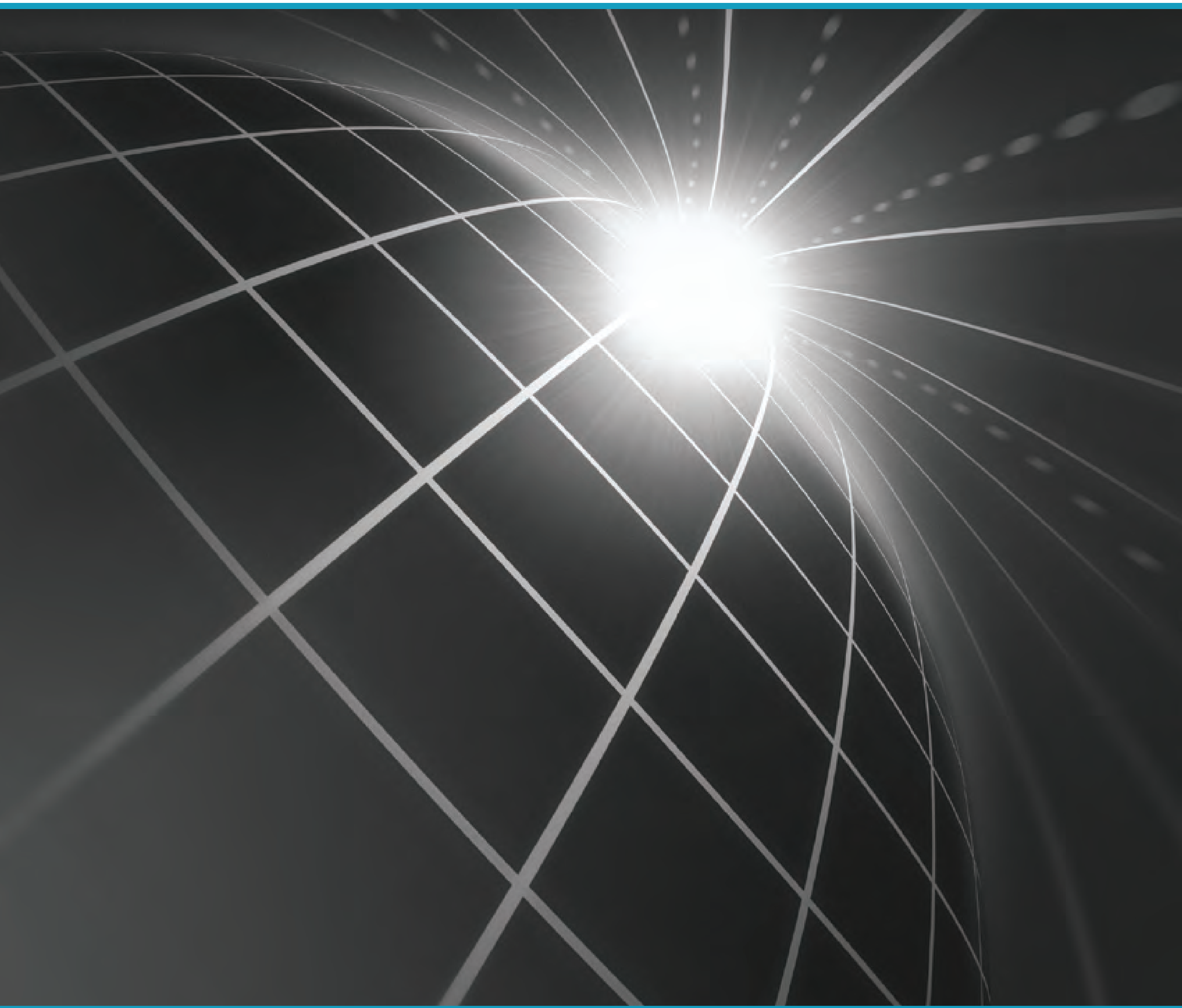
FireEye™

Next Generation Threat Protection



Wondering if Your Defense-In-Depth Team Needs a New Player?

Give your security an "advanced attack" check up.

