

# Thales & Splunk

## Identifying complex security and compliance threats that puts your data at risk



### Security Intelligence solution for Splunk

- Alerts when unusual or improper data access is detected
- Offers detailed user and process information to help investigation
- Protects across heterogeneous environments, including file systems, databases, big data implementations, VMs, cloud environments and SAN/NAS devices

The problem: threat landscapes have drastically changed from just a few years ago.

With advanced persistent threats (APTs), now common—hackers are actively seeking to steal credit card data, personally identifiable information (PII), critical intellectual property (IP), and other legally protected information to sell to the highest bidder. Some of the most effective tools for fighting these attacks are the security intelligence and threat detection capabilities of Security Information and Event Management (SIEM) solutions. SIEM solutions monitor both real-time events and track long-term data to find anomalous patterns of usage, qualify possible threats to reduce false positives, and alert organizations when risks are detected. The Vormetric Data Security Manager from Thales enhances SIEM solutions by providing an additional data feed on events that are occurring on the internal network and provides rich data points about protected data-at-rest.

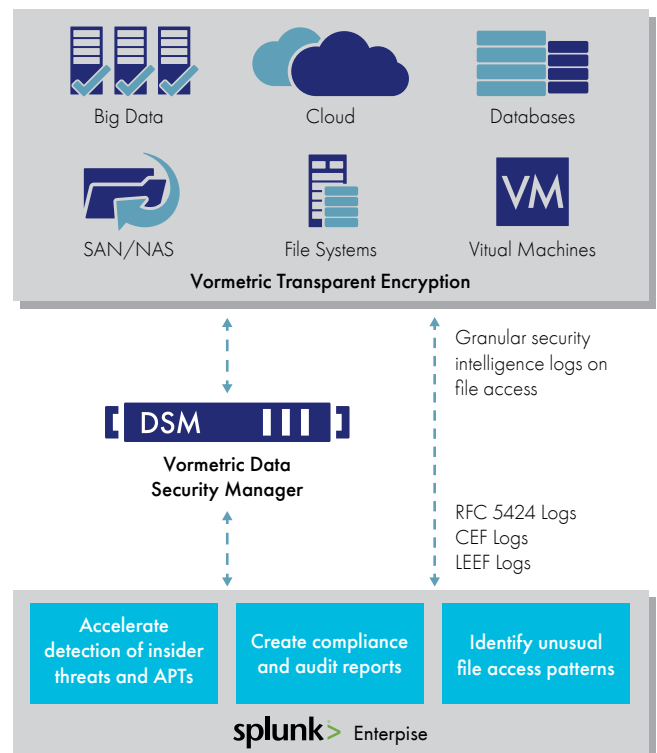


Figure 1:Thales Vormetric Data Security Manager feeds Splunk with the insider file access intelligence needed to identify and stop complex security and compliance threats.

# Splunk and Thales simplifies security and minimizes risk

## The solution: Vormetric Data Security Manager and Splunk

- 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 Splunk Enterprise. Whether the deployment is physical or virtual, the Vormetric Security Intelligence Solution for Splunk can alert you when unusual or improper data access is detected, and can offer detailed user and process information to help investigation. You will gain insight 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 ATP 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.

## Why use Vormetric Data Security Platform with splunk?

The Vormetric Data Security Manager strengthens and simplifies security by automatically feeding logged information to Splunk Enterprise, which proactively monitors activity and alerts when it detects irregularities. These irregularities are usage or login patterns that fall outside of a user’s credentials. This proactive automation can help thwart malicious attacks or actions before they cause harm.





## Splunk

Splunk was founded to pursue a disruptive new vision: make machine data accessible, usable and valuable to everyone. Splunk’s Security and Compliance solutions provide real-time security monitoring, historical analysis and visualization of massive data sets, providing security intelligence for both known and unknown threats. Splunk facilitates data exploration of incidents in real time to perform comprehensive incident investigations, maintain a proactive defense and support the creation of ad hoc reports in minutes. For more detailed technical specifications, please visit: [www.splunk.com](http://www.splunk.com)

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Americas** – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: [sales@thalessec.com](mailto:sales@thalessec.com)  
**Asia Pacific** – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen’s Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: [apacsales.cpl@thalesgroup.com](mailto:apacsales.cpl@thalesgroup.com)  
**Europe, Middle East, Africa** – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: [emea.sales@thales-eseurity.com](mailto:emea.sales@thales-eseurity.com)