Trusted Cyber Technologies

THALES

Securing the Keys to the Kingdom

White Paper

As technology has evolved, the array of devices, applications and infrastructure have exploded, each providing a specialized type of data, protection or service. Distributed systems handle transactions; security/monitoring infrastructure monitors for breaches and slowdowns; a myriad of applications make the best use of Web technologies. Each of these elements generate machine data that can be used to provide competitive advantages, gain insights into customer behavior and avoid security or compliance issues.

Enterprises have long sought for a solution to bring this vast amount of disparate information together to provide invaluable insight into enterprise systems. If such information was correlated, however, another vitally important issue arises – how to secure the resulting data. While the benefit of overarching data to the enterprise is obvious, it is also valuable to hackers, competitors or insiders, as well as vulnerable to inadvertent exposure.

This paper examines the use of Splunk as the platform to collect and index machine data from virtually any source, regardless of its location. Then, we will consider how Vormetric can interact seamlessly with the Splunk system to ensure compliance with security policies and regulatory mandates.

The Data Deluge

To understand the issues around the use of machine data, it's useful to first look at a definition. Machine data encompasses a record of all of the activity and behavior of users, transactions, applications, servers, network and mobile devices that may be physical, virtual, or located in the cloud. Importantly, this data goes far beyond simple logs of activities. Machine data can include configurations, data from APIs, message queues, change events, the output of diagnostic commands, call detail records and sensor data from industrial systems and more. If this data is compiled into a usable form, it can literally provide the keys to enterprise kingdom, with details ranging from user activities to security threats and fraudulent activities.

Every element of a typical enterprise infrastructure is generating machine data every millisecond of the day. In fact, machine data is one of the fastest growing and most complex areas of big data, but like any type of big data, it brings big challenges along with the benefits. While the volume of incoming machine data is daunting, the primary hurdle with using this wealth of information is that the types of data are also completely unique to the devices from which they come. Some systems, such as business intelligence and data warehouse tools, are batch-oriented and designed for structured data with very rigid schemas. IT management or tools designed to provide security information and event management (SIEM), on the other hand, are hard-wired for specific data types.

Machine data comes in an array of unpredictable formats, and traditional monitoring and analysis tools were simply not designed to handle such a variety of data types at this volume.

Get a Bird's Eye View with Splunk

Splunk turns your machine data into Operational Intelligence, with a range of powerful search, visualization and analysis tools. The solution collects machine data from wherever it's generated, including physical, virtual and cloud environments, and creates the ability to search, monitor and analyze data from one place in real time. With Splunk, rganizations can:

- Troubleshoot problems and investigate security incidents in minutes, not hours or days.
- Monitor end- to-end infrastructure to avoid service degradation or outages.
- Gain operational intelligence with real-time visibility and critical insights into customer experience, transactions and other key metrics.

Splunk is available as a software download or as a Software as a Service option, making your machine data accessible, usable and valuable across the organization whether physical, virtual or a combination of both.

Balancing Big Data Benefits & Big Risks

The benefits of correlated machine data from across the enterprise is obvious. What may not be immediately obvious, however, is that as machine data is correlated and made useful, it also becomes extremely valuable. In additional to typical data-oriented concerns about security and privacy, the collection of machine data can introduce some unique risks, including:

- **Advanced Attack.** Organizations typically establish strong controls around the data center, and have likely protected many of the sources from which Splunk pulls data. It is important, however that the Splunk data warehouse itself be strongly protected, as the information is arguably more valuable in this state.
- **Access Control.** It is essential that the valuable information contained in a Splunk database and its logs be accessible only to the proper users. In addition, Splunk administrators can themselves provide a new threat vector. These users have access to a wealth of sensitive information, and may expose it inadvertently. It is therefore important that access to Splunk data be trackable.
- **Data Volume.** Splunk Enterprise provides a vital means to correlate huge volumes of disparate data. But the fact remains that each piece of data is itself vulnerable and must be protected.

Vormetric & Splunk Solution

With all of this data, there is also risk, specifically those entities within the organization that may have access to confidential data either due to their job function or because they are gaining it through surreptitious means.

When used with an Operational Intelligence platform such as Splunk, the Vormetric Data Security Platform not only encrypts and controls access to your files and databases, but also provides information that is utilized by Splunkbase. Whether the deployment is physical or virtual, the joint solution can alert when unusual or improper data access is detected, and can offer detailed user and process information to help investigation. Insight is gained to not only see what is happening from the "outside-in," but also from nefarious activity that may be due to the insider threat. This capability is available as part of the extensible Vormetric Data Security Platform, providing protection across heterogeneous environments—file systems, databases, big data implementations, VMs, cloud environments and SAN/NAS devices. This capability helps to catch bad actors in action, which includes:

