



NEXT GENERATION THREAT PROTECTION

# Next Generation Threat Protection

Move From Compromise to Confidence

**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 different tools and targeting intellectual property and other networked assets.

Replacing mass-market malware, this next generation of threats is personalized and persistent. Threats are targeted, ever morphing, dynamic and zero-day. These carefully staged attacks look innocent as they walk by traditional firewall, IPS, anti-virus and Web gateways that rely on signatures and known patterns of misbehavior. Once inside, malware phones home for instructions, which could be to steal data, infect other endpoints, allow reconnaissance, or lie dormant until the attacker is ready to strike.

**“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*

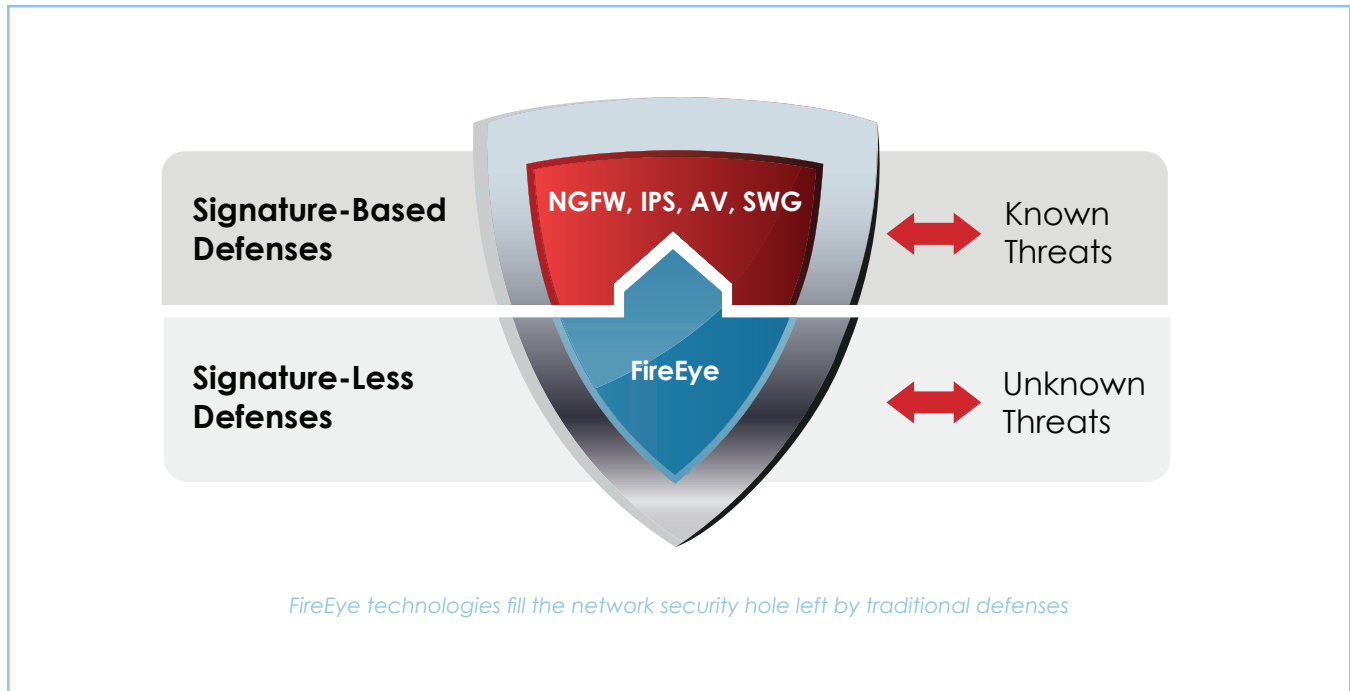
Today, security-conscious enterprises and Federal governments choose FireEye™ for industry leading protection against these next-generation threats. FireEye combats advanced malware, zero day and targeted APT attacks. FireEye's convenient appliances supplement next-generation and traditional firewalls, IPS, AV and web gateways, adding integrated inbound and outbound protection against today's stealthy Web and email threats.

**“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, **95%** of enterprises have discovered compromised hosts within what they thought were secure networks.

—Findings from enterprise evaluations of FireEye Malware Protection Systems.



## The Only Defense Against Advanced Malware, Zero Day & Targeted APT Attacks

FireEye's Web and Email Malware Protection Systems (MPS) defeat the next-generation 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.

Dynamic 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 attachments and Web objects to convict the bad actors and let the good guys go free. 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.

