sertainty
data: empowered

GIVE DATA LIBERTY OR DEATH

A New Paradigm for Cybersecurity in the Data Supply Chain

“We’ve spent a lot of time in the last 20-30 years protecting the perimeter of the enterprise. But the reality is that with the cloud…there is no perimeter anymore; the reality is that your data is everywhere.”

THOMAS SASALA,
CHIEF DATA OFFICER | U.S. NAVY

A Much-Needed Breakthrough in Data Security

"We have to move towards where our data is far more aware and that our data is essentially helping to protect itself, so that it knows where it is, who's trying to access it, and really a lot of context around it so that it can be protected, whether it's on a computer that gets lost in a parking lot or left on an airplane or someplace else."

GRANT SCHNEIDER, US FEDERAL CISO

In a 2018 panel interview, Grant Schneider, US Federal Chief Information Security Officer and the National Security Council's Senior Director for Cybersecurity Policy, articulated the need for security at the data level itself. Note how he uses the term "aware" to describe how secure data might behave in context-sensitive ways to protect itself.

Thomas Sasala takes it a step further. Sasala, Chief Data Officer for the U.S. Navy, articulates both why we need data-level security, and what it might mean for user access.

- "The adversaries are not stealing our network; they're stealing the data on the network."
- "[If] the data isn't protected at the data level — not at the perimeter level or even at the server, system or application level — then we're not going to actually survive moving into the future."
- "Data at rest, data in transit, data encryption: these things all need to be tied together…"

Sertainty offers breakthrough technology in that it gives data the awareness to act and react, creating a new level of protection at the data layer.

This paper discusses the Sertainty breakthrough as it applies to the DATA Supply Chain.

Executive Summary

DATA has a supply chain. For most enterprises, workloads (including security workloads) are moving to the cloud, third-party web services are replacing traditional in-house functions and endpoints have migrated outside of the firewall. This makes traditional perimeter-based security controls less and less effective. DATA is unprotected at the delivery point. The only ideal future state is one in which security travels with the data itself and extends monitoring, visibility and risk mitigation from internal to external networks. Sertainty provides a practical way to effect this solution throughout the DATA Supply Chain.

To gain maximum value for its data, each enterprise must maintain control of its data. Because that data might be information related to their customers, might include Personally Identifiable Information (PII) or Intellectual Property (IP), its value is immense. While customer PII is valuable to cybercriminals, an enterprise's IP — trade secrets, formulas, designs, source code — is the more valuable. Stealing IP can not only save millions and millions of dollars, but more importantly, save time. Years, in many cases. And, obliterate any competitive advantage. More often than not, cybercriminals collude with an insider to steal IP.

To truly prevent IP theft, security and risk professionals must not only protect data at the data level but also strictly control access to the sensitive information, monitoring and mitigating risk in real-time. By simply embedding the Sertainty Intelligence Module into the data-file, Sertainty enables anomaly prevention, policy enforcement and risk management at the data-layer in real time, throughout the DATA Supply Chain.

The Sertainty Self-Protecting-Files Platform (SPFiles) makes it easy for customers to create and deploy self-aware, self- protecting data-files. This serverless solution ensures the protection and integrity of cross-domain, data-at-rest-in-flight workflows, eliminating man-in-the-middle threats.

Enterprises can extend the security infrastructure to the supply chain and gain operational agility through seamless file-sharing, automated policy enforcement and an irrefutable, data-layer event log. Sertainty SPFiles introduces an efficient and effective protection solution at the data-layer for data on and between dissimilar networks. By eliminating the dependency on multiple perimeters and related transport infrastructure, Sertainty SPFiles makes it possible to exchange valuable information between disparate and siloed systems – efficiently, safely and without giving up control to the "insider."

