Solution Brief

SIEM Advanced Threat Detection

Look beyond the perimeter to stop attacks targeting data

You have already deployed McAfee® Enterprise Security Manager to collect, analyze, and report on advanced perimeter attacks. Now gain the visibility of what is happening on the inside—including activity on the server, who is accessing files and databases, which privileged users are accessing your data, and behaviors that indicate malware or advanced persistent threats (APTs) that may have gone undetected past the perimeter.

Vormetric

McAfee COMPATIBLE

Protect Your Most Valuable Asset

They say that information is power. This is certainly the case when it comes to the data that traverses your distributed physical or cloud-based environment on a daily basis. Employees, partners, vendors, customers, and many other user communities regularly leverage your corporate data, the lifeblood of your business. This is why hackers are continuously building "a better mousetrap" to defeat your security, gain the valuable information they want, and profit by using it or selling it to the highest bidder. Even a relatively minor breach can cause irreparable harm, violate regulatory compliance, and put an organization at risk. Some organizations never recover.

Advanced Threats Require Advanced Security

Layered defense-in-depth is essential for enterprises. But the days of relying solely on your perimeter defense are gone. It is no longer enough to just keep up on firewall and intrusion detection systems (IDS)/intrusion protection systems (IPS); make sure that appropriate antivirus is in place; and keep an eye on your network. With the widespread adoption of a distributed environment that leverages cloud and virtualization, the perimeter no longer exists.

Today's attacks are significantly more sophisticated and include zero-day and targeted attacks, social engineering, and spear phishing—all designed to establish a beachhead, mine your private data and critical IP, and keep the 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 security and compliance threats to reduce false positives, and alert organizations when needed. Adding Vormetric Data Security Manager to McAfee Enterprise Security Manager will provide you with the visibility of what is happening behind the perimeter, including server activity, who is accessing the files and databases, what privileged users, such as administrators, are doing, and what malware or APTs may have gotten past the perimeter without being detected. It will also protect your cloud-based environment where there is no clear perimeter.

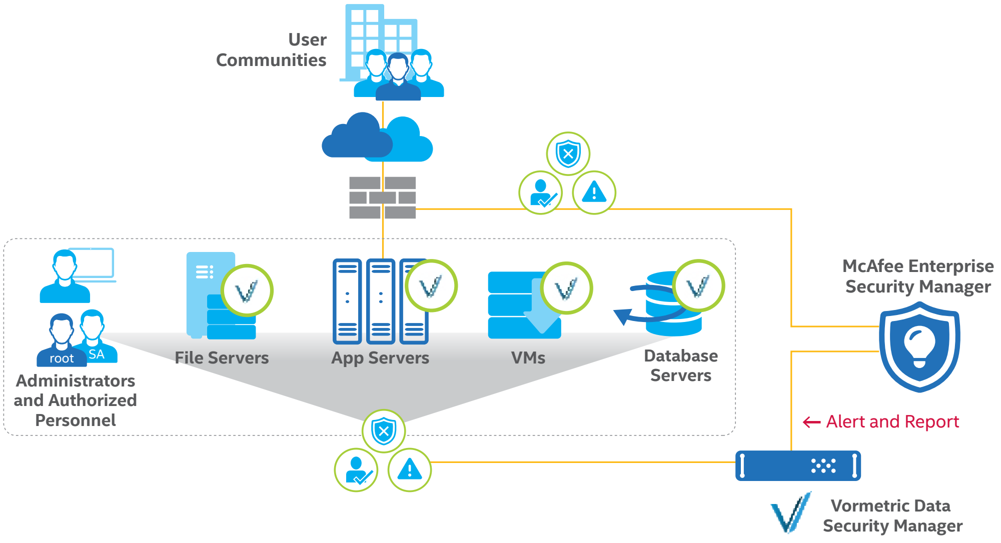
User Communities
Administrators and Authorized Personnel
root
SA
File Servers
App Servers
VMs
Database Servers
McAfee Enterprise Security Manager
← Alert and Report
Vormetric Data Security Manager

Figure 1. Vormetric enhances SIEM with data security intelligence.

The Next Step in Protecting Your Enterprise

McAfee Enterprise Security Manager, the foundational SIEM solution from Intel Security, delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded framework simplifies your ability to audit and proactively report on compliance.

