation platforms that provide continuous test coverage.

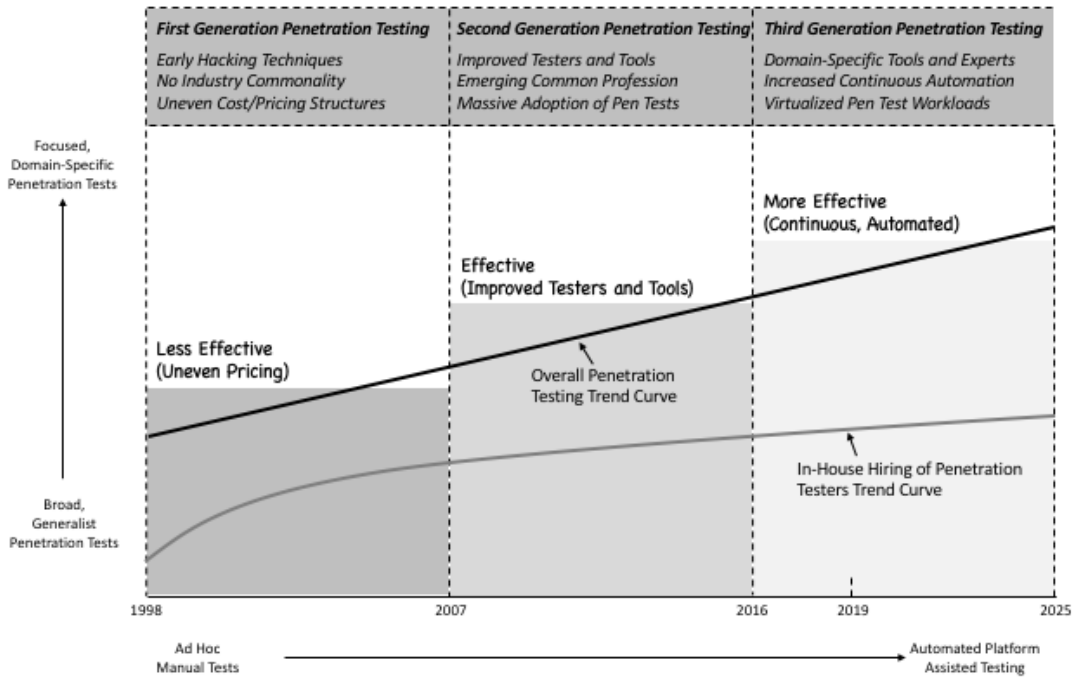


Figure 1-31. Penetration Testing Trend Curve

The future of penetration testing will continue to be characterized by gradual, but steady growth, with domain-specific testing and continuous simulation driving most of the heavier business growth. Despite clear advances in autonomous self-learning, it is highly unlikely that automation and AI will soon replace the need for experts to manage the penetration testing engagements for their infrastructure.

32. Security Analytics/SOC Hunt Tools

Just about every cyber security solution today is marketed as being powered by an underlying analytic platform, which tends to marginalize the importance of this technology discipline to cyber security. Collecting and properly analyzing data for evidence of cyber intrusions is a powerful means for improving the entire cyber defensive process, and the community has embraced analytics as an essential requirement in modern cyber defense, especially in the SOC.

The primary focus areas for *security analytics* tend to fall into three main categories of emphasis – although products can easily include elements of any number of these attributes: *behavioral analytics*, which collect observable meta-data to draw conclusions about actors; *real-time analytics*, which involve fast algorithms that keep up with network speeds; and *AI-based analytics*, which includes machine and deep learning techniques to reduce risk.

Solutions for security analytics can be stand-alone toolkits to be integrated into a customer's environment; they can be embedded as a component in a cyber security appliance or other product; or they can be available as a service, often in the cloud, where the analytics provides results to customers who need a verdict rendered either as part of a malware analysis or some hunt-related activity. In all cases, so-called *SOC hunt* teams are increasingly involved as users.

Some debate does exist across the cyber security community as to the efficacy of AI, machine learning, and other advanced heuristics in dealing with exploits. Evidence seems overwhelming that when applied properly, the results for malware and exploit risk reduction can be dramatic, so long as valid data is used to train the advanced processing on powerful platforms to recognize and accurately categorize previously unseen artifacts.

2019 Trends for Security Analytics

The effectiveness of security analytics and SOC hunt tools has risen through three generations from less effective correlation methods used for indicators, to effective use of advanced analytics using all-source intelligence to improve accuracy, and to reduce false positives. Modern, third generation security analytic usage includes highly advanced algorithms using machine learning to detect variants, new exploits, and other subtle indicators (see Figure 1-32).

Security analytic solutions have transitioned from centralized, stand-alone tools to more distributed analytic platforms that are often embedded in cloud workloads to address threats local to the asset being protected – often in a micro-segmented architecture. This is a powerful advantage, because it removes the needs for a complex, and often ineffective, perimeter to be used to detect attacks inbound to an organization.

The use of AI, and its related techniques of machine learning and deep learning, is the most exciting advance in security analytics – and arguably in all cyber security. Deep learning represents an excellent means for removing the need for tedious test training, by creating powerful arrays of neural processors that can ingest live data and learn to recognize malware and exploits dynamically.

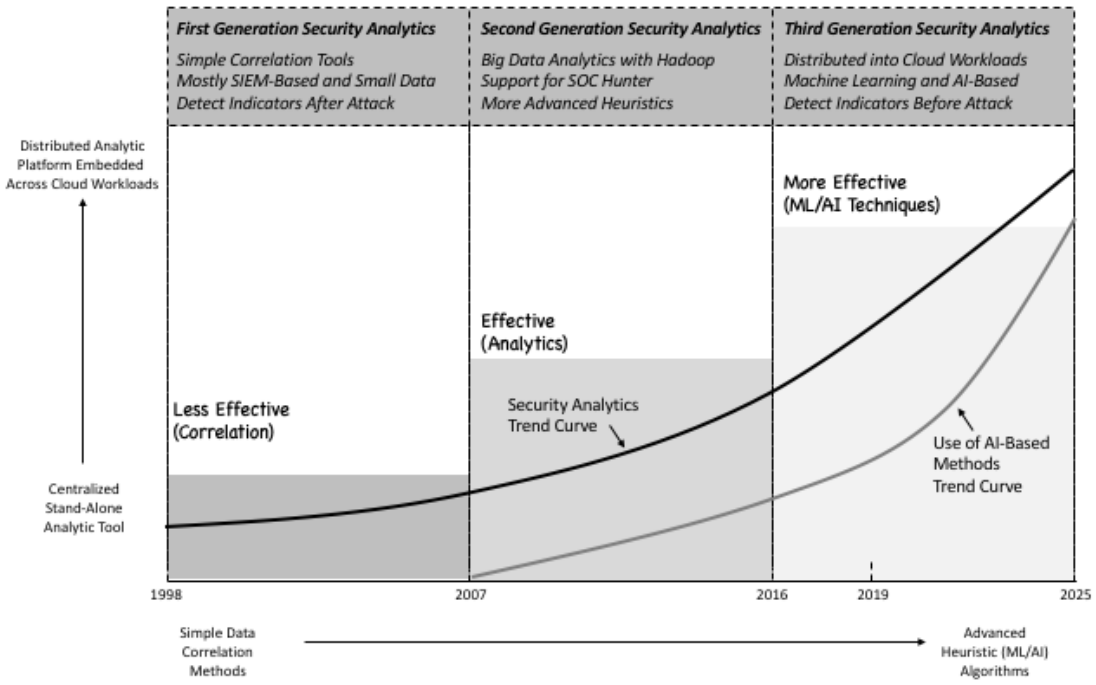


Figure 1-32. Security Analytics/SOC Hunt Tools Trend Curve

The future of security analytics and related SOC hunting resides with advanced algorithmic developments, and soon, this will include autonomous cyber security. To keep up with the prospects of synthetic attacks that are automated to find the weakest link in the fastest and most efficient manner, automation will be required to ingest behavioral and environmental data, and then combine this with the best intelligence to make a real-time security decision.

33. Security Information and Event Management

Virtually every mid-to-large organization today operates a *security information and event management (SIEM)* in their enterprise. Often referred to as the cyber security hub of an enterprise, the SIEM ingest data from applications, systems, and networks via tailored connectors. It then normalizes this collected data into a common representation so that analytics can be applied toward an effective, actionable conclusion.

The traditional SIEM was housed on-premise in the data center, and would be administered locally via console access by trusted, in-house personnel. This evolved toward increased use by managed security service (MSS) teams operating and managing the SIEM more virtually, with a more extensive assortment of connectors. Modern SIEMs reside primarily in the hybrid cloud, with the requirement that data be ingested both on-premise and from cloud workloads.

Recently, more down-market SIEM offerings have been made available that are easily integrated with cloud deployments, and this has greatly expanded the SIEM ecosystem. One might expect to see SIEM usage even find its way into small and even micro-business infrastructure – mostly virtual – and this will have a good impact on compliance and security in these segments of the business environment around the world.

An additional trend involves the use of advanced tools that help the SIEM better orchestrate security operations across an enterprise. This begins the transition of the SIEM as a passive collection device, into a more active operations hub for enterprise cyber security. This transition will create interesting marketing integration (and collision) with CASBs, microsegments, and even next generation firewalls.

2019 Trends for SIEM

The effectiveness of SIEM solutions has risen through three generations of usage from less effective early tools, through effective tools built for data analytics, into the modern, third generation where the SIEM is more effective, cloud-ready, and much easier to use. The coverage for SIEM deployments has transitions from mostly large organizations to basically all organizations in the coming years – which is a welcome evolution (see Figure 1-33).

The architecture for SIEM deployment and use has evolved from LAN-based appliances on physical servers to much lighter, cloud-based virtual offerings. A clear trend is that one should expect to see a dramatic drop-off of on-premise hosted SIEM infrastructure in favor of more virtualized coverage. This follows the reduction in emphasis on a perimeter-based LAN supporting the business and government enterprise.

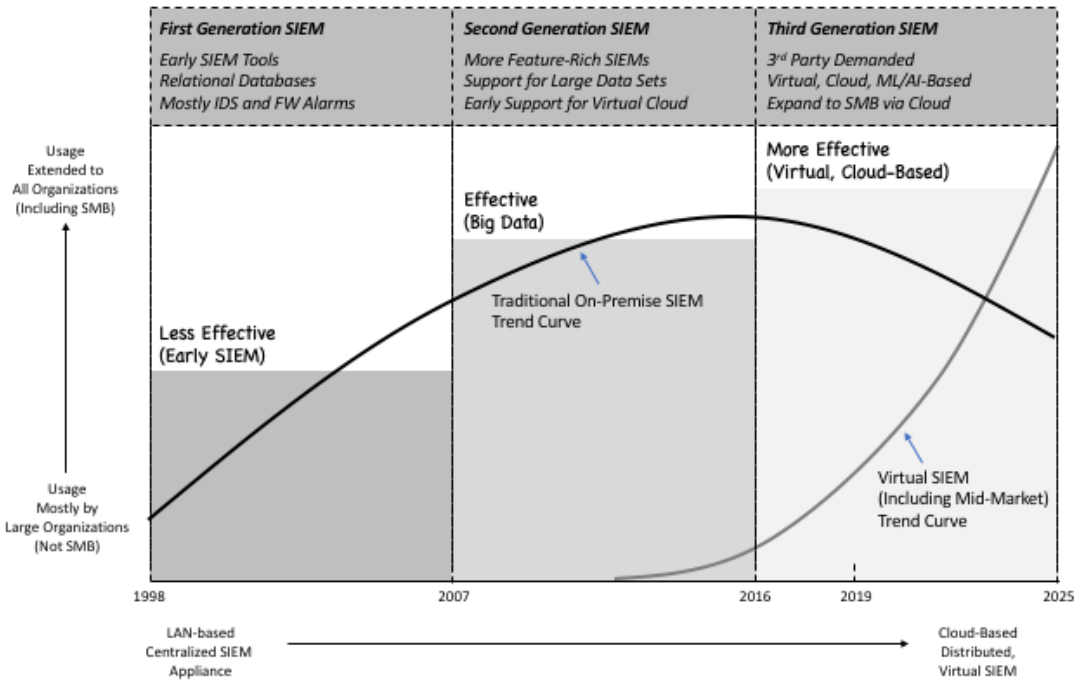


Figure 1-33. Security Information and Event Management Trend Curve

The future of the SIEM is clearly in its expanded market, with the current trends into mid-market infrastructure extending to the micro-business and even family or personal systems. It would seem a natural extension of current SIEM capabilities; for example, ISPs could provide a solution for the home, perhaps hosted on cloud operating systems in generic hardware. This would help families do a better job avoiding serious breach attempts at their personal finances.

