# Vormetric Data Security Enhances Security Intelligence

## When the barbarians penetrate the perimeter, how do you protect your critical data?

Layered defense in depth to protect sensitive information has become essential for enterprises. The days when keeping up your firewall and IDS/IPS, making sure that appropriate anti-virus was in place, and watching your network were enough to protect your organization are gone.

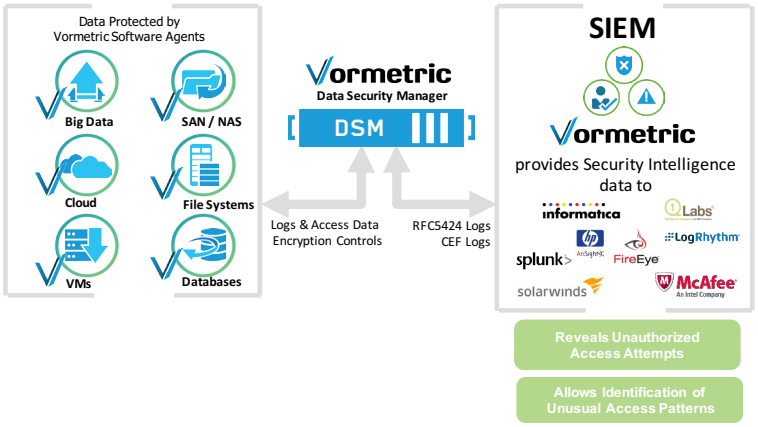
Now that attacks to steal data are a multi-billion dollar industry, criminals can easily build or buy tools that can't be detected by existing security solutions– zero-day exploits. Once social engineering and spear phishing penetrate an organization, criminals then leverage these zero-day exploits to establish a beachhead, and beginning mining your private data and critical IP – keeping their data mining operation working undetected for as long as possible.

Some of the most effective tools for fighting these attacks are the threat and security intelligence capabilities of Security Intelligence and Event Management (SIEM) solutions. SIEM solutions monitor both real-time events and a mountain of long term data to find anomalous patterns of usage, qualify possible threats to reduce false positives, and alert organizations when needed.

## Vormetric Security Intelligence + SIEM – The next step in protecting your enterprise

An SIEM solution can be blind to possible threats to your protected data without the kind of detail provided by Vormetric Data Security. A leader in enterprise data protection, Vormetric protects essential structured and unstructured data with encryption and key management wherever it resides – in physical, virtual, cloud and big data environments. While enforcing encryption rules and data access controls in all these environments, Vormetric agents collect and log information on file access by users and processes, as well as details on the use of the Vormetric infrastructure that protects them.

The detailed information Vormetric provides, in the form of RFC5424 or CEF logs, represents essential data that can be analyzed using an SIEM solution's security intelligence capabilities to identify usage patterns that may represent a threat.




## Combine Vormetric Data Security with a Security Intelligence and Event Management solution to protect what matters:

- Pinpoint unusual patterns of user access to protected data that indicate malware (or a malicious internal user) could be stealing data
- Detect possible malware or malicious insiders making unauthorized access attempts (Vormetric also blocks the attempts – even from root or super user level users)
- Monitor process access to protected data for anomalous patterns of use that could indicate a process has been co-opted by malware
- Identify attacks on the Vormetric Data Security Management appliance from unauthorized users

"Cyberattacks are a fundamentally different threat because, with no shots fired, they potentially can disrupt utilities, banking, business and military networks, yet remain essentially untraceable to a country or an agent of origin. … This is a very difficult, but real and dangerous, threat."

**-Chuck Hagel, Fmr. US Defense Secretary**

- **Advanced Persistent Threats (APTs)** – Find patterns of abnormal activity indicating that a user or process has been compromised. An administrative account that suddenly begins accessing volumes of data, for instance, may be indicative of a compromised user.
- **Malicious Insiders** – The same activity pattern recognition tools that will identify a compromised user could also indicate an insider with a grudge, or who has decided to profit from their position.

Vormetric solutions go beyond providing data that can identify abnormal usage patterns– They also include data access enforcement. Only allowed accounts and processes have access to unencrypted data (even super users and administrators will not have access). And the data produced by unauthorized access attempts can be monitored and used to investigate possible threats.

Access Attempts from Unauthorized Agents

Last 7 days

| shost | count | percent |
|---|---|---|
| PHENSCHEID-WIN7.vormetric.com | 31 | 38.27 |
| fslpar215.i.vormetric.com | 26 | 32.09 |
| bob.i.vormetric.com | 24 | 29.62 |

**Unauthorized Access Attempts**

User Logins

Last 7 days

| Name | Result | count | percent |
|---|---|---|---|
| User1 | OK | 199 | 95.2 |
| anand | OK | 5 | 2.39 |
| User1 | Failed | 4 | 1.91 |
| voradmin | OK | 1 | 0.47 |

**Unusual Administrative Login Patterns**

- **Unauthorized access attempts to the Data Security Manager (DSM) appliance** – Use to detect possible malware or insiders attempting to gain access to the keys and certificates that protecting your data and communications
- **DSM appliance user logins** – Use the data to spot anomalous access patterns from administrators using the DSM Audits of all accesses to a file in the event of a data leak to assist with the investigation
- **Identification of all files accessed by a user** – To aid in the investigation of someone who is under suspicion
- **Recording of file activity entitlements** – Identify unusual instances of administrative users creating new accounts with rights to access protected data that may indicate a compromised administrative account.
- **Dormant user auditing** – Auditing to discover dormant users or hosts and un-used access rights that may represent a risk

Even information on access attempts to Vormetric management infrastructure is available – enabling enterprises to "watch the watcher", making sure that security and administrative accounts are not compromised.

Beyond abnormal activity recognition, the combination of Vormetric log data with an SIEM solution also allows visibility into:

## Detect unusual or improper data access that may indicate a threat

Combine Vormetric Data Protection logs with SIEM solutions intelligent analysis and pattern recognition to gain detailed user and process access information for protected data

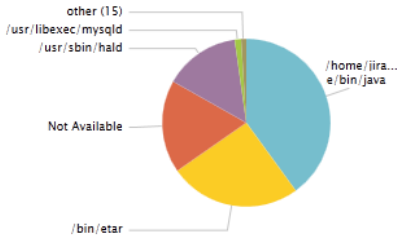
Top 10 Users

Last 7 days

| uinfo | count |
|---|---|
| root,uid=0,gid=0\root,bin,daem | 459366 |
| haldaemon,uid=101 (User Not. | 368313 |
| jira,uid=1005,gid=100\users\ | 289836 |
| mysql,uid=27,gid=27\mysql\ | 14082 |

Top Processes

Last 7 days




## ABOUT VORMETRIC

A leader in data security solutions, Vormetric (@Vormetric) protects data-at-rest in physical, virtual, big data and cloud environments. Trusted by businesses and governments for over a decade, the Vormetric Data Security Platform secures the data of more than 1,500 global enterprises—including 17 of the Fortune 30. With Vormetric, a single infrastructure and management environment protects data wherever it resides with file, volume and cloud storage encryption, tokenization with dynamic data masking, field-level application encryption, sophisticated access control policies, third party and integrated encryption key management. For more information, please visit www.vormetric.com.

**Vormetric, Inc.**
2545 N. 1st Street, San Jose, CA 95131
United States: 888.267.3732
United Kingdom: +44.118.949.7711
Singapore: +65.6829.2266
info@vormetric.com
www.vormetric.com