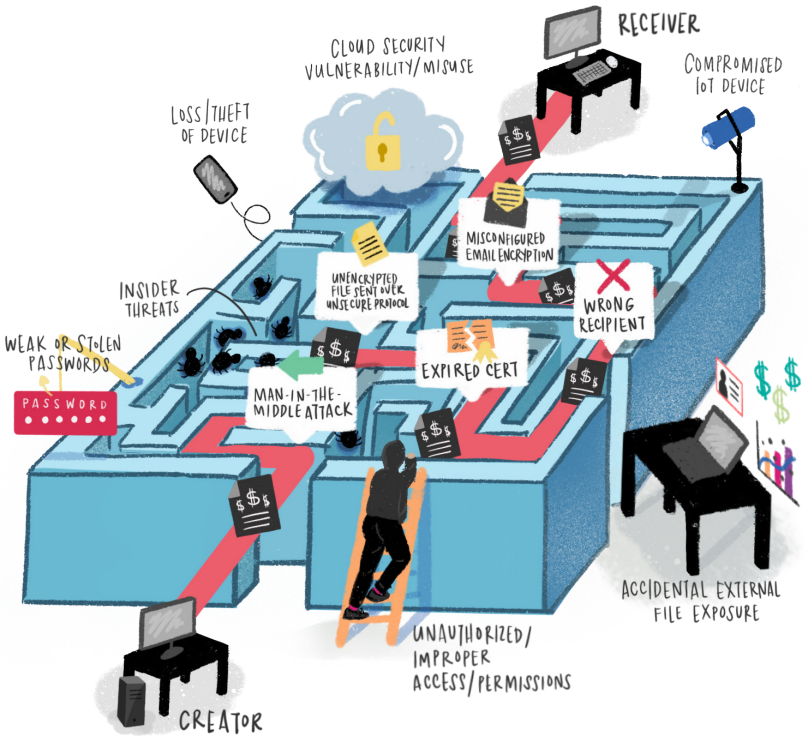
Vulnerability in the DATA Supply Chain

Companies, whether intra-networked, inter-networked, or cross-domained, currently employ solutions that have been developed over generations, using time-tested data security practices and products. But, the DATA Supply Chain is one of re-packaging and how human mistakes circumvent enterprise systems security policies and practices. It consists of many fractured process steps. While these practices, products and processes have been largely successful in protecting valuable data, they were designed around the assumption that data must always be available when needed. Consequently, current security approaches focus on building labyrinthine defenses around ostensibly defenseless data. This byzantine process is not a solution, it is the problem. It is not applicable to the DATA Supply Chain. These defenses must then be navigated in sequence—like a maze—in order to share data. Consider:

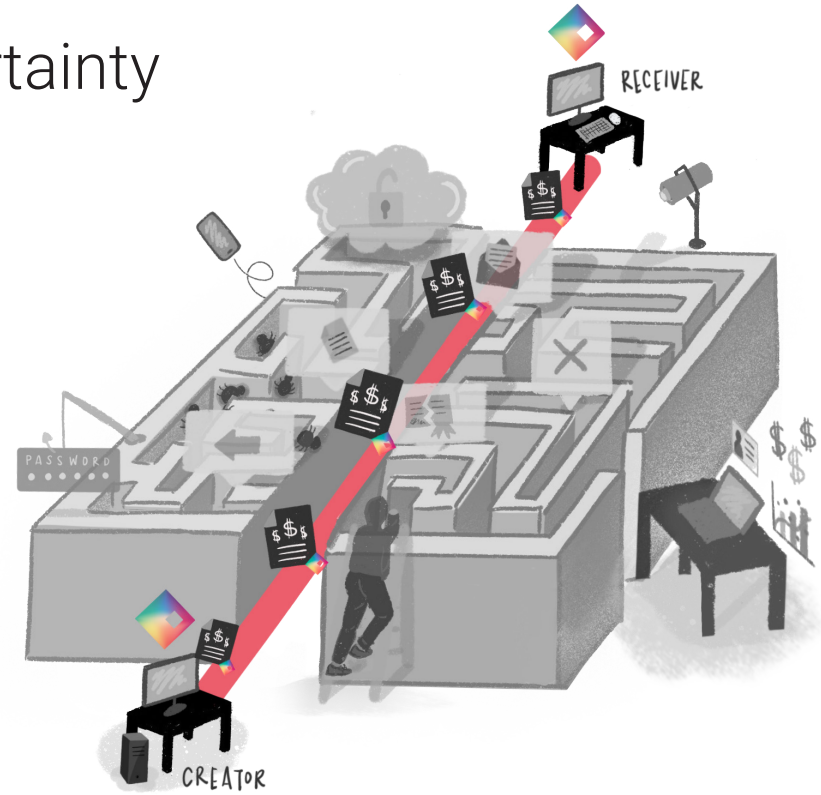
- **Defensive/offensive physical controls**, such as firewalls, proxy servers, and endpoint-protection solutions all require discrete management, and they have no effect when data is outside of the enterprise-controlled environment.
- **Data encryption,** while the most effective way to protect data in all forms, is complex to implement and manage, is highly susceptible to human error, and in its current implementation actually introduces moments of complete vulnerability into the data supply chain.
  - Encrypting data at rest locally requires one application and key(s), often built into the operating system of the local machine, while encrypting data in a remote/cloud environment requires another application and key(s).
  - Encrypting data during sharing/moving requires another method of key management altogether, depending on the protocol. SSH, SSL/TLS, VPNs, PKI, etc.: each require separate, discrete key and identity management systems. Additionally, these keys and systems require absolute protection from theft, creating the need for yet another security solution.
  - The fatal flaw in these two scenarios lies in the fact that — in the current world of encryption — the file must be fully unencrypted to be used. This is true whether it stays in the same location or is shared via another secure protocol in the data supply chain. Every new security protocol added to the data supply chain inescapably introduces another moment of vulnerability. The more protocols in the chain, the more instances of vulnerability, as data is unencrypted by one protocol in order to encrypt it in another. However brief the interval, such moments are pivotal opportunities for damage or theft by malicious actors.
- **Data cannot manage who accesses it,** what is accessed, where access occurs, or anything else about itself. It requires external management and control systems — systems that can be bypassed or exploited by someone who has obtained superuser credentials — to set and monitor access parameters.
- **A data owner is dependent** on the external encryption controls in order to protect the data. The data can determine neither who created it, nor who owns the information it contains, nor whether anyone has tampered with it. In other words, the data owner cannot ensure the integrity of the data's value.

In today's cloud-based, BYOD world, these legacy PKI-dependent protection methods are proving ill-suited to ensuring data integrity across environments and throughout the DATA Supply Chain.

Today



With Sertainty



Sertainty Technology: An Overview

While CISO's have inherited IT cybersecurity tools and process that focus on continuity of operations, user-based event analytics and automated hunt capabilities, malevolent actors have continued to steal and exploit valuable customer and company data --- threatening the company's survival. Trillions of dollars of Intellectual Property are siphoned out of our Nation on an annual basis. We believe this fundamentally weakens our Nation and ultimately puts our citizens at risk. We want to stop it.

The Sertainty solution overcomes all of the byzantine steps associated with the DATA Supply Chain and allows/enforces data access of singularly controlled and audited data objects that are always protected by a homogeneous set of policies and tools.

The Sertainty Self-Protecting-Files Platform implements the Sertainty Intelligence Module to effect data-layer protection and policy enforcement in and between enterprise and cloud security infrastructures. The Sertainty SPFiles is a serverless solution in the form of an agent located on file-creator and file-user machines. The agent creates Sertainty files and enables access to information in those files through the embedded Sertainty Intelligence Module. In turn, Sertainty files ensure self-protection, monitoring, authentication and approval within an existing data flow, whether intra- or inter-networked, for data-at-rest and data-in-transit, without any required code changes to native applications. Because the data defends itself, it allows a user to share information easily and with confidence. Put simply, the Sertainty SPFiles bypasses the old security management maze altogether.