34. Threat Intelligence

The use of *threat intelligence* to enhance the usefulness of cyber security products, services, and enterprise processes is now well-established in our industry. The analogy of oil lubricating an engine seems accurate in describing how threat intelligence drives high-quality security solutions. The most traditional example is the real-time URL intelligence that has been used for years to update and maintain web security proxies.

Many vendors now offer threat intelligence as a feed, often derived from teams of experts, usually former law enforcers and hackers (which one suspects can produce an interesting mix of personalities around the office water-cooler). These feeds can be ingested in both structured and unstructured formats. The trend is toward automated sharing of threat data by systems that can ingest and process data with the goal of taking mitigation action.

Considerable threat intelligence is now derived from marginally-unsavory sources such as the deep and dark web, and the lifecycle handing of stolen credentials offers a new opportunity. By embedding into the early stages of credential theft and then sharing, intelligence teams in commercial entities can identify this stolen information and use it as the basis for creating early detection and prevention of exploits.

Platforms for sharing threat intelligence in organized groups continue to play important roles in the cyber security community. Government-organized or even mandated sharing initiatives have been helpful, but international and competitive pressures have hampered some efforts. Commercial solutions have thus been especially helpful in creating private sharing enclaves where senders and receivers of intelligence establish a meaningful level of trust.

2019 Trends for Threat Intelligence

The effectiveness of threat intelligence sharing and usage has transitioned from less effective early approaches, through effective processes with improved delivery of threat intelligence, to the current more effective generation of threat intelligence usage, where the goal is actionable results. This progression is good news, because coordinated defenses are the best approach amidst growing capabilities from capable adversaries (see Figure 1-34).

A clear transition in threat intelligence has been from human-time management of often-manual processes for dealing with ingested information to the real-time delivery and analysis of ingested data for immediate defensive adjustment and mitigation. In addition, threat intelligence has moved from collection of data from a single source, to all-source ingest from a variety of different trusted entities.

It is worth mentioning that the Federal Government includes its own unique sets of factors in the use of threat intelligence for national security and information assurance. Nation-state military and intelligence teams can collect information at a level that is impossible for commercial entities. Human intelligence and signals intelligence, for example, permit a level of attribution that would be unheard of in industrial settings.

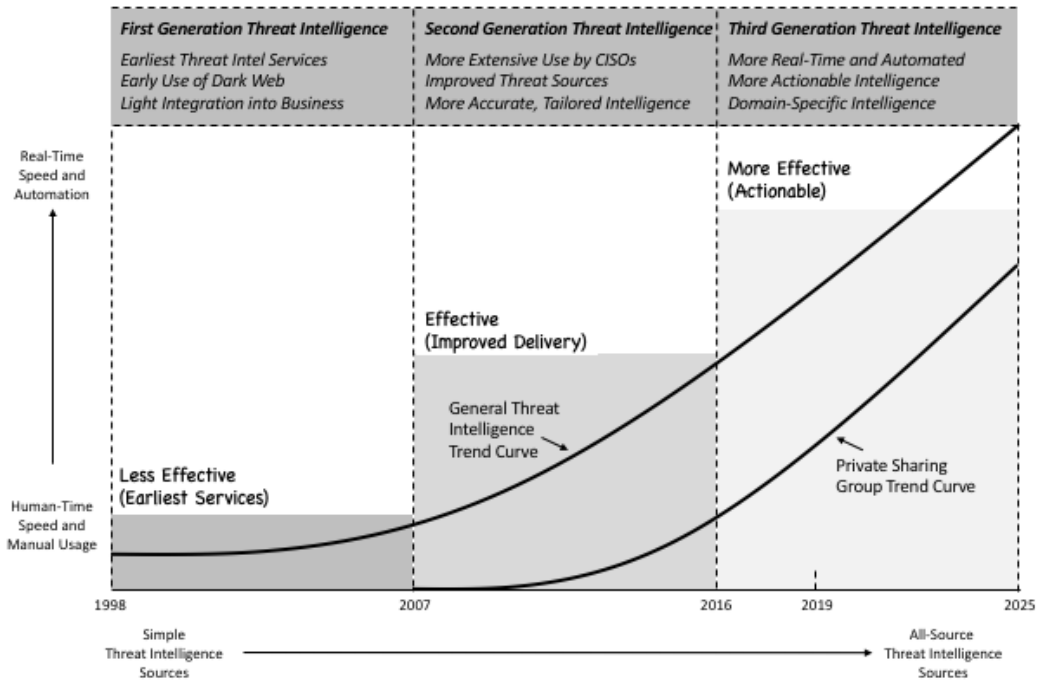


Figure 1-34. Threat Intelligence Trend Curve

The future of threat intelligence is toward increased automation, improved autonomy, and more real-time actionable results from ingested data. The use of private sharing groups, perhaps temporary or project-based, is likely to increase considerably, which follows the increasingly transient nature of business partnerships. One can also envision cloud services soon including threat intelligence APIs as a normal course of business with its customers.

35. Application Security

Perhaps the most challenging aspect of enterprise cyber security involves dealing with the unique and sometimes legacy issues of *application software*. Few would argue that applications, including mobile apps, exhibit the highest degree of update and change in all of computing. Where infrastructure software and systems might be installed and left intact for months or years, applications can experience meaningful changes on an hourly basis.

If you add the fact that software engineering remains a craft with little hope of producing bug-free code in non-trivial products, then you have a tough environment for securing apps. This helps explain the many approaches in this area: Static code review, app scanning, software maturity, behavioral visibility, application telemetry, containerized protections, risk scoring, and micro-segmentation are all promising risk reductions for apps.

One clear trend involves more active analysis of applications, and many vendor focus on and offer *run-time application self-protection (RASP)* solutions. The trend with many RASP offerings involves a shift toward telemetry generation first, with active mitigation support coming second. This seems a rational deployment methodology, given the challenges of dealing with the unique complexities of modern applications for both Web and mobile.

Most experts agree now that the most common root cause for advanced exploits and breaches in the enterprise will be found at the application level. It is also not uncommon for different vendor solutions that purport to do the same general function (e.g., scanning) to produce wildly different output. This can be unsettling for an enterprise security team, and really highlights the unscientific methods for application security that are still followed by many teams.

2019 Trends for Application Security

First generation *application security* was less effective, because it focused on simple methods such as scanning that helped, but were insufficient to address the threat from software. Second generation application security became effective from many new options including improved maturity models, run-time security controls, and early self-protection. Modern third generation options are more effective and are beginning to converge (see Figure 1-35).

Early, ad hoc manual code reviews have transitioned to automated, intelligent, self-learning, run-time security for application security. This is a massive shift, and does provide a significantly improved level of security for application-level software including mobile apps. In addition, this function – which was originally a non-component of most early enterprise security teams – is now considered an essential, highlighted component of every CISO program.

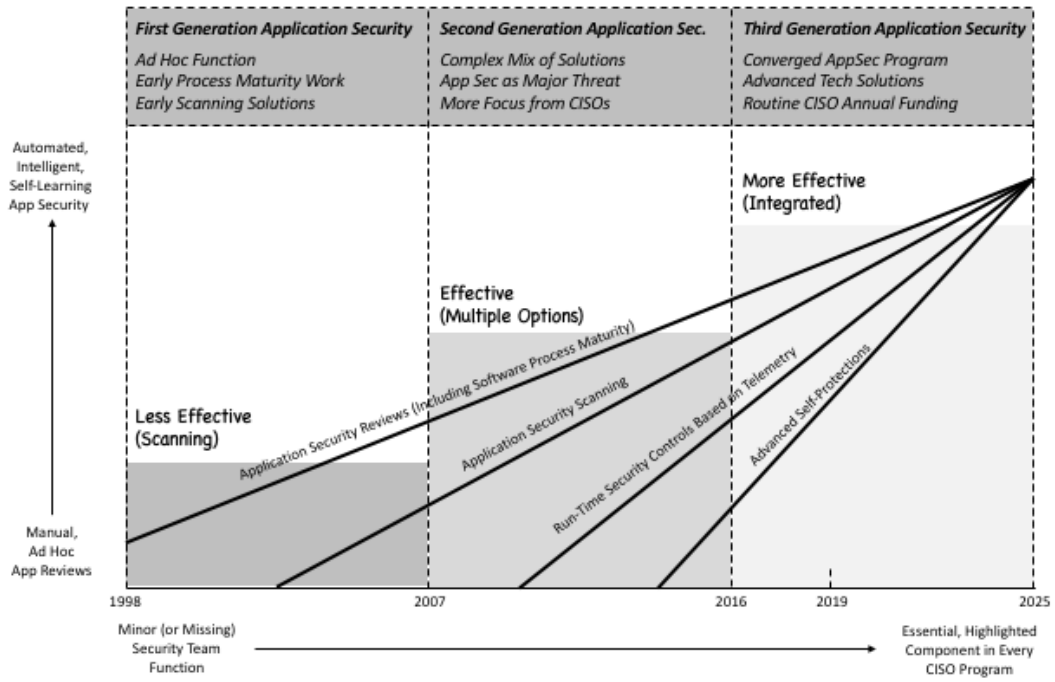


Figure 1-35. Application Security Trend Curve

The future of application security involves convergence, especially for run-time protections in cloud workloads and containers. That is, rather than select from a menu of different and largely non-integrated options for application security, the emerging generation of enterprise security teams will have a common, unified philosophy for application security. The tools and processes used to ensure AppSec goals will be provided in a more integrated, cohesive manner.

36. Content Protection

Content protection has traditionally been rooted in the use of *digital rights management (DRM)* technology, which many consumers, especially young ones, do not like. Consider, for example, the continued bumpiness and uneven approaches used to protect and monetize movies, television shows, apps, games, media, music, and other content across non-heterogeneous platforms such as Microsoft Windows, MacOS, iOS, and Android.

The protection of this type of *media* content is largely outside the scope of this report, because it is an issue that 99% of CISO teams do not have to contend with. But the deployment of enterprise DRM to provide protection of intellectual property is an enormous concern for every CISO team – and is hence considered an important control area. The bad news, however, is that previous enterprise DRM with PKI-enabled infrastructure has proven highly complex to run.

The good news is that with the rapid adoption of cloud-based, as-a-service data handling, the securing of intellectual property using content protection tools will grow considerably. This is a natural extension of how cloud storage, cloud data management, and cloud security are being handled. One would expect smaller firms to adopt encryption and related content protections in cloud more readily than larger firms, which will come later.