Risk Factor	Test
"71% of surveyed IT Security Professionals said the 'changing/evolving nature of threats' is a major challenge or challenge."[1]	Can you show that current defenses stop advanced targeted attacks across both Web or email?
"Malicious attacks were the root cause of 31% of the data breaches studied."[2]	Do you automatically block attempts to exfiltrate sensitive data, such as credentials, source code, or personally identifiable information (PII)?
"Incumbent defense technologies fall short."[3]	Does detection of inbound threats in Web and email trigger outbound blocking across multiple protocols, including HTTP, IRC, FTP, and other custom protocols, to shut down multi-stage threats?
Malware detection and analysis and incident response take up more than half of IT Security professionals' time.[4]	What percentage of your infection and attack alerts are false alarms? How long does it take you to find the affected host when you know a system has been compromised?
New malware is released about once per second.[5]	How often is your protection updated to reflect the changing global threat landscape?

[1] Forrsights: The Evolution Of IT Security, 2010 To 2011, Forrester Research, Inc., February 15, 2011, Jonathan Penn and Heidi Shey

[2] Ponemon 2011 U.S. Cost of a Data Breach Survey, http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

[3] Malware And Trojans And Bots, Oh My!, Chenxi Wang, Forrester Research, Inc. February 28, 2011.

[4] InformationWeek's 2010 Strategic Survey.

[5] http://www.sophos.com/security/topic/security-threat-report-2011.html

Like water, cybercrime moves effortlessly around obstacles. Since governments and enterprises have implemented stronger policy- and signature-based protections for regulated data and endpoints, sophisticated criminal organizations have changed their tactics, using advanced targeted attacks and targeting intellectual property and other networked assets.

Replacing mass-market malware, these advanced targeted attacks are personalized and persistent. Threats are targeted, ever morphing, dynamic and zero-day. These carefully multi-staged attacks look innocent as they walk by traditional and next-generation firewall, IPS, anti-virus, and gateways that rely on signatures and known patterns of misbehavior or reputations. Once inside, advanced malware calls back for instructions, which could be to steal data, spread laterally into network file shares, allow reconnaissance, or lie resident until the attacker is ready to strike.

Today, security-conscious enterprises and federal governments choose FireEye™ for industry leading protection against advanced targeted attacks. FireEye stops advanced malware, zero day and targeted APT attacks. FireEye's appliances supplement traditional and next-generation firewalls, IPS, AV, and gateways, adding integrated multi-stage protection against today's multi-vectored Web, email, and file-based threats.

"Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products."

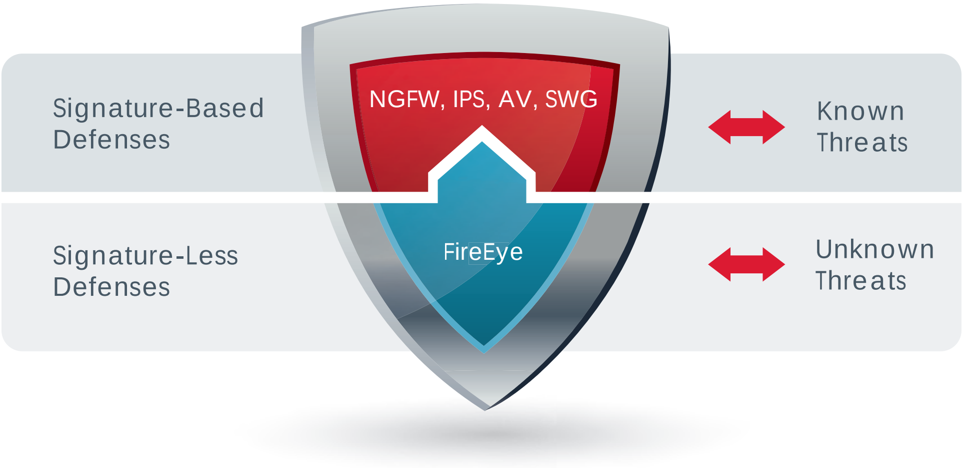
Advanced Evasion Techniques: Weapon of Mass Destruction or Absolute Dud?, Bob Walder, Gartner, 2011

"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 antivirus."

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

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.



FireEye technologies fill the security hole left by traditional defenses

The Only Defense Against Advanced Targeted Attacks

FireEye's Web, Email, and File Malware Protection Systems (MPS) defeat advanced targeted attacks that aggressively evade signature-based defenses and compromise the majority of today's corporate networks. FireEye appliances block known malware and its outbound transmissions and then utilize the most sophisticated virtual execution environment in the world to detect and block advanced malware.

