FireEye
SECURITY REIMAGINED

FireEye Enterprise Network Security Solution

Detect the threats that matter. Streamline and scale your workflow.

SOLUTIONS BRIEF

SECURITY REIMAGINED

HIGHLIGHTS / BENEFITS

- **Comprehensive and Integrated Solution to Minimize the Risk of Cyber Breaches**
  Targeted attacks often use multiple information vectors, such as web, email, and files. The FireEye Enterprise Network Security solution defends all major threat vectors from known and never-before-seen attacks, including zero-day threats.

  The solution identifies and correlates events across different attack stages (initial exploit, malware activity, endpoint control) and vectors to identify multi-stage and blended attacks. Centralized management provides a unified view that simplifies administration and improves visibility of threats and threat context.
- **Effective and Efficient Protection to Aggressively Neutralize Threats**
  Unlike conventional firewall, IPS, or AV solutions, the FireEye Enterprise Network Security solution detects attacks with high accuracy and fewer false positives. It also correlates suspicious activity with globally shared threat intelligence, attack context, and attacker profile—all in real time.

  This combination of sophisticated detection, actionable intelligence, and proactive notification gives your security team the ability to quickly focus on and neutralize real threats.
- **Flexible and Scalable Platform to Meet Your Security Needs**
  The FireEye Enterprise Network Security solution has been designed for organizations of all sizes and infrastructure deployment models. It provides inline detection that scales from small branch offices to large-scale networks. Solution elements can be deployed on premises, in the cloud, or both.

  Deployment options can help you maintain a consistent security model and nimbly evolve as your business infrastructure and needs change.

THE CHALLENGE

Organizations recognize that legacy cyber defenses no longer work. In a typical breach, attackers remain undetected for over 200 days. Targets usually learn of the incident only after someone else (such as law enforcement) discovers it. Recent headlines make it clear: enterprises of every size and in every market across the globe are affected.

The web, email, and data files essential to our digital economy blur organizational boundaries and open doors for external threats. More than 90% of recent cyber attacks combined web and email vectors to breach organizations[1].

To stop breaches and limit their impact, organizations need an integrated, seamless solution that helps detect and respond to genuine threats in near real time.

THE CONVENTIONAL APPROACH

Modern business tools, such as IPS, firewalls, and traffic gateways fail to provide adequate cyber security:

- **Ineffective tools that leave major security gaps** – Traditional tools rely on a decades-old approach of binary signatures and reputations to tell friend from foe. Newer malware developers create unique binaries, constantly change IP addresses, and compromise legitimate URLs to overwhelm these tools. Signature-based defenses are no longer viable: 70-90% of malware samples are unique to an organization.

- **Inefficient workflows that increase operational expenses** —Traditional products trigger thousands of alerts without enough context to prioritize alerts and scope the scale of response. Organizations spend more time and resources chasing down trivial alerts and false positives, which increases costs for little benefit.
- **Limited and disconnected tools that cannot see complex attacks** —Point security tools are often poorly integrated. Even when they work as designed, they can't see blended attacks that use multiple vectors.
- **Non-adaptive defenses that fail as attackers evolve** — Attackers will always find the next layer of gaps in defense technologies. To stay relevant and effective, defenses must adapt as attackers and threat landscapes evolve.
- **Lack of scalability and flexibility that limits inline protection** – Security tools must keep pace with changing business needs. Tools must perform at any scale, from small branch offices to enterprise-wide networks. And security deployments must support flexible deployment models.

A NEW SOLUTION

The FireEye Enterprise Network Security solution provides organizations with a comprehensive, effective, adaptive, and operationally efficient defense against both known and never-before-seen network threats, including zero-day and targeted attacks.

This solution helps you safeguard all major threat vectors in real time and with almost no false positives. It protects data at rest in file systems and data in motion in network and email systems. Integrated intelligence enables organizations to minimize the impact of breaches by prioritizing alerts, scoping the scale of response, and accelerating resolution.

HOW IT WORKS

Solution tools and capabilities include:

- **FireEye Network Threat Prevention Platform with Intrusion Prevention (NX Series with IPS)** Stop network-based attacks with Multi-Vector Virtual Execution (MVX) technology, which minimizes false positives to increase operational efficiencies.
- **Email Threat Prevention (EX Series or ETP cloud with AV/AS)** or in the cloud (ETP) to stop email-borne threats, and block spam and viruses to thwart traditional attacks with AV/AS options.
- **Content Threat Prevention Platform (FX Series)** Protect your data center and file systems from data-at-rest attacks via files you receive from customers and partners.
- **Malware Analysis Platform (AX Series)** Scan your web servers to protect critical web applications and avoid secondary attacks.
- **Central Management (CM Series)** Consolidate administration, reporting, and data sharing among other components of the Enterprise Network Security solution. Establish a local threat intel-sharing hub to help correlate and combat multi-vector blended cyber attacks.
- **Threat Intelligence - Dynamic Threat Intelligence (DTI), Advanced Threat Intelligence (ATI), Advanced Threat Intelligence Plus (ATI+)** Gain contextual insights and get detailed threat actor dossiers from FireEye and Mandiant research teams along with 24x7 remote monitoring by FireEye experts. All this helps prioritize and respond quickly to FireEye alerts. FireEye Threat Intelligence integrates context from millions of network and endpoint based sensors, hundreds of IR engagements, and billions of security events— all analyzed daily.

Visit our Enterprise Network Security solution page for more information.

[1] Verizon Data Breach Investigations Report, 2014

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