A major requirement to support this DRM-like adoption in cloud and as-a-service solutions will be ease of use, and integration with common, existing tools such as Microsoft Office tools for dealing with business files. Furthermore, the underlying PKI controls will have to be hidden and managed from enterprise teams to avoid the complexities that have held back business content from being access-controlled with strong, mandatory protections.

2019 Trends in Content Protection

Less effective early enterprise DRM solutions could not find a growth curve, and with the dissolution of the perimeter, will continue a downward trend. Instead, cloud-based protection, including encryption of data, have already found that growth curve and will be a successful new enterprise control. This results in stand-alone DRM moving to embedded content protections in cloud, resulting in stronger security (see Figure 1-36).

Content protections for media will gradually shift toward increased enterprise relevancy as more businesses opt to utilize creative video, social media, and other forms that might have previously not been considered common for use by companies. This might create some intersection in the DRM community between consumer and business use of encryption and key management. Nevertheless, the encryption and access control for media will remain largely separate from similar tools used to protect business information.

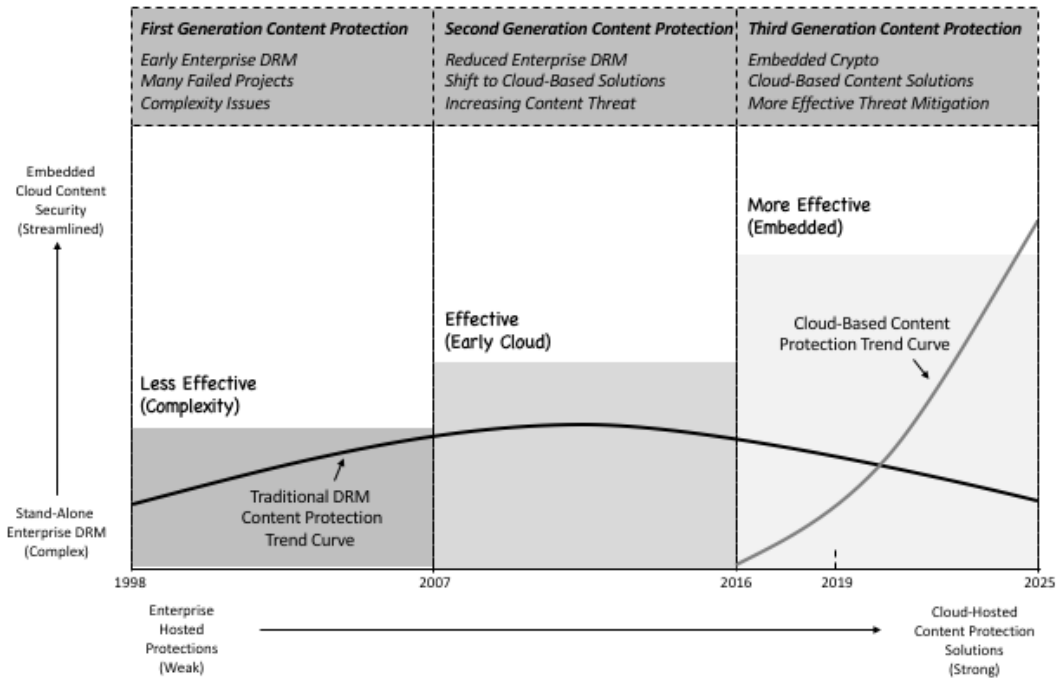


Figure 1-36. Content Protection Trend Curve

The future of content protection lies in stronger forms of encryption, data protection tools, and intellectual property security in virtualized, cloud-hosted infrastructure. Enterprise teams will include more routine inclusion of source selection requirements from enterprise teams for these types of data security capabilities when companies are selecting vendors to support storage and other functions to be implemented in the cloud.

37. Data Destruction

Perhaps the least attended to requirement in the CISO arsenal is *data destruction* – and this is somewhat mystifying – at least to this analyst. Consider the following: One of the most well-established and insidious challenges every enterprise security team faces each day involves the malicious theft of data, information, and intellectual property. Such resources typically exist in the form of files, records, presentations, folders, and other stored receptacles.

This would imply, one would guess, an obsessive focus on deleting, destroying, and removing every such piece of information that is not essential to the function of the enterprise. It would also imply, one would guess, that data destruction methods follow a basic principle of minimal storage. That is, information should be stored in its most limited and isolated manner for as short a time as possible – like handling radiation.

The reality, however, is that most security teams have either non-focus or limited visibility into how IT or local business unit teams handle this important function. In smaller businesses, there might be zero emphasis on policies for storing company data; in mid-sized companies, a policy might be in place, usually for printed materials that should be shredded. In larger companies, *records information management (RIM)* policies are generally established, but mostly ignored.

Cloud services can potentially change the equation here, but only if enterprise security teams begin to more forcefully demand this function in every as-a-service capability they select and use. Standards exist for proper destruction of data, and RIM policies are in place – so this is not a technically challenging issue. The problem is one of emphasis: Ask ten CISOs about how they do data destruction in the enterprise or cloud, and expect a non-answer.

2019 Trend in Data Destruction

The effectiveness of data destruction methods has remained effective through three generations of usage. With cloud services, the techniques are even more effective. The challenge instead has been around the attention, application, and enforcement of data destruction tools – both hardware (for physical media) and software, to ensure attention to minimal storage of corporate information (see Figure 1-37).

The trend one should expect in the coming years is that this function will eventually progress from a weak, ad hoc option to a strong, mandatory control. In addition, the function as a local physical destruction option, including shredding in the office, will transition to a cloud-hosted virtual option, where less paper is involved and more standards-based destruction of unneeded information will become the norm.

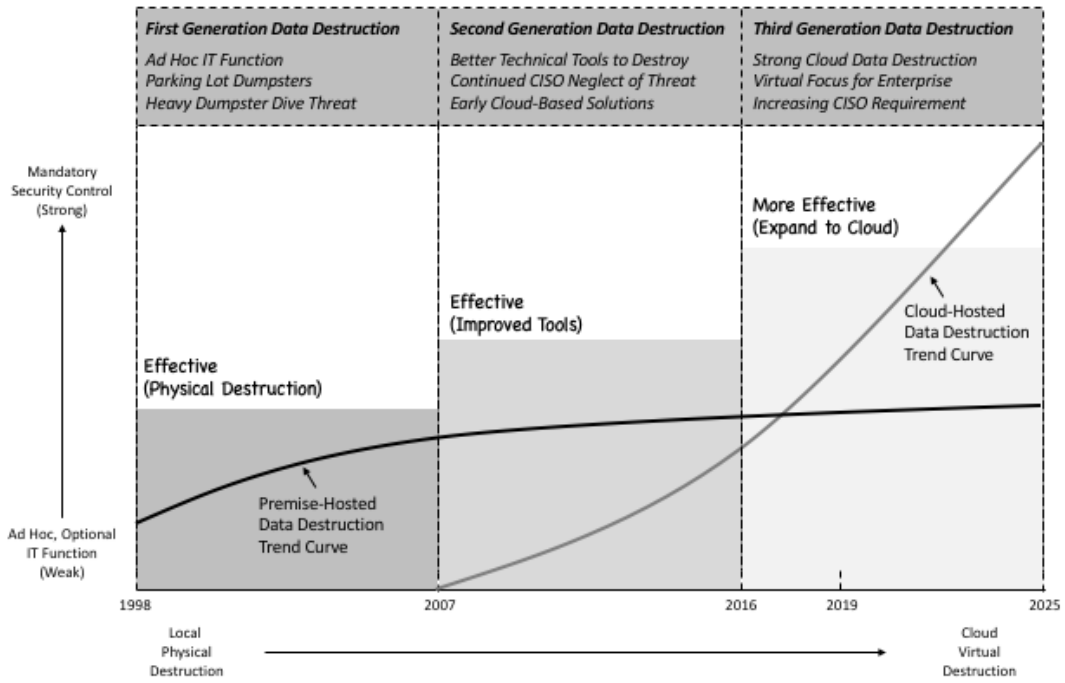


Figure 1-37. Data Destruction Trend Curve

The future of data destruction resides in the cloud. Older images of companies shredding paper will gradually evolve to virtualized functions that are automated and properly attended to in the cloud. Legal provisions will continue to play an important role here, because some important corporate data must be maintained; but in all cases where data can be deleted, it will be – and the cloud providers will have this responsibility to implement the destruction.

38. Data Encryption

Data encryption has been largely synonymous with computer security for many decades. In academia, entire courses on security might include 90% of the lectures on encryption. While this might make for excellent and interesting class discussions and exercises, it misses the point on the role that encryption plays in modern cyber security as an underlying foundational method in the context of broader protection methods. It is a *means* to an end; not an end.

The data encryption business has been hazardous for many vendors since the early days of our industry. The challenges have been many – including the difficulty of providing easy-to-use administration tools, the technical issues of algorithmic and protocol interoperability, the legal and political debates that arise between law enforcement and industry, the ambivalence of most users about properly storing data encrypted, and on and on.

Perhaps the only reason encryption has seen some commercial success through practical application is the obsessive influence the compliance community has had on its use. Every security compliance framework demands encryption of data – both at rest and during transmission – and this has resulted in reasonable adoption and use of encryption. But as a commercial business, it's never realized its full potential – but this might change with cloud.

All this said, the modern enterprise will continue to require and demand the strongest forms of encryption for data at rest and in motion. Both are required in every security compliance framework and by every business auditor, so the requirement will not change. What hopefully does change is the ease with which such encryption support is offered across heterogeneous services provided in hybrid cloud environments.

2019 Trends for Data Encryption

The effectiveness of data encryption in the context of enterprise protection has transitioned through three generations from less effective, manual techniques, through effective solutions with improved automation, into the present approach of more embedded data encryption. Such an integrated, embedded methodology reduces the need for key management and related administration (see Figure 1-38).

Key management is shifting from ad hoc techniques and tools to more standard approaches, often using the power of hardware security modules (HSMs) to assist in the protection. Stand-alone data encryption is being replaced by tools that are embedded smoothly into cloud workloads, databases, and even the data representation itself. All these are positive shifts which will help make data encryption more accessible down-market.

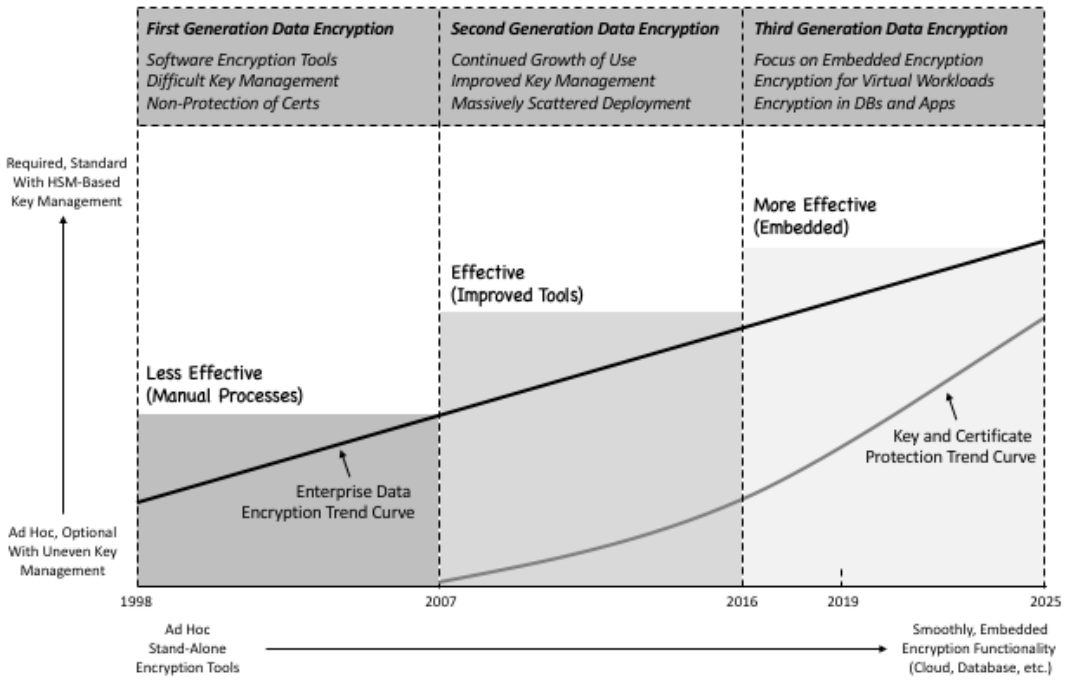


Figure 1-38. Data Encryption Trend Curve

The future of data encryption, from the perspective of vendor success and growth, is in cloud and other services, including software-defined networks (SDNs) where the telecommunications provider will offer advanced encryption not only for data in motion, but also in storage. Encryption algorithms will continue to improve gradually and will face existential replacement needs in five to ten years due to advances in quantum computing.

