FireEye™

FireEye: Reimagining Security to Prevent, Detect, Contain, and Resolve Today's Advanced Attacks

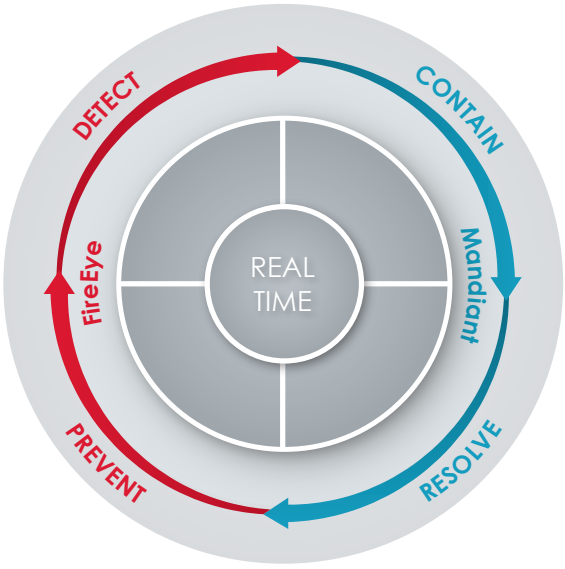
"With FireEye, we can now see and stop the attacks targeting our in-house and remote users. It has been an eye-opener for us to be able to determine with accuracy the threats that are passing through the firewall, URL gateway, IPS, and anti-virus."

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

Yesterday's defenses can't hold off today's assaults. The traditional security model is not just eroding – it has collapsed. Despite tens of billions of dollars spent on IT security every year,[1] today's advanced cyber attacks easily bypass most defenses. A widening gap between threat actors' offensive abilities and woefully outdated defenses has left organizations more exposed than ever.

To protect corporate assets, organizations must take a fundamentally new approach to cyber defense. That is why FireEye has reimagined and redefined security. The FireEye platform, which includes services from Mandiant, is the first in the industry to deliver truly continuous threat protection.

This powerful synthesis of technology, services, and dynamic threat intelligence safeguards your corporate assets in real time, all the time. From ingress point to endpoint, FireEye helps organizations around the world prevent, detect, contain, and resolve today's advanced threats.



FireEye Continuous Threat Protection

The changing threat landscape

Today's cyber threat landscape is rapidly evolving. Broad, scattershot attacks designed for mischief have given way to highly advanced attacks focused on specific objectives. Nationstate threat actors, well-funded campaigns, highly motivated adversaries, and remarkably sophisticated attacks have become the norm. The headlines are a constant reminder: attackers are dead set on breaching your systems and stealing valuable assets such as intellectual property, customer data, financial information, and the like.

These targeted attacks occur across all industries. They are sophisticated and stealthy. They are targeted and persistent. And they go largely undetected by traditional security technologies, such as next-generation firewalls, traditional IPS, anti-virus (AV) software, and secure email and Web gateways.

Cutting across multiple threat vectors, such as Web, email, file shares, and mobile devices, these attacks unfold in multiple stages. Through a sequence of calculated steps, malware gets in, signals back out of the compromised network, and gets valuables out.

Traditional defenses were designed for an older generation of attacks. They rely heavily on malware signatures and known patterns of behavior. That approach leaves organizations exposed to fast-moving, ever-evolving threats that exploit previously unknown, zero-day vulnerabilities. Even most sandboxes, touted as a fresh approach to security, are constrained by many of the same old flaws.

To combat these attacks, organizations must embrace a continuous threat protection model. This means preventing and detecting threats in real time. And it means reducing the time to contain and resolve them – before they can hurt your organization.

1 IDC. "Worldwide Datacenter Security 2012-2016 Forecast: Protecting the Heart of the Enterprise 3rd Platform." November 2012.

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

Findings from enterprise evaluations of FireEye platforms.

The FireEye platform

The core of the platform is the patented FireEye® Multi-Vector Virtual Execution™ (MVX) engine, which dynamically analyzes advanced malware in real time. The MVX engine captures and confirms zero-day and advanced persistent threat (APT) attacks. The MVX engine does not rely on malware signatures or reputations. Instead, it detonates suspicious files, Web objects, and email attachments within hardened, instrumented virtual-machine environments.

It analyzes multiple stages, and flows, of attacks to understand their full context. This stateful analysis is critical to piecing together the entire attack life cycle, from initial exploit to data exfiltration.

Point products that focus on single objects – such as executable (EXE), dynamic linked library (DLL), or portable document format (PDF) files – miss advanced attacks. These products include most sandboxes, which analyze files and objects in isolation. They, too, are blind to the full attack life cycle.

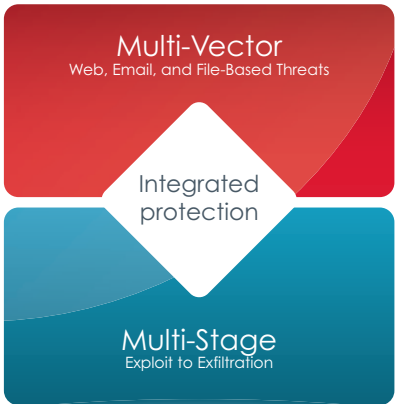
With the FireEye platform, organizations can leverage cutting-edge technology, world-class services, and dynamic threat intelligence to protect their most important assets.

