



Imperva SecureSphere and FireEye Malware Protection System Integration

Integration Benefits

- Prevent malware-compromised devices from accessing critical applications and sensitive data
- Take a risk-based approach to malware remediation
- Isolate malware infected machines
- Audit all access to sensitive data
- Alert on, or block, sensitive data access
- Dynamically learn legitimate application and data usage

Protect Critical Applications and Sensitive Data from Next-generation Threats

Targeted, zero-day malware attacks are growing in number and sophistication, and can easily bypass conventional security defenses like firewalls, next-generation firewalls, intrusion prevention systems (IPS), anti-virus (AV) and Web gateways. When advanced malware compromises devices inside of your organization, their target is often your most sensitive data. The results can be disastrous.

Compromised insiders, unaware that advanced malware has infected their devices, unknowingly provide criminals with a conduit to access your networks, critical applications and sensitive data. Once inside of your network, hackers will do whatever it takes to reach their targets—steal passwords, escalate privileges, hijack servers, etc.

Imperva and FireEye offer a joint solution that protects applications, databases and file stores from targeted attacks originating from malware-compromised machines.

Neutralize Malware Activity

Imperva and FireEye enable a comprehensive security solution that automatically restricts applications and data from being accessed by a malware compromised system. The FireEye Virtual Execution (VX) technology identifies infected hosts and then passes that information along to Imperva SecureSphere. SecureSphere uses this actionable intelligence to prevent infected machines from accessing critical business applications and sensitive information in database and file servers, while FireEye blocks any data exfiltration attempts by the malware-compromised host.

Minimize Downtime with a Risk-based Approach to Data Access

When machines become infected with malware, they must be quarantined, diagnosed and the offending malware removed. Disconnecting the compromised device from the network and taking the user offline can take time, impact business operations, and slow productivity. The Imperva-FireEye integration allows administrators to automatically identify compromised machines and apply access controls to critical applications and sensitive data. This restricts the malware's ability to access and exfiltrate data. By selectively isolating access to specific applications and data, disruptions to the user and ongoing operations are minimized.

With the FireEye-Imperva joint solution, organizations can pinpoint machines that have been compromised by malware, and then enforce access controls that prevent malware-compromised insiders from accessing critical applications and sensitive data.

FireEye Malware Protection System

Traditional and next-generation firewalls, IPS, AV and gateways can't stop advanced malware, thus leaving significant security holes in the majority of corporate networks. The FireEye Malware Protection System is the only complete solution to stop advanced

Traditional and next-generation firewalls, IPS, AV and gateways can't stop advanced malware, thus leaving significant security holes in the majority of corporate networks.



FireEye Malware Protection System enables organizations to:

- Protects data against zero-day, advanced cyber attacks
- Blocks malware data exfiltration attempts across multiple protocols
- Stops blended Web- and email-based attacks
- Dynamically generates actionable malware intelligence



targeted attacks across the Web and email threat vectors and malware resident on file shares. The platform offers integrated, multi-vector protection utilizing stateful attack analysis to stop all stages of an advanced attack. Each of FireEye's products features the Virtual Execution (VX) engine that provides state-of-the-art, signature-less analysis using patented, proprietary virtual machines. The Malware Protection System builds a 360-degree, stage-by-stage analysis of an advanced attack, from system exploitation to data exfiltration, in order to most effectively stop would-be APT attackers.

Imperva SecureSphere Business Security Suite

SecureSphere is the market leading solution for business security. SecureSphere provides comprehensive, integrated application security and data security to prevent data breaches, streamline regulatory compliance and establish a repeatable process for data risk management. Powering the SecureSphere suite is a common platform that provides flexible deployment options, unified management, deep analytics and customizable reporting. The SecureSphere platform enables enterprise scalability and accelerates time to value. Underscoring Imperva's commitment to business security, the Imperva Application Defense Center (ADC) is a world-class security research organization that maintains SecureSphere's cutting edge protection against evolving threats.

Key Capabilities:

- Dynamically learns legitimate Web application and data usage
- Alerts and blocks unauthorized activities, in real time
- Audits all access to sensitive data
- Identifies excessive user rights and dormant users
- Accelerates incident response and forensics investigations

About FireEye

FireEye is the leader in stopping next-generation threats, such as zero-day and APT attacks, that bypass traditional defenses and compromise over 95% of networks. The FireEye solution supplements signature-based firewalls, IPS, anti-virus, and gateways, and provide the world's only cross-enterprise, signature-less protection against Web and email threat vectors as well as malware resident on file shares. It is the industry's only integrated solution that stops attacks across every stage of an attack lifecycle, from exploit to exfiltration. Using its patented Virtual Execution technology platform across its portfolio, FireEye is uniquely able to protect against next-generation threats. FireEye solutions are deployed in over 40 countries and in over 20% of the Fortune 500.

About Imperva

Imperva is a pioneer and leader of a new category of business security solutions for critical applications and high-value data in the data center. The Imperva award-winning solutions protect against data theft, insider abuse, and fraud while streamlining regulatory compliance by monitoring and controlling data usage and business transactions across the data center, from storage in a database or on a file server to consumption through applications.