PRODUCT OF THE MONTH

sertainty

Self-Protecting-Data (SPD) Technology Platforms

Mihir Bagwe, Technical Writer
CISO MAG

CISOs are investing more in cybersecurity tools and processes that focus on data supply chain operations, user-based event analytics and automated threat hunting capabilities. Security professionals have implemented countless defensive measures and complex encryption solutions, yet attackers have somehow always managed a way to circumvent them. Attackers and threat actors have evolved, stolen and exploited the most valuable customer and company asset – DATA. The size of the organization and the quantity of data do not matter, big or small, they are all targets for attackers.

Data is passive and defenseless in systems that are inherently vulnerable. Systems were never designed to control data but to protect it. The problem with data is that its neither self-protecting nor self-aware; it can be manipulated, exposed and exploited. But imagine a solution that transforms your data into a self-reliant, self-aware and self-protecting asset.

Data Security with 'Sertainty'

The Sertainty Self-Protecting-Data (SPD) technology enables developers to mix intelligence into data-files, giving data an ability to act and react to its environment. It shifts data control and risk mitigation from an indirect/re-active paradigm to a direct/active paradigm by delivering "data-layer" governance, provenance and protection into your intra and inter-network data workflow solutions.

Sertainty SDP technology reduces the dependency on trusted insiders and system hardware. It enables the data-owner to store and share valuable information without increasing the risk of data leakage or manipulation. No longer is there a perimeter or extraneous control of data exerted by an application like a firewall or other system; the data **controls, protects** and **mitigates risks** itself – in real-time.

PRODUCT OFFERING

SERTAINTY SELF-PROTECTING-DATA TECHNOLOGY PLATFORMS

Enterprise Self-Protecting-Data platforms include the **Self-Protecting-Files Platform**, **Self-Protecting-Messages Platform** and the **Self-Protecting-Cloud Platform**. Each are augmented with Mobile Channel add-ons (Android, iOS) and SIEM plug-ins (Splunk, Devo, Elastic). Sertainty SPD technology is agnostic to OS and cloud architectures.

SELF-PROTECTING-FILES PLATFORM

The Self-Protecting-Files (SPFiles) Platform provides for a serverless SPD solution. It allows system administrators and integrators to deploy, assign, monitor and enforce encryption and governance policies – **at the data layer** – to BOTH data-at-rest and in-flight, without having to manage the transition.

The SPFiles Platform includes a developer's kit (SDK) allowing custom build of an SPD application. SPD's ability to selectively decrypt information in the data file for any given user ensures that the right user, at the right time, has the right information, without exposing any other information in the file. A user, at the right time, has the right information, without exposing any other information in the file.

SELF-PROTECTING-MESSAGES PLATFORM

The Self-Protecting-Messages (SPMessages) Platform provides an effective way to implement secure machine-to-machine or node-to-node messages where encryption is heavy and maintenance intensive. SPMessages is a light-weight mechanism for IIoT, SCADA, ICS communication environments for machines, devices and applications to guarantee the integrity of the message and ensure both the sender and receiver to be legitimate.

SELF-PROTECTING-CLOUD PLATFORM

The Self-Protecting-Cloud (SPCloud) Platform is a backup data protection and recovery solution, providing any business to quickly access their backup data in the event of ransomware, disruption or destruction, resulting in limited down time and minimal cost to continue productivity.
Compliance with regulations such as GDPR, CCPA, HIPPA, PCI and NIST 800 is increasingly required of all participants in the supply chain and Sertainty's SPD Platform enables an elegant and simple solution to comply with these regulations.

SALIENT FEATURES

Governance	Provenance	Protection
With Sertainty, data governs itself by first determining its environment (physical device, location, time, etc.) when any entity attempts access to important information. If an anomaly is detected, the self-governing data takes appropriate action. This includes denial of access to data, alerting the data-owner, requesting access permission from an external authority, presenting an alternate or hoax view to the user or process, and in certain scenarios self-destruct to mitigate risk.	Sertainty deploys anti-tampering technology and maintains a record of ownership which assures integrity of the data. The record of ownership includes environment(s), access attempts and event occurrences. These event logs are irrefutable, provide a chain of custody and are protected with Sertainty SPD technology.	Sertainty technology provides security and controls within the data file, reducing the dependency on infrastructure (hardware, firewalls, endpoints, etc.) for protection and governance. Encryption keys are never exposed. Instead, your data manages the keys internally, removing the vulnerability of shared/stolen keys.