39. Digital Forensics

Digital forensics remains a vital analytic technique to be used by experts to make sense of artifacts that might provide evidence of cyber exploits or malware. In the past, this discipline was the sole concern of highly-trained experts with advanced tools, often from law enforcement. But today, the digital forensics space is being populated by individuals who require less training and can achieve good results with accessible, affordable security tools.

The emphasis in digital forensics was also previously around reactive response to a past cyber or criminal incident; but today, this emphasis has shifted to the right in the overall attack kill chain. This implies that instead of treating the forensic process of dealing with just evidence of past attacks, it can also deal with early indicators of attack. Some forensics vendors see this as an opportunity to slide into the endpoint protection space.

Nevertheless, the core focus of digital forensics remains the same: It is a vital and growing discipline focused on extracting intelligence from artifacts to draw conclusions about physical or electronic hacking, criminal activity, policy violations, and the like. To this end, as the potential behavior of interest moves more toward cloud, mobility and other emerging areas, then digital forensic tools and techniques must shift accordingly.

2019 Trends for Digital Forensics

The effectiveness of digital forensics tools has risen from its first generation, rudimentary beginnings to the more effective, embedded tools in use today. This is good news for forensic analysts and even law enforcement, but social and political policies play an important and vital balancing role to ensure that these tools are properly positioned in terms of power and capability. Apple's famous debate with the US FBI about decryption exemplifies the issue.

The most comprehensive transition that is occurring for digital forensics is the shift from stand-alone tools for an isolated analyst working after an event has occurred toward a much more integrated platform of support for hunting and response teams searching for evidence of past, but also on-going incidents. This implies that digital forensics tools, when applied to indicators, can be preventive (see Figure 1-39).

An additional on-going transition in the digital forensics space involves a shift from data under local control – such as on a captured disk drive or mobile device – to the analysis of data perhaps under remote or third-party control. Obviously, law enforcement can sieve such data under the proper circumstances, but for commercial digital forensic analysts, this option might not be available.

As such, one should expect to see more intense use of digital forensic options from cloud service providers handling data of interest. This can be done in a professional service context, or it can be automated into the as-a-service environment. The publication of APIs for digital forensic analysts interested in determining the low-level characteristics of some stored artifact would not seem out of the question.

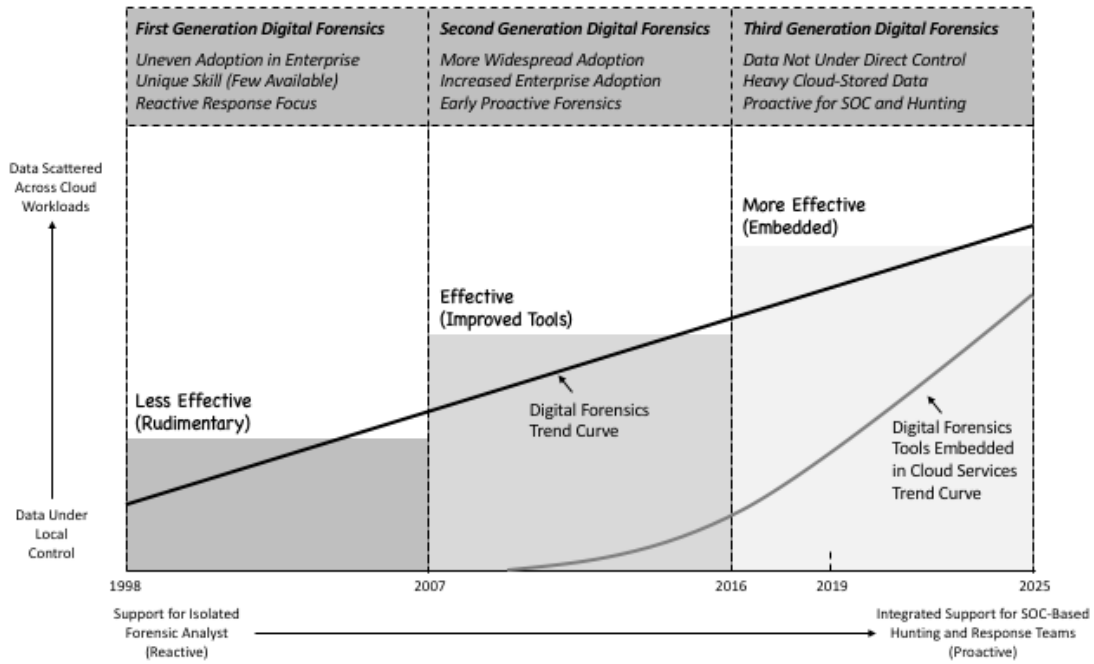


Figure 1-39. Digital Forensics Trend Curve

The future of digital forensics lies in emerging virtualized support for artifacts that are scattered across hybrid architectures. This will not remove the need for specialized analysis of specific devices such as mobile phones, but will create an enhanced means for establishing context around the forensic analysis of a given incident or exploit. Commercial digital forensics platforms will evolve to provide this broader view.

40. Identity and Access Management

Every enterprise security team will attest to the increasingly fundamental role that *identity and access management (IAM)* technology, systems, tools, and processes all play in the protection of organizational assets. This has always been true, as evidenced by the lopsided percentage of the overall IT security budget that usually finds its way to IAM. With the dissolution of the perimeter, IAM takes on a new security significance.

The cloud introduces considerable new opportunities, but also tough challenges, for organizational IAM infrastructure and applications. Obviously, it is more straightforward to operate and deploy an IAM system onto a perimeter-protected LAN, if only because so-called east-west visibility can be assumed to most relevant resources. Despite IAM's historical reputation for complexity, its operation was, in fact, assisted by a flat enterprise network.

So, now with the transition to hybrid cloud architecture, the IAM becomes the primary control for access to resources, replacing the firewall. That is, rather than presenting hackers with an initial hurdle in the form of packet filtering or application-level policy enforcement in a firewall, the new arrangement requires that access to the cloud gateway be permitted for publicly-hosted resources. This implies that IAM will be required to differentiate good from bad users.

With this adoption of IAM as a primary control will also come increased attentiveness from the compliance and audit community – as if IAM experts have not had enough of this already. New cloud-based IAM solutions have generally been designed with security in mind, rather than pure compliance. One might expect that with IAM-in-the-cloud offerings, the overall attention assigned to automated support for audit is likely to increase.

2019 Trends for Identity and Access Management

The effectiveness of IAM has evolved from less effective deployments that were highly complex, through a second generation of effective installations that began to address some cloud usage, into the present more effective IAM solutions which are distributed and support virtual computing. This gradual evolution toward better IAM has been made possible by attention across this sector in reducing complexity (see Figure 1-40).

A clear transition has occurred during this evolution from centralized systems installed on a LAN toward more hybrid systems distributed across premise, network, and cloud systems. In addition, increasingly decentralized control of identities for authentication, access, and authorization is also consistent with the hybrid arrangement. IAM is thus considered an important aspect of cloud infrastructure for business.

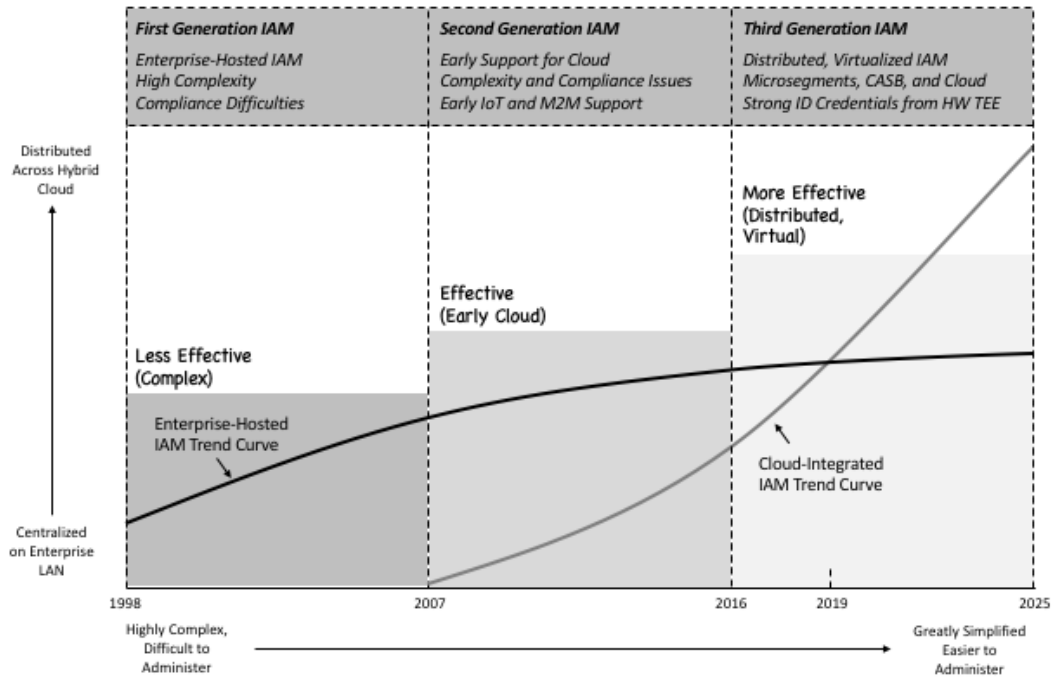


Figure 1-40. Identity and Access Management Trend Curve

The future of IAM will see three trends: Continued integration into cloud infrastructure, continued focus on simplification of administration and use, and continued drive toward more secure, decentralized storage and management of credentials. These are positive trends, consistent with emerging compliance needs. IAM will thus see continued growth across all industrial sectors, including smaller businesses becoming more reliant on these solutions.

41. Security Compliance and Risk

Every business understands the importance of a *security compliance* program, if only because modern regulatory and audit requirements demand attention to this area. Credit card usage, customer data storage, third-party support, and on and on – all require attention to ensuring a minimum level of security protections; hence, the security compliance industry has thrived, with products and services available to assist businesses of all sizes.

The most common commercial engagement in security compliance involves use of a consultant to provide either pre-audit advice, formal attestation, or post-audit improvement. This can be done by trained consultants in the context of a well-established compliance standard such as the Payment Card Industry (PCI)/Data Security Standard (DSS); or it can be done by established experts in the context of generally accepted security practices.