Sertainty technology uses the strongest level of encryption authorized by the National Institute of Standards and Technology (NIST) for global utilization. The SPFiles eliminates the dependency on PKI, EKM and MFT solutions for encryption and policy enforcement. Additionally, Sertainty makes it virtually impossible to spoof the creator/user/data relationship, no matter how torturous the DATA Supply Chain path.

Sertainty Technology: An Overview

END-TO-END-TO-END PERSISTENT PROTECTION: SELECTIVE DECRYPTION

Sertainty technology is about stopping the malevolent actor not about "access control" to files: it's neither an IAM nor a DRM solution. Instead, it controls access to information *in* the files. Each embedded Sertainty Intelligence Module is unique to each file and manages its own symmetric encryption keys. Likewise, it enforces the embedded security protocols. In this way, the safety and integrity of information contained in the files along the entire supply chain is maintained without a dependency on local network apps or remote servers. What's more, using the Sertainty Self-Protecting-Data Platform makes it possible to enable access to information on a selective basis: user (person or machine) access can be controlled to a granular level according to policy. No person or external process has access (or need for access) to any keys. This features prominently in the case study which appears later in this document (see "Efficacy" section later in this document).

POLICY ENFORCEMENT: ANOMALY DETECTION AND REAL-TIME MITIGATION

The Enterprise wants to extend enforcement of its policies throughout the DATA Supply chain. When the embedded Sertainty Intelligence Module is activated by the SPFiles Platform, the Sertainty file becomes "aware" of its environment. The Sertainty file detects and defeats anomalies in real-time — from an illegitimate access attempt to an unrecognized location, network, or device, the wrong time of day or an apparent tampering effort. In each case, the Sertainty Intelligence Module can take any number of actions prescribed by Enterprise policy to defeat the anomaly, ensuring compliance, mitigating or eliminating risk in real-time.

AUDIT AND EVENT LOGS: DATA AS AN ENDPOINT

The wanton theft of our Nation's Intellectual Property ultimately puts our citizens at risk. Just like the members of our own families, we want to know we are safe. Businesses want to know their data is safe – who is accessing it – which is no longer possible when it leaves their networks. The Sertainty file captures every action taken by users, records it, and reacts according to policy. The embedded event log captures access attempts (both successful and unsuccessful), additions, modifications, deletions, signatures, time and location of the activity, user, and more. Activity can be recorded and maintained within the Sertainty file, exported via email or other means, and stored in an external repository or SIEM tool. These embedded event logs cannot be edited, making them a powerful resource for legal entities and businesses to track and verify specific behaviors. In this way, embedded event logs satisfy many auditing requirements, including login activity, user activity, information access and tampering. The Sertainty file, from the network's perspective, is an endpoint.

The Sertainty Value Proposition: Risk Calculus

The probability of failure is the sum of all probabilities that any one component/process will fail. As the number of components/processes increase the probability of failure increases.

- We need to reduce the number of protection steps the data takes as it transits the DATA Supply Chain
- The probability of data loss decreases when there is uniformity of data protection methods throughout the DATA Supply chain

The SPFiles Platform resolves data-at-rest-in-transit complexities and vulnerabilities, thereby reducing risk. Moreover, because it depends on neither storage nor transport infrastructure for protection and policy enforcement, the SPFiles:

- Eliminates the risk of breaches at the storage or transport layers, thus further reducing risk
- Minimizes, and in some cases eliminates, the operating costs of traditional encryption key management and digital rights management solutions, thereby reducing the vendor's (supply chain) capital and operational investments

The Sertainty Self-Protecting-Files Platform enables an enterprise to interpret and manage their valuable information as a protected, self-managed, mobile endpoint.