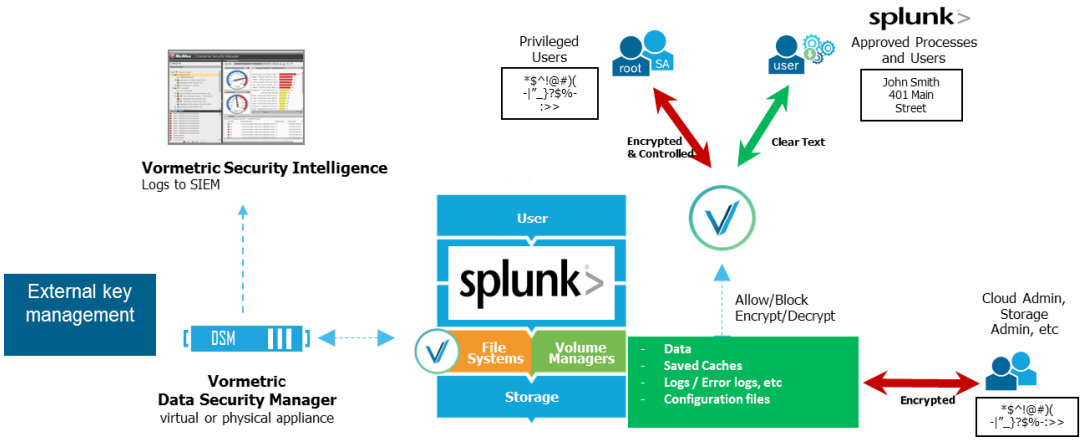
- Identifying anomalous process and user access patterns for investigation. Vormetric logs detail the processes and users accessing protected data. Splunk then performs an analysis of log information, which identifies usage patterns that are inconsistent with that user or process profile. This could identify an APT attack or malicious insider action.
- Visualizing unauthorized access attempts to protected data. Vormetric Data Security identifies and controls access, including privileged users. When attempts are made to access protected data by an unauthorized user or process, data is logged and made available to Splunk. Even privileged users logged in with authorized user credentials (e.g., using Switch User commands) are controlled and logged.

Essential elements within the Vormetric platform include:

- Vormetric Data Security Manager (DSM) – The core of the platform, the DSM provides centralized administration of encryption keys and data security policies
- Vormetric Transparent Encryption – File system agents provide protection of the Splunk data warehouse, as well as files, folders, documents, logs and more.
- Vormetric Security Intelligence – Created by the DSM, this application produces detailed security event logs that are themselves integrated into Splunk.

Vormetric Data Security Manager

Vormetric's DSM simplifies the process of handling security at scale for data-at-rest by centralizing and simplifying the provisioning of encryption keys. The DSM is accessed from a secure Web-management console, CLI or through APIs. This centralized control enables security teams to enforce strong separation of duties when managing the solution so that no single administrator has complete control over Splunk machine data or the encryption keys that protect it. Clustering DSMs provides high availability and scalability to tens-of-thousands of Vormetric Transparent Encryption that run across many different Splunk Machines operating in both centralized and geographically distributed environments. And regardless of where the data resides, encryption keys remain in enterprise control, ensuring that data cannot be collected or access by others without consent.



Encrypting the Data

Vormetric Transparent Encryption is a software agent that enables data-at-rest encryption, privileged user access control and the collection of security intelligence logs without change to applications, databases or infrastructure. Vormetric Transparent Encryption Agents run at the file system level or volume level on a server that has Splunk software installed. This data encryption solution stops root, system, cloud storage and other administrators from accessing Splunk data in any form or location, while preserving their ability to do their jobs. Vormetric Transparent Encryption Agents are distributed and optimized for specific file system and encryption acceleration hardware across servers, resulting in very low latency and overhead. Agents employ logic and fine-grained policies defined by the DSM to evaluate attempts to access protected data, and then either grant or deny access; all activities taking place around the protected data are logged. The Agents have been deployed over tens of thousands of servers, making them the right solution for Splunk Enterprise Big Data requirements.

Adding Security Intelligence

Vormetric Security Intelligences captures granular logs of all file access attempts to accelerate advanced threat detection behind the perimeter. The Vormetric Security Intelligence Solution for Splunk is specifically designed to feed logs about activity back to the Splunk system. At its core, the Vormetric Security Intelligence Solution for Splunk extends the reach of SIEM capabilities to detect and through advanced correlation, counter attacks on sensitive data.

Conclusion

As threats to enterprises grow, collecting actionable intelligence from a huge variety of different systems on the network becomes essential. And as attacks become increasingly complex, that very intelligence has come under attack; in fact, this information can itself be a prime target for insider attacks, as the number of company insiders with access to the data grows.

Now more than ever the combination of aggregated data compiled by Splunk and easy-to-deploy encryption from Vormetric is a compelling one. Furthermore, the information provided by Splunk can help root out advanced persistent threats that are built to evade point security products. Vormetric provides security of this essential data along with an additional feed that give a view of potential security threats that may occur on the inside of the network. This seamless integration ensures that in a world fraught with new persistent and sophisticated attacks that SIEM can now identify threats that are both internal as well as external; and regardless of the type of threat, the organizations most sensitive data will remain secure and fully compliant with regulatory statues.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Vormetric Security Platform is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com