Many commercial tools that assist with the compliance process tend focus on *security risk*. In fact, an enormous industry sector has emerged for collecting security risk-related artifacts, analyzing and synthesizing them into a coherent view, and then presenting these risks as a dashboard for executives. The usefulness of risk analysis, management, and reporting tools is two-fold: They help with compliance, but they also help with pure cyber security.

An additional major factor for both compliance and risk involves third-party coverage. Most of the major breaches that have happened in the past few years have involved third-party suppliers, partners, and support teams. Automation will be required to deal with this massive growth in third-party initiatives, including outsourcing and offshoring. As the work scatters across a more complex organization, the compliance and risk must follow.

2019 Trends for Security Compliance and Risk

The effectiveness of both security compliance and cyber risk management tools has increased from less effective platforms in the first generation, through an effective period of both compliance and risk support, to a more effective third, present generation. Security compliance support has increased gradually and linearly; risk management support is in a more accelerated growth curve for both commercial success and effectiveness of solution (see Figure 1-41).

The accelerated success that risk platforms have experienced can be traced to their dual value proposition for both compliance and security. For example, if an executive team or board would like information on compliance metrics or on general cyber security posture of the organization, a risk reporting platform with good visualization would provide an excellent means for providing this information clearly and accurately.

A transition for both compliance and risk is that the pure number of applicable frameworks has grown dramatically. This is an aspect of our industry where growth is probably not a good thing. When additional frameworks are introduced to an environment, the compliance and security teams will rely on the automation to just map existing practices to the new requirements. This introduces more bureaucracy, and rarely results in changes to operations.

An additional transition for compliance and risk has been the shift from largely manual processes that are overlaid onto business unit systems and procedures to more automated and embedded compliance and risk platforms. This is a welcome shift given the larger number of applicable frameworks, as well as the speed and scale increases in most modern business sectors. The automation helps compliance and security teams keep up with the volumes.

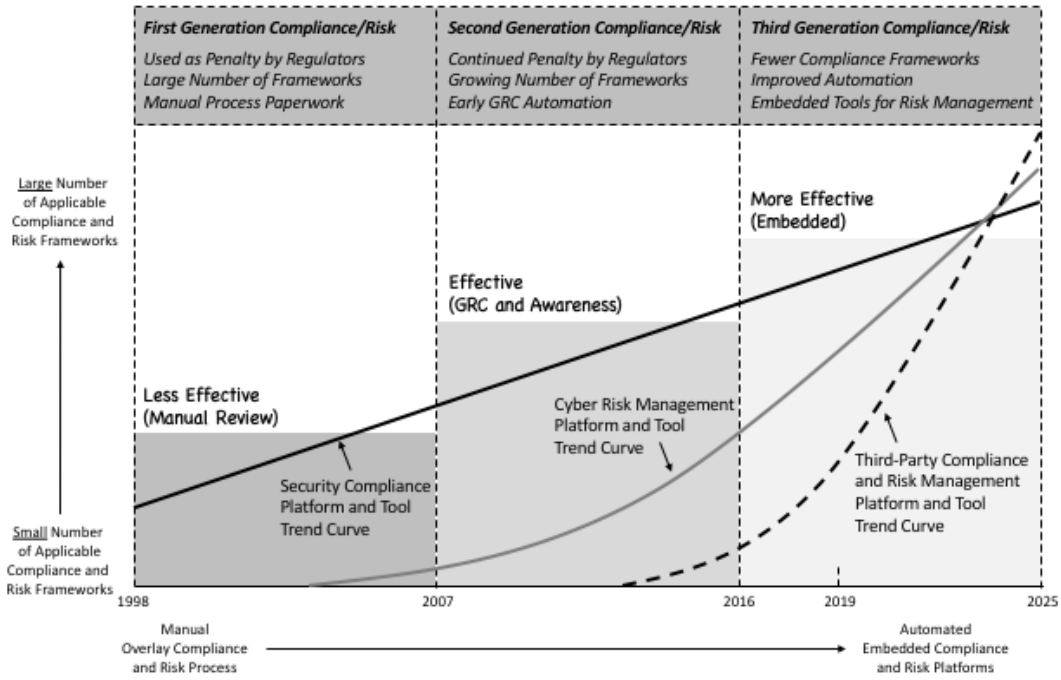


Figure 1-41. Security Compliance and Risk Trend Curve

The future of security compliance and cyber risk involves more automation, more embedded controls, and expanded focus across increasingly hybrid cloud environments. Less compliance and risk data will come from the local LAN, which is dissolving, and more will come from third-party programs. Manual compliance and risk management will gradually fade into executive processes that interpret and utilize insights from the automation.

42. Vulnerability Management

Vulnerability management for enterprise began its life in the business of patch management for servers in the early 2000's. It has since shifted rapidly from this modest beginning, to one of the most essential cyber security processes for identifying, categorizing, tracking, managing, and remediating the massive assortment of cyber-related vulnerabilities that modern organizations face across their servers, endpoints, databases, systems, networks, and so on.

The modern vulnerability management process requires a variety of information, access, tools, techniques, and capabilities, because it tends to reach into every aspect of business unit activity. For example, vulnerabilities can be obvious, such as highly-public exploits that affect all servers in the data center; or they can be hidden and subtle, such as an obscure software bug in a small proprietary application used in a limited manner by a small portion of the company.

This need for wide vulnerability management coverage has resulted in a shift toward greater use of automated discovery, control, and even remedy. That is, vulnerability management has shifted from the days of manual reviews based on Excel spreadsheets of identified issues toward platform-based orchestration of more extensive coverage. This also now includes vulnerability management for cloud and mobile assets as well.

Many existing security consulting teams have found a natural evolution from professional services with clients engaged in vulnerability risk toward the provision of an automated platform for helping to perform enterprise-wide vulnerability management. This is a welcome process, because such experience-based creation of automated platform support based on real projects will result in high-quality advances to vulnerability management offerings.

2019 Trends in Vulnerability Management

Vulnerability management was less effective in its first generation of use, due to overly manual processes that missed important issues. The second generation of vulnerability management was characterized by improved methods, including early automation. Current, third generation vulnerability management is more effective with fully automated platforms ingesting relevant data from all-sources (see Figure 1-42).

Transition has occurred in this area from isolated focus on software patches in the early days toward a comprehensive focus on a range of different vulnerabilities in traditional server and application areas, as well as emerging cloud and mobile. This is characterized by intelligent, automated VM platforms that are on the verge of incorporating advanced heuristics including machine learning to improve accuracy.

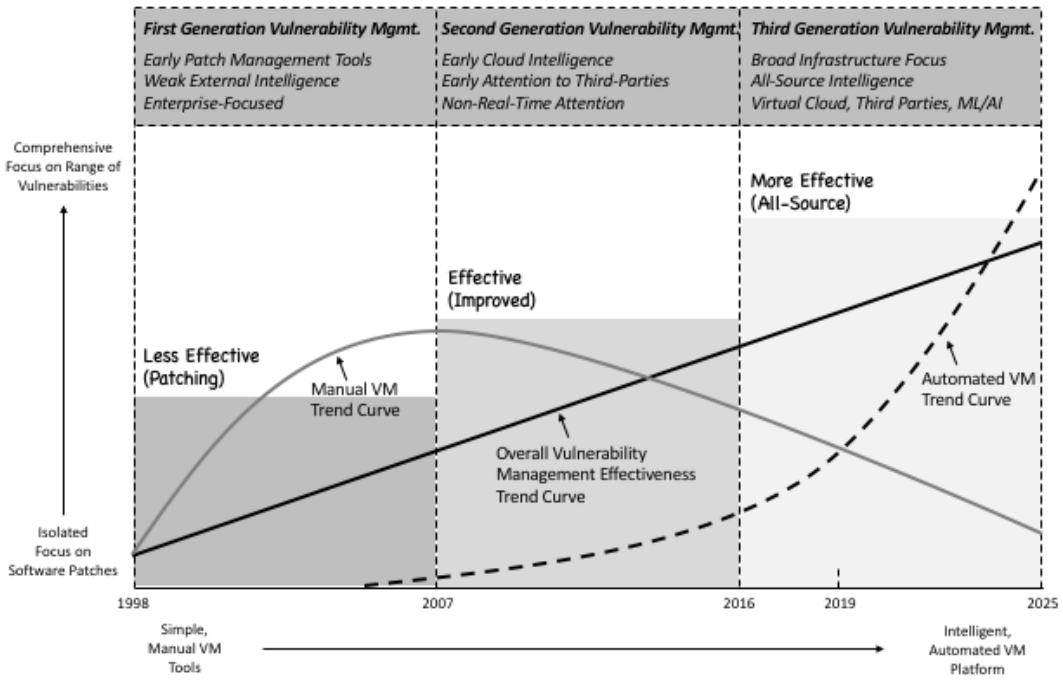


Figure 1-42. Vulnerability Management Trend Curve

The future of vulnerability management lies in more embedded collection tools and management controls. Like GRC functions, VM works best as an integrated component, rather than as an overlay. As such, expect to see most new systems come with pre-defined interfaces for VM platforms to ingest data and to serve up required mitigation based on identified vulnerabilities.

43. Industry Analysis

Industry analysis for cyber security involves the expert provision of advisory guidance, trend information, and relevant insights for the working cyber security professional. It is a vital component of vendor source selection, and when used properly by an enterprise security team, can save time, budget, and effort across the enterprise cyber security ecosystem, across all phases of the kill chain. Few consider industry analysis a *control*, but it most certainly is.

For example, when an enterprise security program is being created, managed, augmented, or assessed, the advisory guidance from experts should plan an essential role in future-proofing the characteristics of that program. Without such guidance, security managers and executives are basically guessing trends, mostly based on vantage points that exist within the walls of a private, proprietary enterprise.

Most industry analysis to date has come from large companies providing two-dimensional grids. They score vendors based – presumably – on objective assessments of their ability to provide a good solution and their insights into the needs of their customers. In practice, however, these grids, waves, and quadrants are expensive, and have tended to serve more as marketing fodder, with relative placement often determined by pay-for-play factors.

This *TAG Cyber Security Annual* is an attempt to shift the cyber security industry analysis picture toward more egalitarian, free, unbiased assessment of security technology vendors, commercial solution offerings, and defensive cyber trends. Good analysis is an important component of security protection – no less important than great consulting support, penetration test insights, or world-class functional architectures.

2019 Trends in Industry Analysis

The effectiveness of industry analysis through its first two generations of use has been less effective, simply because the discipline has not been properly attended to across the cyber security industry. The present generation includes more expert guidance – including this TAG Cyber Security Annual – and should create an important new resource for enterprise security teams making decisions about their cyber risk (see Figure 1-43).

The transition away from quadrants, grids, and waves is the best example of improved analysis in our industry. Every other aspect of our business, financial, and critical infrastructure sectors includes independent, unbiased assessment of the quality and effectiveness of tools, products, methods, and solutions available for purchase. This transition is welcome and will significantly improve the ability of enterprise teams to build cyber security solutions.

An additional transition is that generic guidance from broad, non-specifically trained writers will be replaced by experts with many years of training in domain-specific areas. General industry reports, for example, that are created on industry control system security simply cannot be produced effectively by writers using a browser to search keywords in this area. Luckily, enterprise teams are no longer assigning much value to these reports.