Stateful analysis of zero-day attacks within our virtual environment yields real-time malware security content to protect the local network, intelligence that can be shared to all subscribers of the FireEye Malware Protection Cloud. The MPS appliances also have near-zero false positive rates and are plug-and-play, deploying within 30 minutes for a rapid security ROI.

Full–Fledged Virtual Execution Engine Detects Inbound Zero–Day Attacks

FireEye appliances fully execute suspicious code, analyzing files, attachments, and Web objects to confirm an attack and eliminate false positives. Automation moves malware through a signature filter—a screen against the known bad—into an instrumented virtual environment where FireEye examines the code through its full execution path.

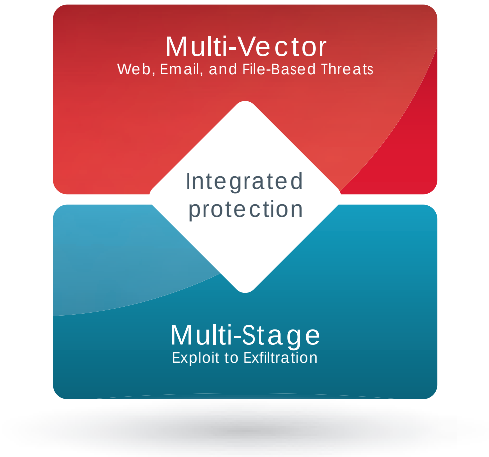
By including a broad range of operating systems, applications, browsers, and add-ons, the FireEye environment presents real-world targets to trigger the full set of zero-day exploits, rootkits, privilege escalations, and other malicious functions in advanced targeted attacks.

Inline Blocking and Quarantining Protects Across Protocols

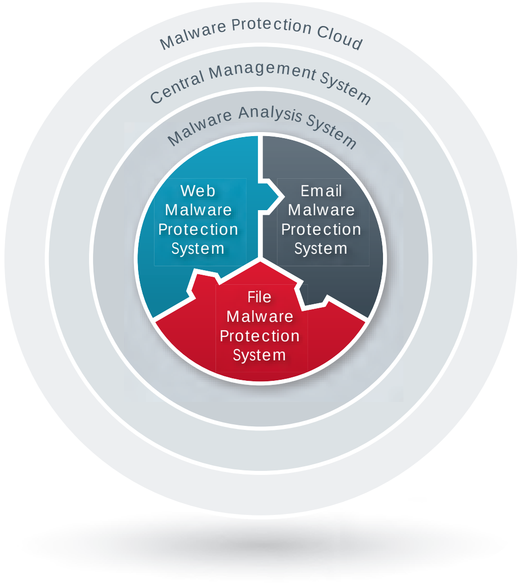
FireEye gleans rich information from this testbed, such as the IP address, protocols, and ports that an attacker uses to communicate and distribute malware. With this data, FireEye can block outreach by a compromised host to its command and control center. Even "patient zero" can be secured against sending out data or downloading more malware when FireEye systems are used inline. Detailed reports help system administrators identify infected hosts for clean up.

Intelligent Cloud For Real–Time Data Exchange

FireEye customers can also subscribe to the FireEye Malware Protection Cloud to share insights and keep protections up to date. As FireEye analyzes code for malicious actions, it creates a fingerprint of all confirmed malware. These dynamically generated signatures can be shared in real time by FireEye Malware Protection Systems.



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


Malware Protection Cloud
Central Management System
Malware Analysis System
Web Malware Protection System
Email Malware Protection System
File Malware Protection System

Complete solution portfolio to stop advanced targeted attacks

Integrated Web, Email, and File Share Protection to Stop Blended Threats

Many threats use multiple vectors and multiple stages to bypass traditional protections. One might enter the network as an innocent looking email with an innocuous shortened URL. When the user clicks the URL, an array of drive-by downloads assaults the browser, looking for any vulnerability. FireEye appliances can team to detect spearphishing, URLs, and malicious attachments and cut off blended threats.

The FireEye Product Family

Through a scalable range of turnkey appliances with centralized management, FireEye can help protect your organization and its data against the fast-changing landscape of advanced targeted attacks.

FireEye

Next Generation Threat Protection

FireEye, Inc. is the leader in stopping advanced targeted attacks that use advanced malware, zero-day exploits, and APT tactics. FireEye solutions supplement traditional and next-generation firewalls, IPS, antivirus and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across both Web and email threat vectors as well as latent malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners and Juniper Networks.

FireEye, Inc.
1390 McCarthy Blvd.
Milpitas, CA 95035

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