FireEye
SECURITY REIMAGINED

FireEye and Imperva

Automated Data Protection Reduces Downtime and Overall Business Risk

SOLUTION BRIEF

SECURITY REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

The integrated solution can:

- Pinpoint compromised machines.
- Prevent APTs from exploiting sensitive corporate data.
- Quarantine malware infected machines.
- Alert on, or block, sensitive data access.
- Audit all access to sensitive data.
- Enable unified management, deep analytics, and customizable reporting.

OVERVIEW

Traditional security that focused on intrusion prevention is no longer sufficient. While perimeters have always been the first line of defense for data networks, they have also become the most porous. Also, endpoint security cannot fully defend against intentional or unintentional malicious actions by internal users.

Intellectual property, business plans, trade secrets, customer and employee information, and the day-to-day data that drives business are at risk against a new generation of hackers. Comprehensive security strategies must defend critical business data and applications from cyber attacks and internal threats. They must also ensure compliance with the myriad of increasingly stringent data protection regulations and mandates, as well as enforce policies, entitlements, and audit controls.

To accomplish all of this may require the coordination and integration of solutions from multiple vendors with specialized capabilities to protect modern networks.

THE CHALLENGE

The new generation of cyber attackers understands and has created ways to bypass traditional defenses. These circumventions put sensitive data at risk. Today's attacks are targeted in nature and aimed at obtaining critical company resources — sensitive personal information, intellectual property, authentication credentials, and insider information. It is imperative for the security solution to detect and stop the attack at the earliest stage so as to limit the scale and scope of a data breach attempt.

Organizations that deploy multiple solutions with defense in depth may be burdened with managing and interpreting information from a myriad of network security sources. This impedes security unless the solutions are integrated to provide cohesive visibility and leverage the shared information to take action on identified threats.

THE INTEGRATED SOLUTION

Imperva SecureSphere defends business critical data stored in databases and file servers from cyber attacks and internal threats. SecureSphere continuously monitors and audits all access to sensitive data stores in real-time. With interactive audit analytics, users can visualize data access activity with just a few clicks.

FireEye offers a robust solution that accurately identifies and blocks the new generation of cyber attacks. When integrated with Imperva SecureSphere, organizations can restrict compromised devices from accessing sensitive data stores. These actions prevent breaches and the resulting exposure, brand damage, and costs that they bring.

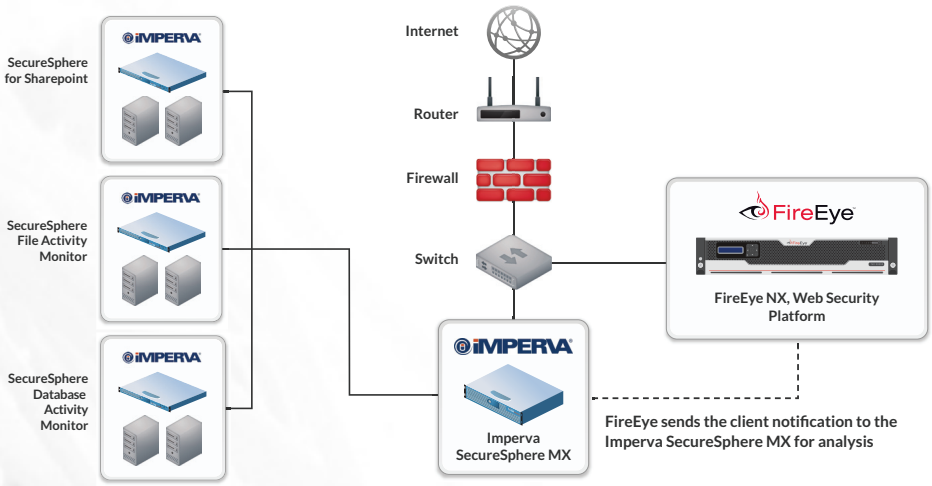
IMPERVA

FIREEYE PRODUCT AND VERSION

NX 7.4.1 and later

IMPERVA PRODUCT AND VERSION

SecureSphere Management Server (MX) version 11.0 and later



HOW THE JOINT SOLUTION WORKS TOGETHER

FireEye and Imperva work together to ensure that sensitive data stored in databases and file servers is protected from advanced targeted attacks. The FireEye-Imperva integration provides a comprehensive security solution that automatically restricts data from being accessed by a malware-compromised system.

The FireEye® NX identifies potentially infected hosts and passes that information to Imperva SecureSphere Management Server (MX). SecureSphere uses the threat intelligence to restrict the machines from accessing sensitive information in databases and file servers while FireEye blocks any data exfiltration attempts by the compromised host.

The FireEye and Imperva integration allows administrators to identify compromised machines automatically and apply access controls to sensitive data without taking the user offline and impacting business operations. This identification restricts the malware's ability to access and exfiltrate data. By selectively isolating access to specific data, disruptions to the user and ongoing operations are minimized.

THE VALUE OF THIS PARTNERSHIP

FireEye and Imperva have partnered to deliver an integrated solution that:

- Prevents compromised devices from accessing sensitive data.
- Enables business to continue while remediation takes place.
- Logs all activities originating from suspected hosts.
- Supports a risk-based approach to malware remediation.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,400 customers across 67 countries, including over 250 of the Fortune 500.

ABOUT IMPERVA

Imperva is a leading provider of cyber security solutions that protect business-critical data and applications. The company's SecureSphere, Incapsula and Skyfence product lines enable organizations to discover assets and risks, protect information wherever it lives — in the cloud and on-premises — and comply with regulations. The Imperva Application Defense Center is a research team comprised of some of the world's leading experts in data and application security. They continually enhance Imperva products with up-to-the-minute threat intelligence, and public reports that provide insight and guidance on the latest threats and how to mitigate them. Learn more: www.imperva.com or Twitter.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**