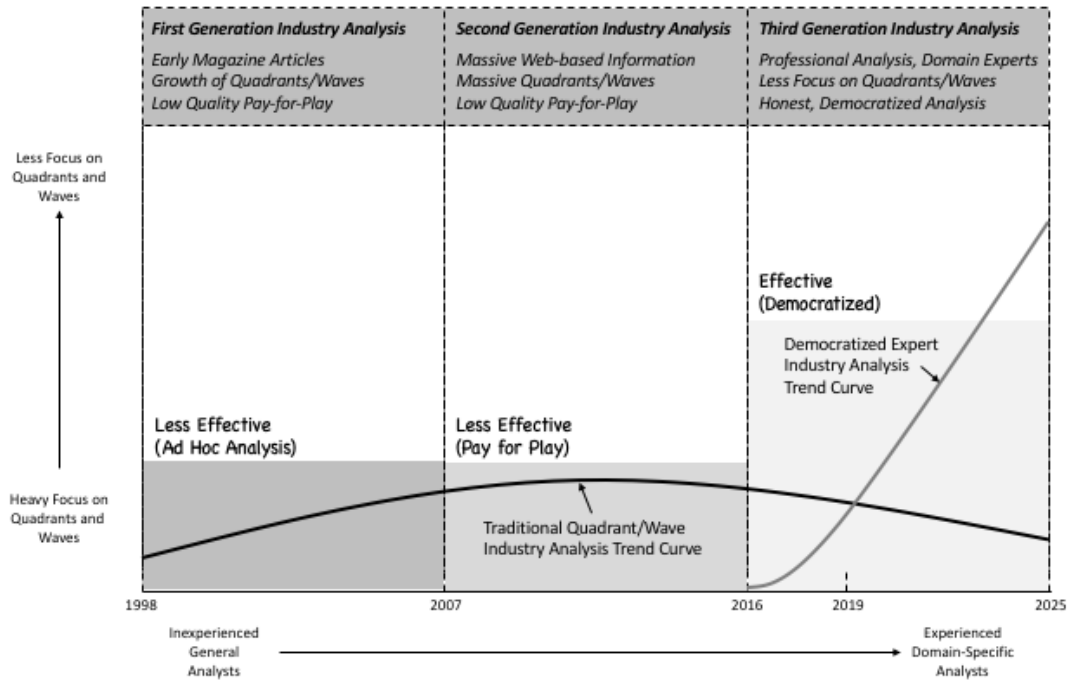


Figure 1-43. Industry Analysis Trend Curve

The future of industry analysis for cyber security lies in democratized, domain-specific guidance provided to enterprise teams by domain-specific experts who are unbiased and motivated only by the need to help reduce risk. This will change the nature of the provision of this information toward more democratized means such as social media, video, and other more accessible means for publishing timely guidance.

44. Information Assurance

The military sector adopted the phrase *information warfare* to designate its offensive use of computers and networks to achieve tactical and strategic goals. The term information assurance emerged as a complement to designate a more defensive approach to achieving military goals. As a result, cyber security solutions – often from commercial teams supporting military customers – have come to be referred to collectively as *information assurance*.

Information assurance solutions have tended to be characterized by three specific aspects: First, they are designed to be easily consumed by military organization; this often includes ease of procurement through military purchase schedules. Second, they are often a combination of hardware, software, and professional services, which is not surprising given the unique needs of the military. Third, they are characterized by unusually high levels of assurance and trust.

Many information assurance vendors in the defense industry have tried – usually unsuccessfully, to transfer their solution offerings to the commercial space. This would make sense on the surface, because banks and other large companies should covet the high assurance aspect of information assurance offerings. In practice, however, the unique marketing culture, lengthy sales cycles, and support processes have not transferred well.

The good news is that the government industry – across intelligence, defense, civilian, state, and local sectors – continues to have a healthy appetite for information assurance offerings from the best vendors. Since the barriers to entry in this marketplace are significant, including a willingness to put up with enormously long sales cycles, the companies offering information assurance products and services should see continued success and growth.

2019 Trends for Information Assurance

The most prominent trend in information assurance has included a shift from purely government oriented solutions – created and integrated specifically for government – toward more integrated solutions that include the best elements of commercial and government focused technology. The result has been a gradual progression from less effective early solutions in the first generation to more effective, expanded solutions today (see Figure 1-44).

In addition, early information assurance approaches included mostly simple, reactive cyber defense tools and programs – often based on intrusion detection. This has transitioned toward more modern, comprehensive and proactive cyber security solutions. Federal government customers in the US and abroad now enjoy world-class, highly effective offerings to protect national critical infrastructure.

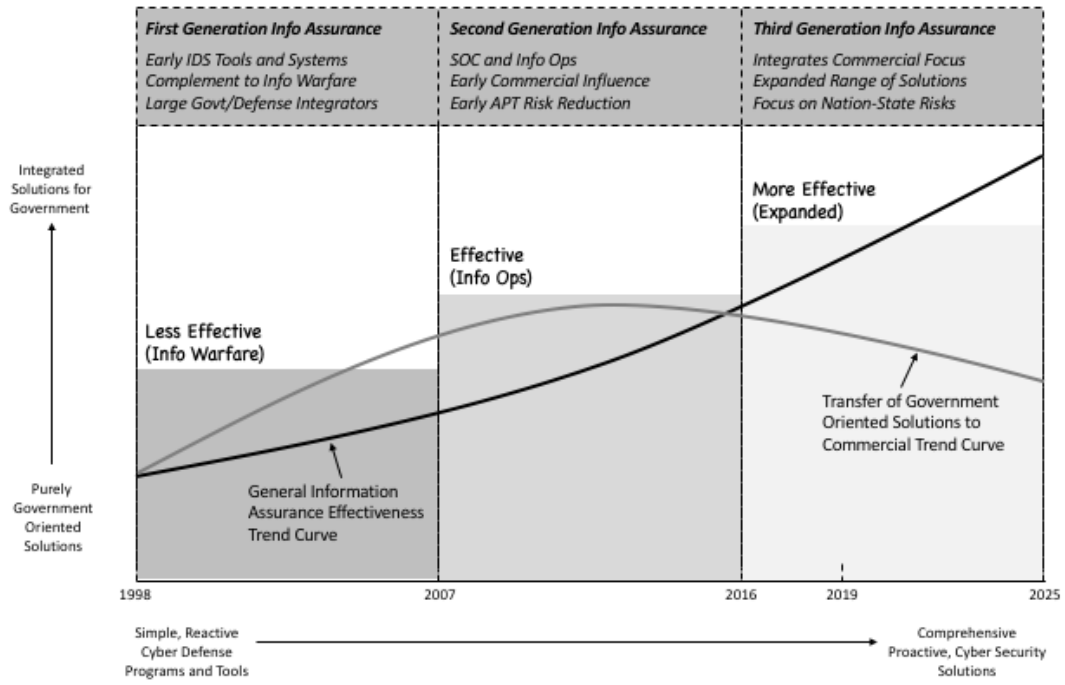


Figure 1-44. Information Assurance Trend Curve

The future of information assurance lies in even more advanced solutions to ward off information warfare actors who will use synthetic, imitation, and intelligence-assisted attack methods to create warfare havoc. The resulting increase in military and national threat will require that information assurance vendors keep up with the latest and greatest defensive techniques including the effective use of AI and machine learning.

45. Managed Security Services

The *managed security services (MSS)* sector in the cyber industry is likely to see the greatest pace of business change in the coming years as any aspect of the security ecosystem. Initially created to remotely monitor the health and status of firewalls deployed to customer gateways, the MSS solution space gradually morphed into a range of outsourced cyber security features marketed to customers.

The canonical MSS architecture has been relatively stable for many years amidst steady growth of the industry. It includes systems – hardware or software – being deployed into a target customer environment, with logs, alarms, alerts, and other telemetry being pulled back to a virtual or physical security operations center (SOC) for handling. An MSS might include status monitoring of deployed systems, or might perform monitoring with no management.

Telecommunications firms have been particularly well-positioned for MSS, simply because the management and monitoring functions match their normal telecom function so closely. This has allowed for easier business case approvals than in other firms with less applicable infrastructure. This advantage will continue for SDN deployments, where virtualized MSS will be an enormous growth engine – should telecom firms decide to follow this path.

2019 Trends for Managed Security Services

The effectiveness of managed security services (MSS) has transitioned from less effective early systems that collected intrusion detection alarms, through effective MSS offerings that began to include analysis in the monitoring function, into more effective current generation MSS that can handle virtualized deployments. The obvious shift coming will involve SDN-based MSS using dynamic service chains as the primary mechanism (see Figure 1-45).

The transition from pure hardware deployments with manual support and help desks toward virtualized deployments of software that benefit from automated support with many self-service features. This transition to automation reduces costs for MSS teams, but also tends to improve the quality of support for customers. It allows more on-demand provisioning requests and even modifications in some cases.

The up-down orientation of early management functions in the MSS has transitioned away from this health and status capability toward a more integrated, situationally-aware, and virtualized control of deployed systems. This results in MSS teams becoming a more capable security operations center (SOC) partner with an improved assortment of available services for business and government customers.

The most obvious and attractive such capability involves greater use of advanced analytics to detect indicators and identify – and even prevent – cyber threats to customer infrastructure. These analytics have shifted from simple correlation tools to behavioral analytics with meaningful underlying mathematical models. Additional introduction of AI and machine learning tools to the MSS SOC will provide even great benefit for customers.

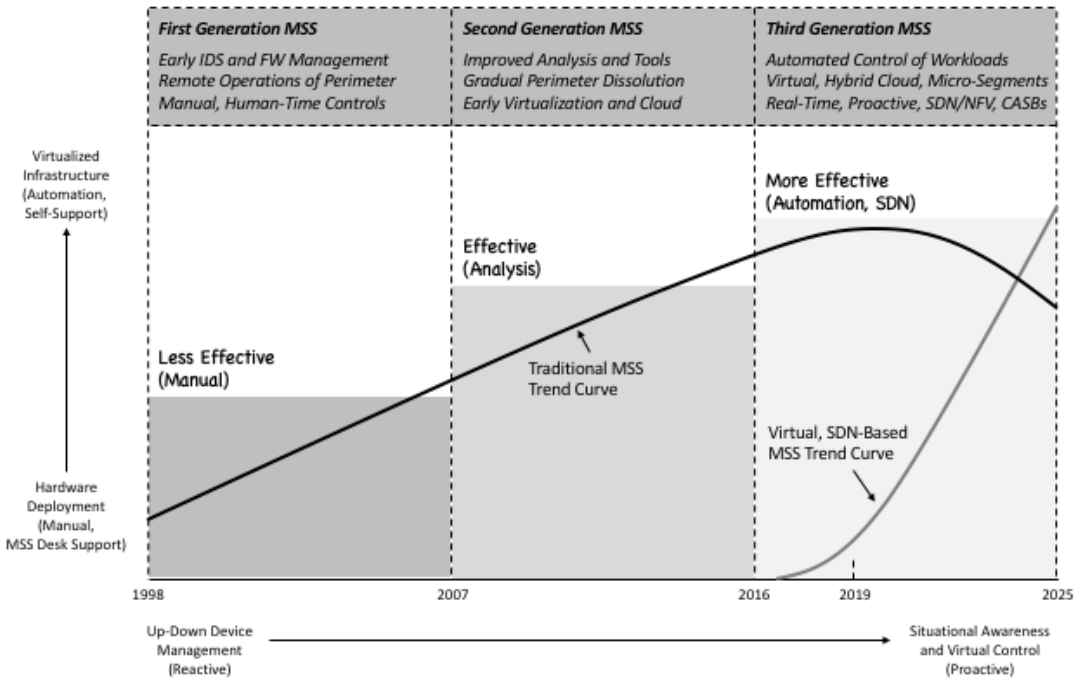


Figure 1-45. Managed Security Services Trend Curve

The future of MSS lies squarely in continued virtualization and a clear trend toward software-defined controls. Telecom firms with SDN-based infrastructure are best positioned to take advantage of this obvious match between MSS needs and dynamic service-chaining technology in SDN. Some question remains how aggressively existing MSS firms will pursue this high-growth opportunity. Ones that do not will see reduction in business growth.

