FireEye™

Next Generation Threat Protection

"With FireEye, we can now see and stop the attacks targeting our in-house and remote users. It has been an eye-opener for us to be able to determine with accuracy the threats that are passing through the firewall, URL gateway, IPS, and anti-virus."

Director of Information and Data Security, Global 500 Financial Services firm

Today's new breed of cyber attacks easily bypass traditional defenses. Since enterprises and government agencies have implemented stronger policy- and signature-based protections for regulated data and endpoints, sophisticated criminal organizations have changed their tactics, using a new breed of cyber attacks, and targeting intellectual property and other networked assets.

Replacing mass-market malware, today's cyber attacks are personalized and persistent. Threats are ever morphing, dynamic, and zero-day. These multi-stage attacks look innocent to traditional and next-generation firewalls, IPS, AV, and gateways that rely on signatures and known patterns of misbehavior or reputations. Once inside, malware calls back for instructions to steal data, spread laterally into network file shares, allow reconnaissance, or lie dormant until the attacker is ready to strike.

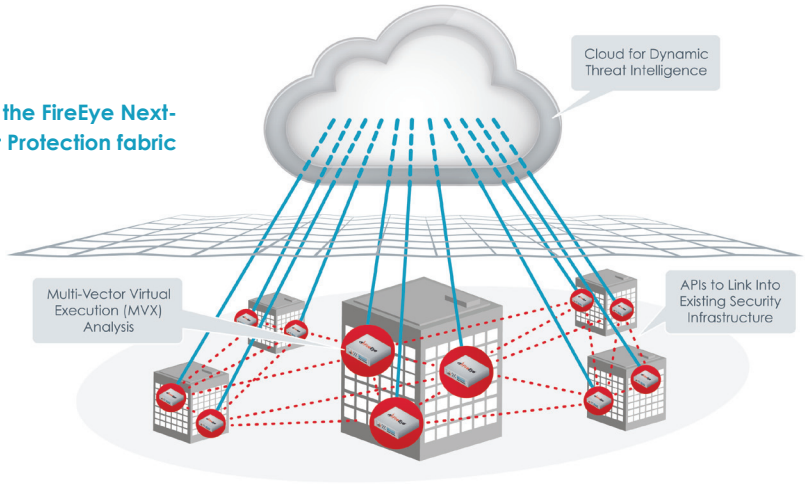
Today, security-conscious enterprises and government agencies choose the FireEye® platform for industry-leading protection against today's new breed of cyber attacks, such as advanced malware, zero-day, and targeted APT attacks. The FireEye platform supplements traditional and next-generation firewalls, IPS, AV, and gateways. The FireEye platform creates a threat protection fabric for integrated next-generation protection against today's multi-vectored Web, email, file, and mobile-based threats.

The only defense against today's new breed of cyber attacks

The FireEye threat protection platform defeats today's cyber attacks that aggressively evade signature-based defenses and compromise the majority of today's networks. The unique FireEye platform is based on:

1. The FireEye Multi-Vector Virtual Execution™ (MVX) engine detects today's new breed of cyber attacks
2. The FireEye Dynamic Threat Intelligence™ Cloud shares anonymized threat intelligence from MVX analysis
3. Security interoperability with a broad ecosystem of partners using standards-based malware metadata and FireEye APIs

Building blocks of the FireEye Next-Generation Threat Protection fabric



"When evaluating FireEye, over 95% of enterprises discovered compromised hosts within what they thought were secure networks."

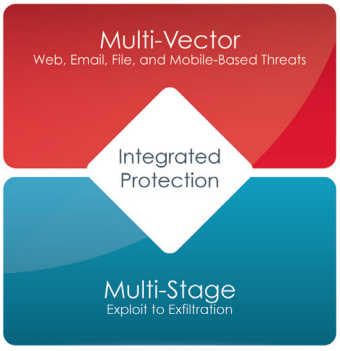
Findings from enterprise evaluations of FireEye Malware Protection Systems.

The FireEye Threat Protection Platform

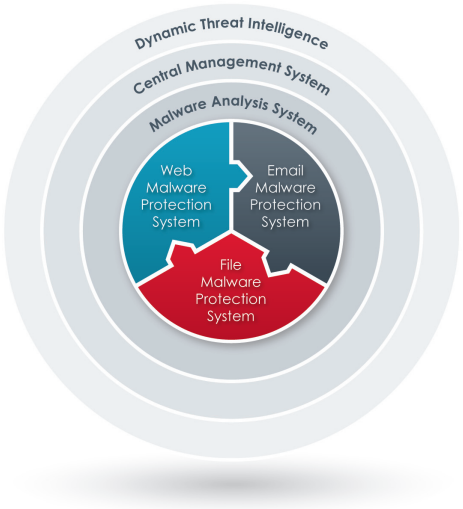
The FireEye platform supplements traditional defenses with a new model of security to protect against today's new breed of cyber attacks. The unique FireEye platform provides the only next-generation threat protection to dynamically identify and block cyber attacks in real time.

Multi-Vector Virtual Execution engine protects across the enterprise

The FireEye platform utilizes a signature-less, virtual execution engine that creates enterprise-specific threat intelligence across vectors; securing against Web, email, file, and mobile attacks. By detonating Web objects, suspicious attachments, and mobile applications within instrumented virtual environments, FireEye is uniquely able to detect zero-day Web exploits, spear phishing attacks, and rogue mobile applications. By correlating multi-vector threat intelligence, this enables the FireEye platform to quarantine zero-day spear phishing emails, block related multi-protocol command and control communications, and identify all the intended victims.



Integrated, multi-threat vector and multi-stage protection against advanced attacks



Complete solution portfolio to stop today's cyber attacks

Security interoperability with APIs and standards-based malware metadata

The FireEye technology partnerships help form an integrated defense to rapidly detect, validate, and respond to cyber attacks. Partner integrations address the network-to-endpoint visibility and enforcement options needed today and enable customers to leverage their existing infrastructure and achieve greater security ROI.

Dynamic Threat Intelligence Cloud

FireEye customers subscribe to the FireEye Dynamic Threat Intelligence Cloud to exchange indicators of compromise and keep protections up to date. The self-learning nature of the data exchange means the security value grows as more customers share real-time, dynamically-generated MVX threat intelligence.

Integrated Web, email, file share, and mobile protection to stop blended threats

Many threats use multiple vectors and stages to bypass traditional protections. The FireEye platform stops these blended threats.

Next Generation Threat Protection

About FireEye, Inc.

FireEye® has pioneered the next generation of threat protection to help organizations protect themselves from being compromised. Cyber attacks have become much more sophisticated and are now easily bypassing traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways, compromising the majority of enterprise networks. The FireEye platform supplements these traditional defenses with a new model of security to protect against today's new breed of cyber attacks. The unique FireEye platform provides the only next-generation threat protection fabric to dynamically identify and block cyber attacks in real time. The core of the FireEye platform is a signature-less, virtualized detection engine and a cloud-based threat intelligence network, which help organizations protect their assets across all major threat vectors, including Web, email, file, and mobile-based cyber attacks. The FireEye platform is deployed in over 40 countries and more than 1,000 customers and partners, including over 25 percent of the Fortune 100.

FireEye, Inc.
1440 McCarthy Blvd.
Milpitas, CA 95035

+1.408.321.6300
1.877.FIREEYE (347.3393)
info@FireEye.com
www.FireEye.com