A leader in enterprise data protection, Vormetric protects essential structured and unstructured data with encryption access control and key management wherever it resides—in physical, virtual, cloud, and Big Data environments. While enforcing encryption rules and data access controls in these environments, Vormetric agents collect, alert, and log information that is missed by perimeter security products. It delivers new visibility to the SIEM as to who, what, when, and how files are accessed on the servers. Information on file access by users and processes, as well as potential security and compliance threats that may have bypassed perimeter defenses, can now be easily visualized, tracked, and alarmed. The detailed information is in the form of RFC5424 or CEF logs, which represent essential data that can be analyzed using McAfee Enterprise Security Manager's security and compliance capabilities to identify usage patterns that may represent a threat. This data includes:

- **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.
- **Compliance reporting:** Gain new visibility into potential regulatory and corporate compliance violations with the insight as to what is happening inside the network. With new capabilities, including logging, alerting, and reporting, you can proactively demonstrate "forward-leaning" compliance enforcement both to corporate leadership and regulatory agencies.
- **Malicious insiders:** The same activity pattern recognition tools that will identify a compromised user could also indicate an insider with a grudge 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 and audit. Only allowed accounts and processes have access to unencrypted data (even superusers and

McAfee Enterprise Security Manager and Vormetric Data Security

Vormetric Data Security 5.2.1 and McAfee Enterprise Security Manager protect your organization from the threats that can destroy your reputation and business.

- Automatically pinpoint unusual patterns of user access to protected data.
- Audit, report, and proactively demonstrate compliance of corporate and regulatory statutes.
- Detect malicious insiders making unauthorized access attempts.
- Monitor anomalous processes and access to protected data that could indicate a probe or reconnaissance or an attack that is underway.
- Reduce the volumes of data that you would typically have to comb through and focus on a prioritized list of security incidents.
- Define actions at a granular level, based on the severity of security threats and alarms.

administrators will not have access). The data produced by monitoring unauthorized access attempts can analyzed to investigate possible threats. Even information on access attempts to Vormetric management infrastructure is available, enabling enterprises to “watch the watcher” to ensure 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:

- **Root/user impersonation:** Detects if users have changed access levels or are pretending to be an operating system administrator or superuser when they are not, or if an administrator has switched his user status to impersonate an authorized user.
- **Identification of all files accessed by a user:** Aids in the investigation of someone who is under suspicion.
- **Recording of file activity entitlements:** Identifies unusual instances of administrative users creating new administrative accounts with rights to access protected data that may indicate a compromised administrative account
- **Dormant user auditing:** Conducts an audit to discover dormant users or hosts and unused access rights that may represent a risk.

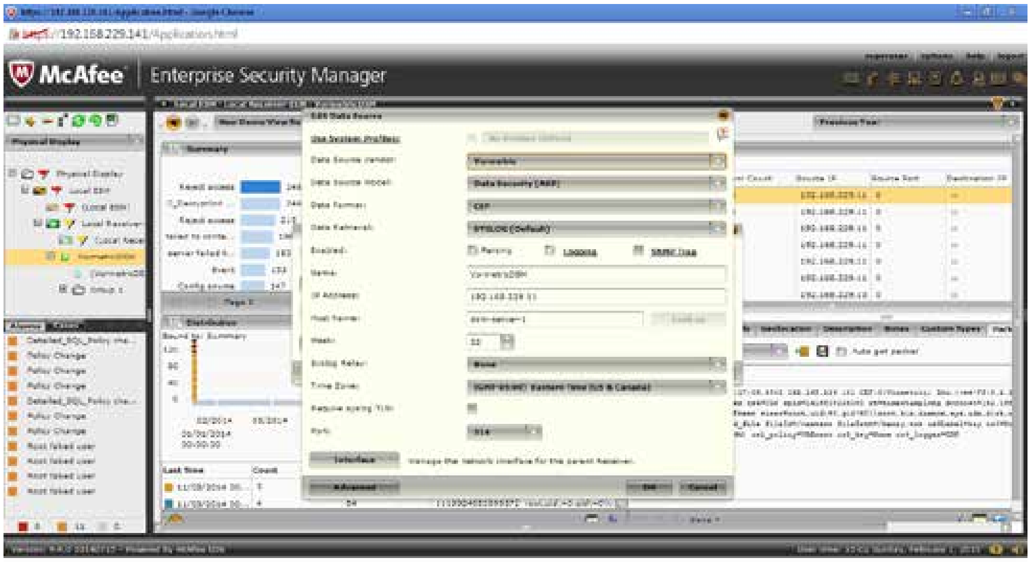
https://192.168.229.141/Applications.html
McAfee
Enterprise Security Manager

Figure 2. Combine Vormetric data protection logs with McAfee Enterprise Security to pinpoint the security and compliance violations among the mountain of alerts you receive every day.

Learn More

Vormetric Security Intelligence works with SIEM vendors to accelerate behind the perimeter threat detection and produces detailed file access and security information logs for auditors and compliance officers. To learn more about the McAfee Enterprise Security Manager and Vormetric Data Security joint solution, please visit **Intel Security** or **Vormetric**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com