46. Security Consulting

The *security consulting* industry has been, and will continue to be a steady growth engine, with excellent prospects for small, medium, and large companies offering all types of professional services. The need for excellent consultants will also expand from larger customers into a much larger base, including business customers of all sizes and shapes, and this does not preclude the micro-business community.

Security services for cyber range from high-level assessments of compliance, program effectiveness, and aggregate cyber risk – usually designed for executive consumption – to more detailed testing, probing, and even code reviews, usually designed for subject matter expert or working level consumption. It is accurate to imagine just about every possible permutation of service in-between these two ends of the spectrum.

It is not easy to isolate the components of security consulting as an industry sector, simply because so many adjacent areas of professional service exist. Information assurance for government, crowd-sourced vulnerability management, penetration testing, and compliance/risk management are all consulting activities, most of which are included in the portfolio of offerings from security consulting firms.

Furthermore, the small barriers to entry to become a security consultant will ensure continued flux and turnover for this sector of the market. That is, any individual or group of individuals with some skill or persistence can establish a consultancy in cyber security. In addition, product vendors often see great opportunity to tighten their relationship with customers – or just add some additional cash flow – through the provision of consulting services.

2019 Trends in Security Consulting

The effectiveness of security consulting services has transitioned from less effective simple assessments in the first generation from 1998 to 2007, through effective engagements with improved advice from 2007 to 2016. There are presently more effective security consulting services that include domain-specific advice on matters ranging from Internet of Things (IoT) to enterprise mobile security (see Figure 1-46).

The transition from generalized, high-level consulting toward more specialized, domain-specific consultants has mirrored the development of new domains, including critical infrastructure areas such as industrial control. The advice provided by security consultants has also transitioned from basic, general guidance on optimizing enterprise security toward architectural guidance, usually involving distribution and virtualization of resources.

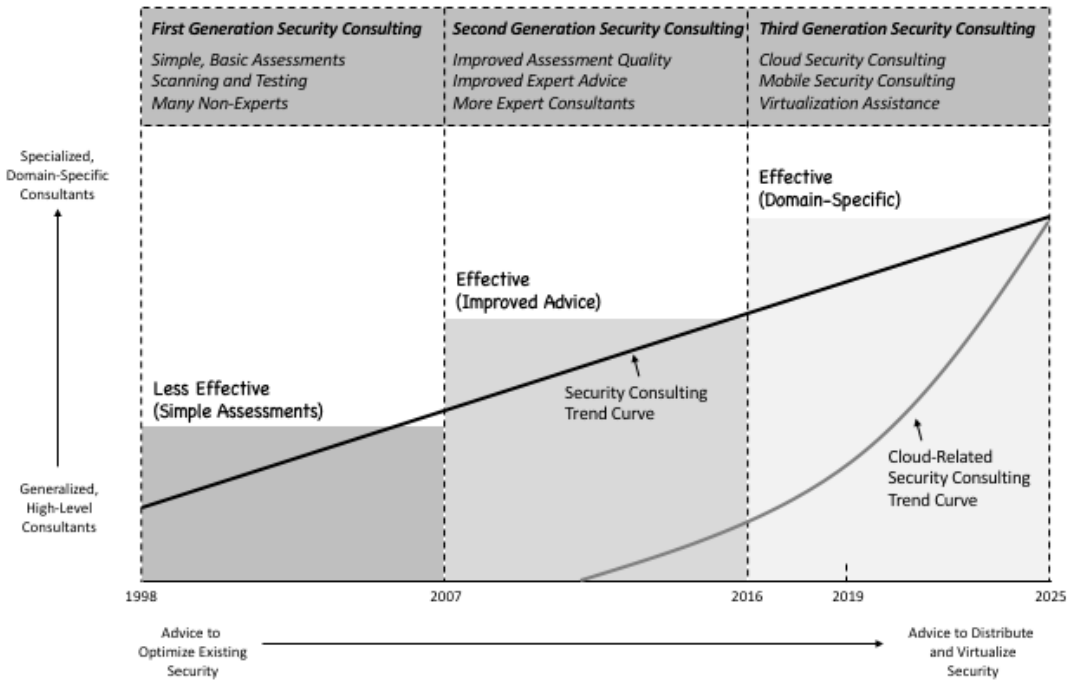


Figure 1-46. Security Consulting Trend Curve

The future of security consulting lies in more advanced, domain-specific services, including advice and guidance for enterprise teams moving in the direction of full public cloud use. Risk-based services with focus on executive reporting will also be an enormous growth area as CISOs move up in the corporate hierarchy. The need to provide cyber risk information through consultation engagements will create considerable growth in this area of the industry.

47. Security Career Support

Providing programs of *security career support* might appear an extravagant luxury for executives and practitioners, but nothing could be more distant from the truth. If enterprise managers would like to retain world-class staff, while also ensuring a constant in-bound stream of new talent for their cyber security groups, then they will have to build effective programs for supporting the careers of new and existing security staff.

Such programs should include heavy emphasis on learning, skills assessment, and coaching – all of which are growing areas in cyber security professional services. But security career support also requires a good working relationship with the best recruiting firms offering services to growing teams. External recruiting is sometimes viewed as evil, often coupled with the practice of firing existing staff; but more often, it involves finding and adding talented individuals.

The two canonical approaches to recruiting in our industry have been so-called contingency recruiting and retained search. In the contingency case, the recruiting company works on a negotiated percentage for staff that are located and ultimately hired. In the retained case, the recruiting company is paid an up-front fee. Presumably, retained search results in a more comprehensive analysis, but no scientific studies exist to substantiate this view.

The increasing recruitment of freshly graduated computer science majors to cyber security has been a growing aspect of the industry, and is a welcome trend. Most computer science programs include some degree of introduction to cyber security, and younger employees tend to be savvy in their understanding of modern technology, cloud and mobile services, and cyber security services.

2019 Trends in Security Recruiting

First generation security recruiting from 1998 to 2007 was less effective and involved mostly headhunters with sometimes unsavory practices. Second generation security recruiting from 2007 to 2016 was characterized by effective practices with increased partnership focus. Current generation security recruiting is more effective and includes a holistic approach to executive, middle management, and new hire recruiting for cyber (see Figure 1-47).

Security recruiting has shifted from an isolated focus on specific job search toward a more holistic focus on career management. This is also characterized by a shift from transactional retained and contingency search deals toward a more relationship-based approach followed by the security recruiting firms as well as enterprise teams looking to build their talent from both internal and external sources.

One trend that works slightly against the security recruiting business has been a slight, but growing trend toward internal development of talent. Early generation security executive positions had no younger bench to draw from, but this is different today. Most enterprise security teams now have several years of experience as a group and this will create internal candidates for new executive positions.

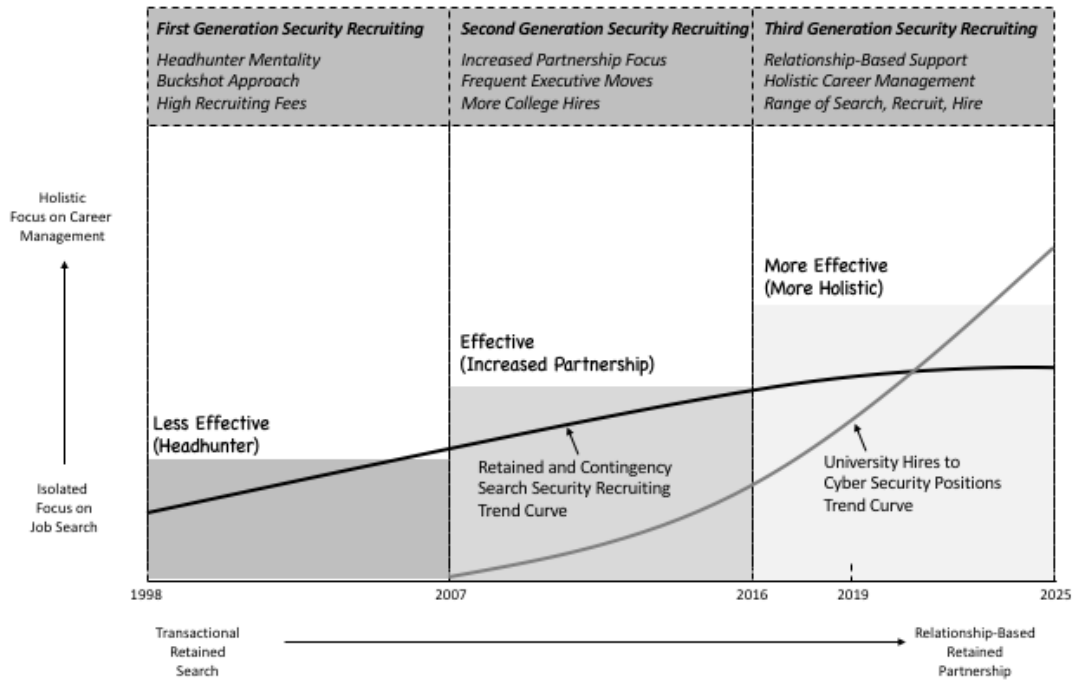


Figure 1-47. Security Recruiting Trend Curve

The future of security recruiting is all about holistic relationships that are less transactions and more career focused. That is, the best security recruiting firms will take the time to understand the long-term goals of their customers and will tailor their support and services to meet those needs. This might even include assistance identifying newer employees directly recruited from their university programs.

48. Security Research and Development

To date, the *security research and development (R&D)* community has existed within academia, federally-funded research and development centers (FFRDCs), university affiliated research centers (UARCs), and other non-profit organizations. It remains unclear why more successful commercial opportunities have not emerged in the marketplace for pure and applied research teams providing cyber-oriented R&D for customers.

The value of security intellectual property (IP) has certainly not shrunk in recent years, so this relatively quiet attention to security R&D as a commercial pursuit is surprising. Nevertheless, any commercial organization that would like to deeply research some aspect of security will have to turn to internal resources, academic organizations, or a non-profit. The defense industry is perhaps an exception with many system integrators including R&D as an offering.

Note that by 'security research,' we do not mean investigation of vulnerabilities or black hat pursuits of finding exploits in systems. While many refer to this as research, we choose to call this 'vulnerability management and penetration testing'. Finding errors in someone's bad code or holes in someone's horrendous system design just doesn't seem to fit the bill in terms of what we would call world-class cyber security research.

2019 Trends in Security R&D

The early days of computer security in the 1980's and 1990's included considerable research in trusted computing design, high assurance computing, security policy modeling, information flow mathematics, and on and on. It was a substantive component of the industry, as evidenced by the degree of focus afforded such research concepts in the earliest major computer and information security conferences (see Figure 1-48).

In the 1990's, the research environment down-shifted as commercial interests overtook research interests – except in the areas of academia and non-profits mentioned above. A second generation ensued which we refer to as the Dark Age of Cyber Research. During this period from 2007 to 2016, all advances in security seemed connected to a start-up or commercial engagement, simply because the business prospects of security were too irresistible to ignore for most innovators.

The present, third generation of cyber research is likely to shift back into focus with a more defensive-orientation than the original offensive focus that characterized many earlier efforts. With organizations, especially in government, understanding the value of pure and applied research, it should be easier for research teams to procure funding and even commercial profit in their engagements.