Threat Prevention Platforms

FireEye threat prevention platforms shield all major threat vectors from advanced attacks. Powered by the MVX engine, these appliances help companies detect and understand the entire attack life cycle. The platforms correlate malicious activity across multiple threat vectors and stages to prevent and detect attacks. And with near-zero false positives, they don't waste your time.

Products include:

- **NX Series** – Stops Web-based attacks, zero-day Web exploits, and multi-protocol callbacks to keep sensitive data and systems safe.
- **MVX-IPS** – This add-on feature of the NX Series enhances the platform with intrusion prevention system capabilities. By leveraging the MVX engine, MVX-IPS eliminates the time-wasting false positives that plague traditional IPS technology.



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

- **EX Series** – Secures against spear-phishing email and other email-based attacks that bypass anti-spam and reputation-based technologies.
- **FX Series** – Analyzes network file shares to quarantine resident malware brought into the network through the Web, email, or other manual means, such as online file sharing.
- **HX Series** – Detects endpoint compromises and isolates infected systems with a single click – even when those systems are outside of the organization's network.
- **AX Series** – Gives forensic analysts handson control over a powerful auto-configured test environment to deeply inspect threats embedded in common file formats, email attachments, and Web objects.
- **CM Series** – Consolidates management, reporting, and data sharing across multiple FireEye appliances in an easy-to-deploy, network-based platform.

Services

The FireEye platform also includes a range of services to help security teams deal with today's ever-changing threat landscape. Whether organizations need help combating unusually complex threats or want to stretch limited IT resources, FireEye and Mandiant services can bolster your security operations. Make security our job so you can focus on your business.

FireEye services include 24x7 product support, threat and vulnerability assessments, training, cloud-based offerings, managed defense solutions, and Mandiant services.

Managed defense
FireEye offers three tiers of managed defense with pricing and service levels to match a variety of business needs and budgets.

The managed defense portfolio includes:

- Continuous Monitoring – FireEye experts monitor your security alerts around the clock to provide a "second set of eyes" to monitor system health, flag the alerts that matter most, and also provide a bird's-eye view of attacks across an industry or geography.
- Continuous Protection – Adds active threat analysis for faster containment and remediation. A compromise report reveals valuable information about the attack and a clear, detailed plan for combatting it.
- Continuous Vigilance – Incorporates custom threat intelligence that enables subscribers to focus their efforts and tailor their defenses to specific attacks as they unfold.

Dynamic Threat Intelligence
To combat today's advanced threats, organizations must understand more than justthe attack itself. They must understand who is behind it, how the attackers operate, and what they're after.

To that end, FireEye offers a wealth of threat intelligence that combines data gathered from FireEye deployments and in-house research from the FireEye and Mandiant teams. Here's how FireEye Dynamic Threat Intelligence helps organizations combat advanced threats:

- The FireEye Dynamic Threat Intelligence™ (DTI) cloud interconnects FireEye threat prevention platforms deployed within customer networks, technology partner networks, and service providers around the world. In addition to auto-generated threat intelligence, the DTI cloud incorporates new threat findings from FireEye Labs.
- The APT Discovery Center catalogs and analyzes hundreds of current and past APT campaigns and characterizes APT attacks by technical footprint, geography, and target customer or industry.

The combination of the DTI cloud and APT Discovery Center help security teams, law enforcement, and governments understand the trends and drivers behind various threats to continuously improve defenses.

Network Forensics Platform
The FireEye® Network Forensics Platform allows you to identify and resolve security incidents faster by capturing and indexing full packets at extremely rapid speeds. With the Network Forensics Platform, you can detect a broad array of security incidents, improve the quality of your response, and precisely quantify the impact of each incident.

The Network Forensics Platform provides a powerful complement to the FireEye comprehensive threat prevention capabilities. In addition to receiving precise alerts and correlated threat information, analysts can also get a fine-grained view of the specific packets and sessions before, during, and after the attack to confirm what may have triggered a malware download or callback, to respond rapidly and effectively, and to apply this information to enhancing future protective strategies.

Ultrafast access to historical network data is a necessity for security personnel in reducing mean time to resolution, as well as answering the key questions: how long has the breach been present, what data may have already left the network, and how many other hosts may already have been compromised?

Highlights

- Continuous, lossless packet capture with nanosecond time stamping at recording speeds up to 20 Gbps
- Real-time indexing of all captured packets using time stamp and connection attributes. Export of flow index in NetFlow v5, v9, and IPFIX formats for use with other flow analysis tools
- Ultrafast search and retrieval of target connections and packets using patent-pending indexing architecture
- Web-based, drill-down GUI for search and inspection of packets, connections, and sessions
- Session decoder support for viewing and searching Web, email, FTP, DNS, chat, SSL connection details, and file attachments
- Packet payload search using regular expressions
- Industry-standard data storage and export in PCAP format, which can be stored with flexible storage options: on the appliance, SASattached, or SAN-attached storage

AVANTEC
Competence. Security. Trust.
Badenerstrasse 281 ▪ CH-8003 Zürich
Tel. 044 457 13 13 ▪ www.avantec.ch