



FireEye and Vormetric Threat Analytics Platform and Vormetric Data Security

SECURITY
REIMAGINED

INTEGRATED SOLUTION AT A GLANCE

- Granular details of who is accessing sensitive directories and files
- Audit users/processes accessing unauthorized files
- Audit administrative users imitating another user
- Identify suspicious file access patterns and privileged escalations
- Identify threats and accelerate response time by layering
- Real-time FireEye threat intelligence over enterprise event streams
- Raise the visibility of the threat landscape by providing rich insights into threat actor profiles
- Manage incidents to improve efficiencies in assigning, tracking, and resolving events with on-demand portal access

Moving security close to the data is more effective because it minimizes the potential for any unauthorized access. FireEye and Vormetric offers a rapid approach for protecting databases and files across the entire organization.

The best line of defense against data breaches is to protect the data itself with encryption, access controls, and visibility into file access attempts. An effective corporate data encryption and access policy architecture must be comprehensive in scope so that it can cover data in structured databases, Big Data, and unstructured data stores and work across physical, virtual, and cloud environments. Piecemeal solutions risk losing control of the data as it moves to different environments that are protected by different systems and policies.

HOW THE JOINT SOLUTION WORKS

The Vormetric data security platform produces detailed security intelligence log information on file level access of sensitive data including server activity, access attempts and privileged escalations.

Combining this log data with the FireEye Threat Analytics Platform (TAP), allows a company to pinpoint patterns of unusual user access to protected data that could indicate malware or other malicious user activity that is occurring beyond the perimeter security.

The Vormetric security intelligence logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented

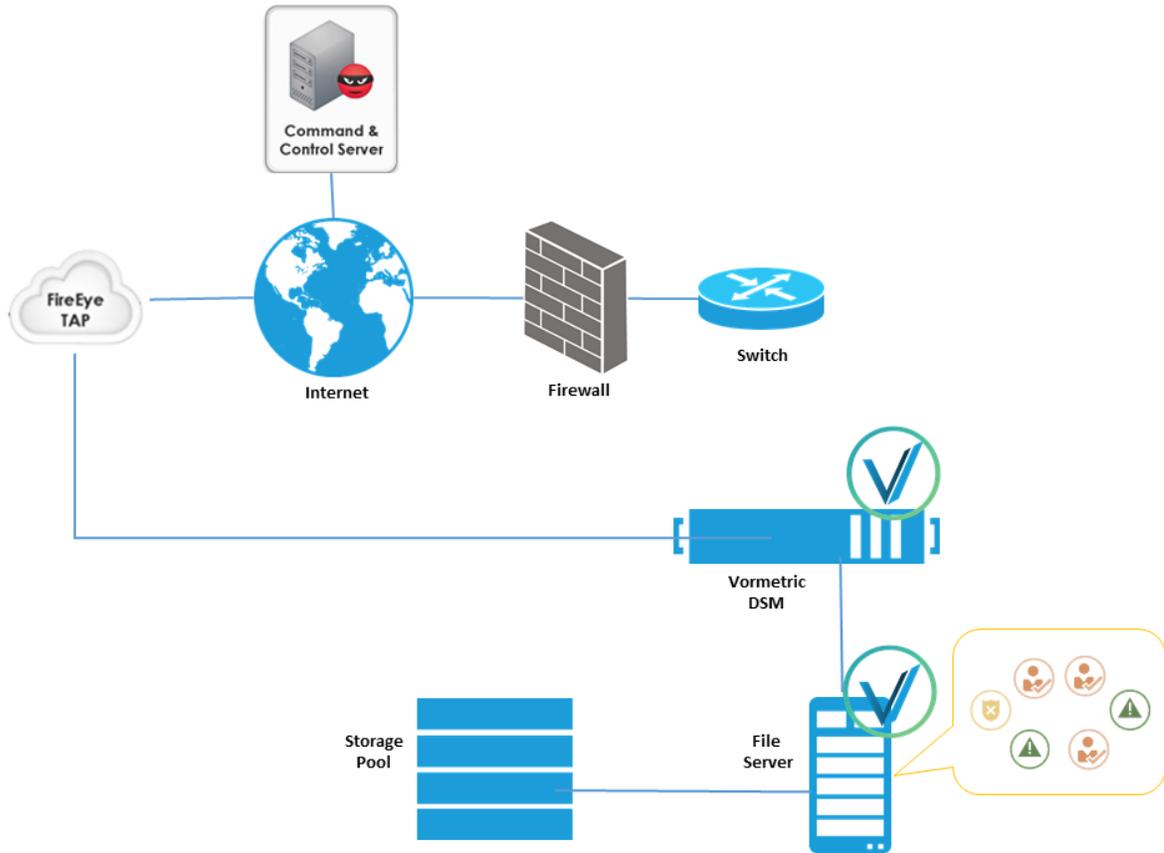
insight into file access activities. Logging occurs at the file system level, removing the opportunity of stealthy access to sensitive data.

The security intelligence logs can inform of unusual or improper data access and accelerate the detection of insider threats, hackers, and the presence of advanced persistent threats (APT) that are past the perimeter security.

The Data Security Manager (DSM), is the centralized policy and key manager for the Vormetric platform. It changes the data security management game by enabling an IT organization to have a consistent and repeatable method for encrypting, enforcing access policies, and gaining security intelligence for all structured and unstructured data.

The security intelligence logs are compressed, encrypted, and sent to FireEye TAP where the logs are parsed and pre-defined FireEye and Vormetric rules are used to identify malicious activity. TAP is able to notify the incident responder of the threat, so that they can thoroughly investigate the activity and confirm whether the threat is real or not. The incident responder can utilize TAP to monitor the issue and also forward it to a responder for resolution.





ABOUT FIREEYE

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 3,400 customers across 67 countries, including over 250 of the Fortune 500.

ABOUT VORMETRIC

Vormetric is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1700 customers, including 17 of the Fortune 30 and many of the world's most security conscious organizations, to meet compliance requirements and protect what matters – their sensitive data – from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application – anywhere it resides – with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation and security intelligence.

For more information, please visit: www.vormetric.com.