

“Custom exploits. Custom malware. [Threats that] thought leaders in the industry have been predicting ... are now an every day occurrence.”

– Amit Yoran, (former) Director of US Cybersecurity

Malware Protection System Overview

FireEye secures against broad and targeted information, identity, and resource theft due to modern malware. The core technology stops both inbound, zero-day attacks and outbound malware communications protecting against the criminal compromise of assets as well as data exfiltration attempts.

Conventional technologies rely upon signatures and lists to stop known attacks targeting known vulnerabilities. However, they were not designed to defend against modern attacks that target unknown vulnerabilities and use polymorphism or code obfuscation to evade current defenses.



Zero-day Malware Protection at Near-zero False Positives

FireEye achieves near-zero false positives with its multi-phase malware inspection engine that identifies targeted, zero-day attacks. Known and zero-day attacks (as well as its outbound transmissions) are blocked preventing data theft, alteration, and destruction.

In addition to blocking known attacks, FireEye stops zero-day attacks using a malware inspection engine that features advanced capture heuristics coupled with virtual machine technology to confirm if the suspicious traffic infects the virtual machine. The engine is a cyber Petri dish to confirm the presence of malware. Zero-day malware inside the virtual machine is then analyzed to create a full malware profile including dynamic signatures, callback destinations across protocols, and malware commands issued.

Global Network to Share Local Malware Intelligence

Customers share and add to their local malware intelligence by tying into the Malware Analysis and Exchange (MAX) Network. Auto-generated security intelligence is distributed to subscribers worldwide to stop global attacks targeted at their local network.

Security Without Operational Trade-offs

With FireEye, IT administrators have a clientless solution that deploys in 30 minutes and requires absolutely no tuning. It deploys in several modes, including out-of-band monitoring via a SPAN port, inline monitoring, or inline active blocking to stop attacks and outbound transmissions.

Integrated Security To Stop Malicious Data Theft

FireEye accurately protects systems against inbound infection and stops unauthorized data transmissions to criminal servers. This integrated approach enables the most comprehensive threat protection against modern threats that attack across multiple vectors. FireEye's unique multi-phase inspection engine pinpoints zero-day, targeted attacks that continue to bypass conventional security. With FireEye, it is possible to stop the proliferation of cybercrime, cyber espionage, and cyber reconnaissance attacks.

KEY TECHNOLOGY DIFFERENTIATORS

- Accurate inbound attack detection using a multi-phase malware inspection engine
- Outbound filtering of malware transmissions to prevent data theft
- Global network to share malware intelligence and callback destinations
- Only solution to stop network- and application-based exploits in content, such as HTML, PDF, and Flash

KEY BUSINESS DIFFERENTIATORS

- Prevents data, identity, and resource theft due to targeted malware
- Stops targeted attacks like Aurora, bots, and Trojans that IPS & antivirus miss
- Protects against zero-day inbound malware at near-zero false positive rates
- Real-time intelligence network to prevent global threats against the local network



FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035

+1 (877) FIREEYE (347.3393)
info@fireeye.com

www.FireEye.com