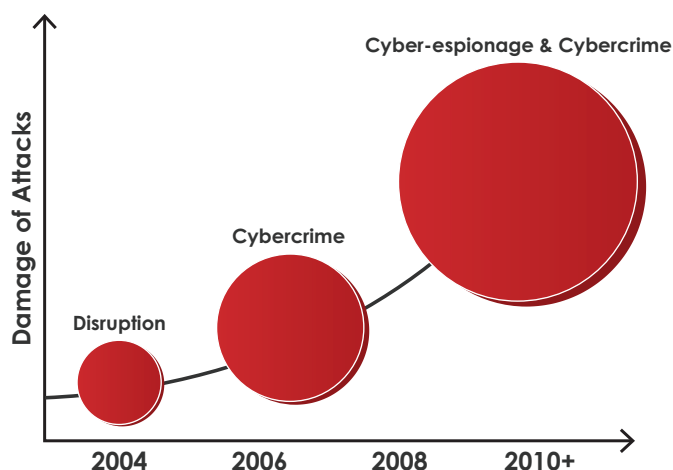
By including a broad range of operating systems, applications, browsers, and add-ons, the FireEye environment presents real-world targets to trigger the full set of zero day exploits, rootkits, privilege escalations, and other malicious functions in next-generation threats.

## Outbound Blocking Protects Automatically Across Protocols

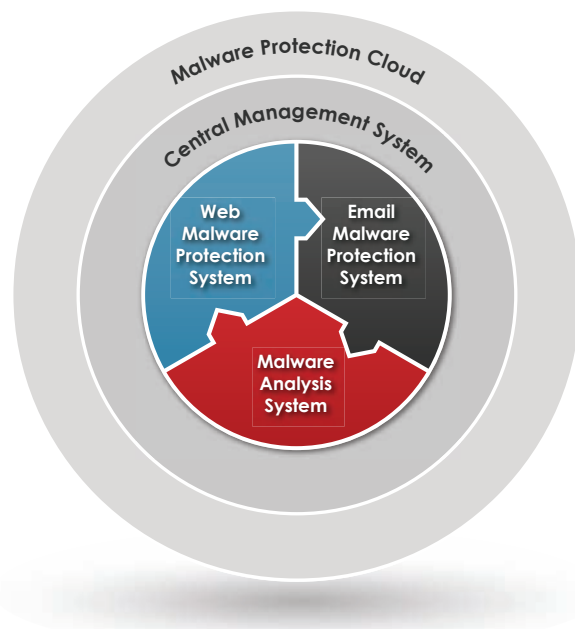
FireEye gleans rich information from this testbed, such as the IP address, protocols and ports an attacker uses to communicate and distribute payloads. With this data, FireEye can block outreach by a compromised host to its command and control center. Even "patient zero" can be secured against sending 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 intent, it creates a fingerprint of all confirmed malware. These dynamically generated signatures can be shared in real time by FireEye Malware Protection Systems.



*The New Status Quo : Advanced Attacks*



*Integrated, multi-stage protections keep FireEye customers ahead of advanced malware*

## Integrated Web & Email Protection

Many threats use separate channels and successive stages to bypass traditional protections. One might enter the network as an innocent looking email with an innocuous or 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 next-generation threats.

# WONDERING IF YOUR DEFENSE-IN-DEPTH TEAM NEEDS A NEW PLAYER?

Give your security a “next-generation threat” check up.

Risk Factor	Test
“71% of surveyed IT Security Professionals said the ‘changing/evolving nature of threats’ is a major challenge or challenge.” <sup>1</sup>	Can you show that dynamic defenses stop targeted, zero-day attacks in Web or email or both?
“Malicious attacks were the root cause of 31% of the data breaches studied.” <sup>2</sup>	Do you automatically block attempts to exfiltrate sensitive data, such as credentials, source code, or personally identifiable information (PII)?
“Incumbent defense technologies fall short.” <sup>3</sup>	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. <sup>4</sup>	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. <sup>5</sup>	How often is your protection updated to reflect the changing global threat landscape?

<sup>1</sup> Forrsights: The Evolution Of IT Security, 2010 To 2011, Forrester Research, Inc., February 15, 2011, Jonathan Penn and Heidi Shey

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

<sup>3</sup> Malware And Trojans And Bots, Oh My!, Chenxi Wang, Forrester Research, Inc. February 28, 2011.

<sup>4</sup> InformationWeek’s 2010 Strategic Survey.

<sup>5</sup> <http://www.sophos.com/security/topic/security-threat-report-2011.html>



FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

---

**FIREEYE, Inc.**  
1390 McCarthy Blvd.  
Milpitas, CA 95035

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