FireEye as a Service
Technology, Expertise, and Intelligence at Your Service 24x7

SECURITY
REIMAGINED

HIGHLIGHTS

- **Monitoring by Experts.** Patented FireEye technology augmented by expert security analysts monitoring 24x7 reduces average threat detection & response time from months to minutes.

- **Applied Intelligence.** Mobilizes the latest tactical intelligence to find threats in your environment faster by operationalizing information flow from front-line incident responders, network VMs and endpoint sensors across the FireEye global defense community.

- **Answers, Not Just Alerts.** Validated compromise reports contain information about attackers and their intentions, and then tell you how to respond.

- **Purchasing Choice.** Flexible subscription and capital expense options allow you to match your security needs with payment preferences.

- **MSSP-Friendly.** Complements and strengthens the services of your existing managed security partner.
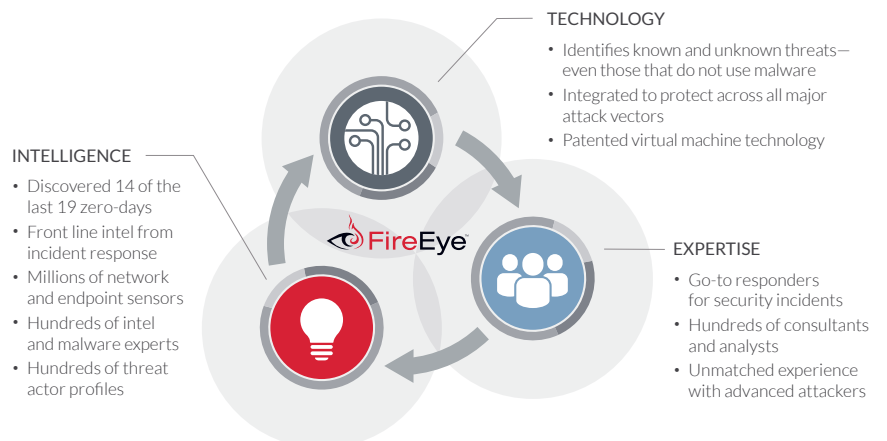
Overview

Your adversaries are people: creative, nimble and persistent. They create new malware, probe for vulnerabilities and vary exploit tactics until they gain entry. Once inside, they cover their tracks and wait patiently, assembling a toolkit and formulating an attack plan over time as they watch and learn about your employees and your network.

Technology alone will not defeat a determined attacker. You need the world's top security experts monitoring your network and systems around the clock with the industry's most advanced technology platform and the latest curated intelligence from around the world. With this combination you can detect, prevent, analyze and resolve security incidents in a fraction of the time compared to conventional approaches.

Introducing FireEye as a Service

Our aim is to help you avoid becoming a victim. First, our patented virtual machine based technology is deployed to detect and prevent most intrusion attempts against all major attack vectors. Second, we monitor your environment around the clock using analysis techniques developed from 100,000+ hours of front-line experience. When we validate signs of compromise, we send you a full report detailing the what, when, and how of the threat—context you need for effective response. In some cases, we may recommend containment using FireEye technologies to immediately quarantine systems and prevent attackers from moving laterally. Finally, FireEye incident responders with forensic expertise can help you resolve the incident quickly and assess impact for prompt, accurate disclosure.

TECHNOLOGY
- Identifies known and unknown threats— even those that do not use malware
- Integrated to protect across all major attack vectors
- Patented virtual machine technology

INTELLIGENCE
- Discovered 14 of the last 19 zero-days
- Front line intel from incident response
- Millions of network and endpoint sensors
- Hundreds of intel and malware experts
- Hundreds of threat actor profiles

EXPERTISE
- Go-to responders for security incidents
- Hundreds of consultants and analysts
- Unmatched experience with advanced attackers

Capabilities

Powerful Defense

FireEye technologies, which perform 50 billion+ virtual machine analyses and process 400,000 unique malware samples each day, are deployed in your environment. Millions of sensors collecting new intelligence around the globe are then layered with rich contextual intelligence and are updated into your FireEye ecosystem every 60 minutes, providing a powerful detection and prevention defense.

Expert Monitoring and Investigation

The FireEye team of expert threat analysts monitors your networks and endpoints 24x7, applying the latest intelligence and proprietary methodologies to look for signs of compromise. When a potential compromise is detected, the team performs an in-depth analysis on affected systems to confirm the attack.

Answers, Not Alerts

FireEye analysts leverage system and network forensics on live systems to investigate, classify, and analyze the risk in real time. Detailed reports on exactly what happened and recommendations on how to contain the threat are immediately provided.

Immediate Containment

When data theft or lateral movement is imminent, FireEye's containment feature makes it possible to react immediately by quarantining affected hosts, whether they are on or off your corporate network, significantly reducing or eliminating the consequences of a breach.

Incident Response

Quickly engage expert incident responders, when needed, to investigate breaches, re-secure your network, remediate technical damage and assess the business impact so you can make prompt and accurate disclosure, if necessary.

Continuous Improvement

Get personalized threat profiles that provide unique insight into your organization's specific risks. Who targets you and others in your industry? How, and why? Knowing these answers enables you evolve your capabilities and defenses to meet future challenges.

Global Security as a Service Centers

FireEye has audited SOC facilities in strategic locations in North America, Europe, and Asia. FireEye is Safe Harbor Certified, helping you meet your compliance requirements.

Business Model Choice

We offer a variety of technology and service purchase options, depending on your preference for capitalizing costs up front or operationalizing expenses over time. You can also scale up or down, as your needs change.

With FireEye as a Service, you have a trusted partner providing powerful technology, actionable intelligence, and skilled expertise as a fully managed service focused on advanced threat prevention. For organizations with an existing security operations center or MSSP, our co-managed model adds a fully managed service around advanced threat protection, with FireEye Threat Prevention technology, intelligence, and skilled security expertise.

FireEye