- With uniformity of data protection processes, uniformity of data handling policies will follow and thus risk of loss will decrease further
- With uniform data protection and policies the entire DATA Supply Chain risk can be modeled and computed to provide both enduring security and flexibility for all businesses

Efficacy — A Study in Transformation

THE SETTING

Transformations, Inc. (TI) is a Critical Communications Management (CCM) software provider to Print Service Providers, Business Process Outsourcers and Enterprises. Customers in a variety of sectors including healthcare, finance, utilities, insurance and law use Uluro®, the TI CCM platform for print, mail and web presentment of transactional documents. TI's customers compose, present and send sensitive and confidential documents, such as invoices, payments, bankruptcy notices, banking and benefit statements.

TI customers need consistency, speed, simplicity, and assurances of compliance. The value they derive from adopting the Uluro platform lies in how effortlessly they can communicate with both customers and vendors while maintaining brand standards and the integrity of data. Given TI shares the Sertainty belief, that theft of proprietary and confidential information ultimately puts consumers at risk, it's no surprise that they place a premium on protecting data and assuring compliance. TI customers must comply with PII, Payment Card Industry (PCI), HITRUST and similar regulations, thus are attractive targets for malevolent actors. The value of CCM offerings depends on assuring data privacy even as the frequency of cyberattacks in those sectors has skyrocketed in the last few years.

THE CHALLENGE

Previously, the only method available to TI for protecting information in their DATA Supply Chain was persistent end-to-end encryption. For Uluro customers, this meant that the data had to be decrypted and re-encrypted repeatedly as it passed from one stage in the workflow to the next — requiring multiple sets of keys — with each step in the process increasing the opportunity for human error and malfeasance. TI needed a more efficient way to secure that data, so it could deliver higher assurance to its customers that their data's integrity was intact.

THE SOLUTION

TI partnered with Sertainty Corporation to develop a persistent, end-to-end, B2B2C DATA Supply Chain data protection solution for its Uluro offering. Using the Sertainty Self-Protecting-Data Enterprise Platform, Transformations built industry-first software solutions (uProtect, uSecure, and SmartDelivery) implementing Sertainty technology without having to alter the underlying Uluro architecture. They developed a persistent, selective decryption methodology, ensuring the right information was decrypted for the right user at the right time, without exposing any other information in the file. This workflow solution keeps data secure throughout the entire production and communications process in a manner that is simple, economical and productive, and which removes human error from the equation.

THE RESULTS

TI's visionary standing enables their customers to avoid unneeded investments in either human capital or network infrastructure. "It's very difficult to produce products that change markets," says Bill Tidwell, TI's CEO, "but Sertainty Self-Protecting-Data does just that." By implementing Sertainty technology, TI has enabled their customers — and their customers' customers — to attain a competitive advantage in highly regulated markets that are under constant and intense pressure from cyberattacks.

THE NEXT GENERATION

Sertainty technology transforms the data protection paradigm of the DATA Supply Chain, making it possible to mitigate risk, improve compliance and reduce costs. Because data defends itself, TI clients and their customers no longer worry about compromise of valuable information. They can exchange valuable information without losing control, they can use cloud services with confidence, they can assure compliance at lower cost, because Sertainty Self-Protecting-Data is "aware." Whatever the uncertainty of the next generation of malevolent actors or what may come in the next iteration of data storage and sharing, Sertainty technology assures TI's DATA Supply Chain to be future-proof.

sertainty
data: empowered

While industry-standard security protocols have a long and storied history of efficacy, collectively have become unwieldy to manage in an uncertain world redefined by the DATA Supply Chain. Worse, they were not designed to protect information at the level at which it is increasingly being targeted: the data layer. The Sertainty solution sets the standard for data-centric security, protecting our Nation's Proprietary and Confidential Information, our Intellectual Property, and enables organizations to monetize their valuable information without compromising protection, performance or privacy.

To learn more about Sertainty and how it can transform your own DATA Supply Chain, click the link below.

www.sertainty.com

sertainty.com | sales@sertainty.com