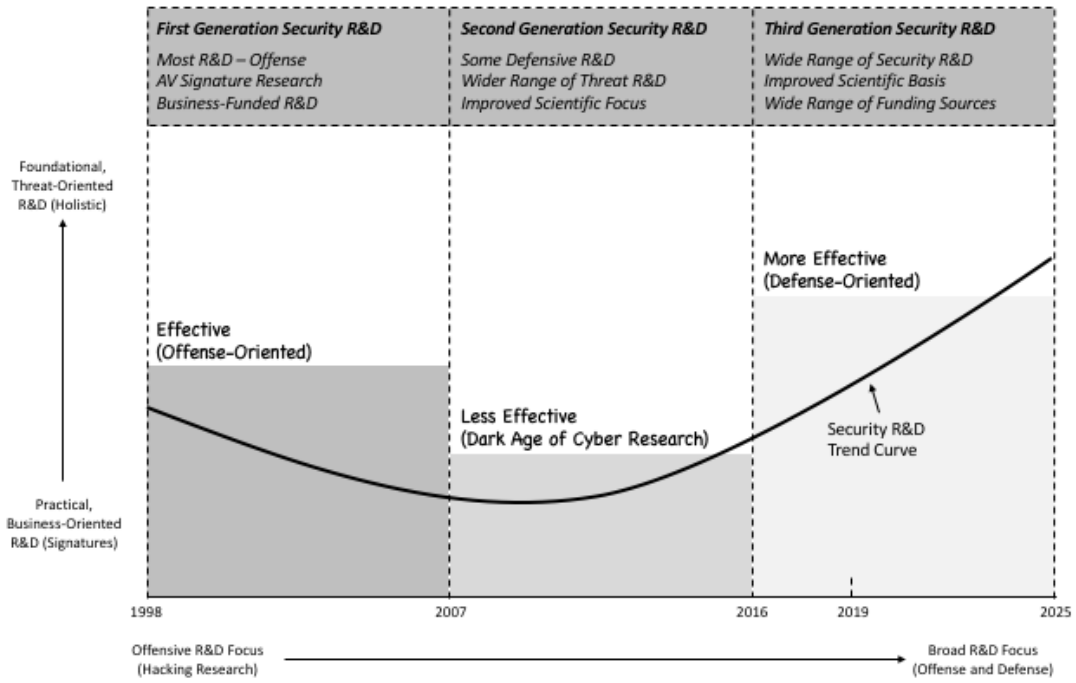


Figure 1-48. Security Research and Development Trend Curve

The future research focus areas for security will track the major advances of the day – including autonomous computing, artificial intelligence and machine learning, increased automation of industrial control systems, smart medicine, and on and on. In each of these areas, foundational research is required to provide a suitable base on which to design and building meaningful operational systems.

49. Security Training

Security training can be delivered as general *security awareness* for anyone in contact with organizational assets, or as *expert training and certification* for practitioners who need more advanced education in cyber-related technology, procedures, or policies. Both approaches are moving toward more creative, hands-on, multi-media training, often delivered virtually, in ways that support the most flexible learning environment.

Security awareness is an efficient form of enterprise risk reduction, simply because user behaviors contribute directly to the success (or failure) of many different security attacks. Even the most advanced persistent threats (APTs) from nation-state actors will generally include exploitation of human weaknesses. So, training employees to be savvier, especially about email phishing probes, is an excellent investment.

Expert training and certification in cyber security also provide good returns on investment, although the quality of the training will vary. Security conferences, such as the massive RSA gathering each year, generally include many professional training opportunities. Increasingly, though, courses tailored to specific disciplines such as firewall administration or cryptographic protocol management, are available for practitioners.

2019 Trends in Security Training

First generation security awareness programs were less effective, generally offered as stiff directives from early security practitioners with weak training skills. Second generation security awareness became effective as early use of video and some on-line options were made available. Third generation security awareness programs should be expected to become more effective, with maximal use of creative training options (see Figure 1-49).

Expert training and certification in security was less available in the early years, mostly obtained through conferences, books, and other materials. Good on-line options for experts who need domain-specific training in cyber security have begun to grow dramatically, and this represents an excellent advance for practitioners. Virtually every aspect of cyber security technology, procedures, and practice have great options for on-line learning today.

The trend for both awareness and expert training as been from general coverage toward more focused training on domain-specific areas. Additionally, the early conventional InfoSec sessions of the 80's and 90's for general and expert audiences, have been replaced with social, viral, and video training options. Certifications continue to lag somewhat, although the Certified Information Systems Security Professional (CISSP) is still popular.

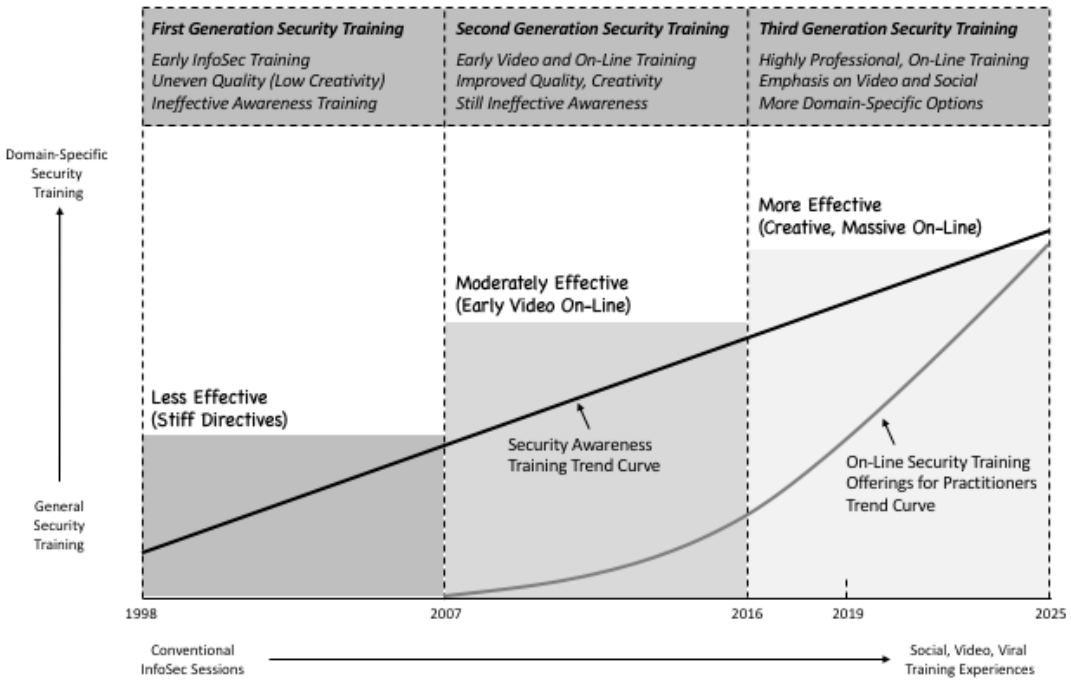


Figure 1-49. Security Training Trend Curve

The future of training for both general awareness and expert learning involves even more creative options for video and social learning, as well as greater use of massive open on-line courses that allow learners to progress at their own pace. The quality of these courses has steadily increased to the point where some match the best available options from even the best universities.

50. Security Value Added Reseller

The earliest purpose of the *security value added reseller (VAR)* was to assist with the selection, procurement, payment, maintenance, integration, update, support, and replacement of cyber security solutions for the enterprise. This function was particularly valuable in the context of the relatively lengthy cycle times for introducing new hardware/software-based systems such as firewalls and intrusion prevention systems.

The original benefit for vendors was also quite powerful, in that the best security VARs offered channel opportunities that many smaller start-ups couldn't otherwise fathom. Even larger vendors benefitted from the expanded channel, especially in remote regions of the globe where a local VAR knew the language, culture, and customs of potential enterprise customers of their supported vendor products.

More recently, the security VAR has had to adjust to an increasingly virtual world – one in which the selection and procurement of vendor solutions is moving toward a point-and-click type arrangement. This is both a challenge and an opportunity for the best VAR teams, because with this general transition away from hardware purchases (not all, obviously) will come the need for good professional services to guide enterprise teams toward the right approaches.

An important area in which security VARs are advised to focus is the transition to cloud-based services for most enterprise team. Selecting and integrating the best available tools for micro-segmentation, CASB integration, cloud-based IAM, and cloud compliance will require the trust and support that security VAR teams have already established with their clients. This will give the security VARs an advantage over many existing security consulting teams.

2019 Trends for Security VARs

The effectiveness of security VARs during the first generation was based on one-stop shopping as part of the enterprise relationship. This was followed by a recent second generation of security VARs, where too many companies were vying for a reduced number of transactions, with weak focus on emerging cloud systems and virtualized data centers. The emerging third generation will be effective and focused more on relationship-based work (see Figure 1-50).

A transition occurred in security VAR solution provision from mostly hardware sales and support toward emerging support for hybrid cloud architectural support in the areas of strategy and planning. An additional transition occurred from the administration of product resale, toward the emergence of security VARs as solution consultants and trusted partners for enterprise security teams.

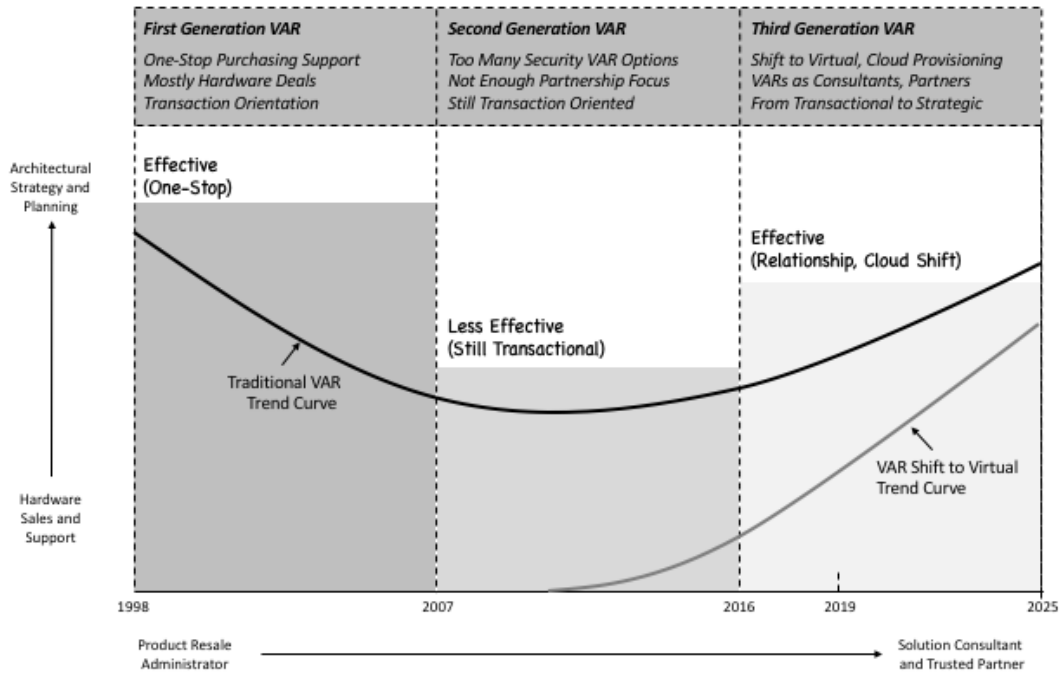


Figure 1-50. Security Value Added Reseller Curve

The future of the security VAR will see a massive shift toward relationship-based consulting with higher end services at higher margins for companies moving toward hybrid cloud arrangements. This is good news for the best security VARs who will seize the opportunity, but terrible news for any security VAR that is determined to resist change and cling instead to older business models that will not work in a hybrid cloud-oriented world.