FIREEYE™

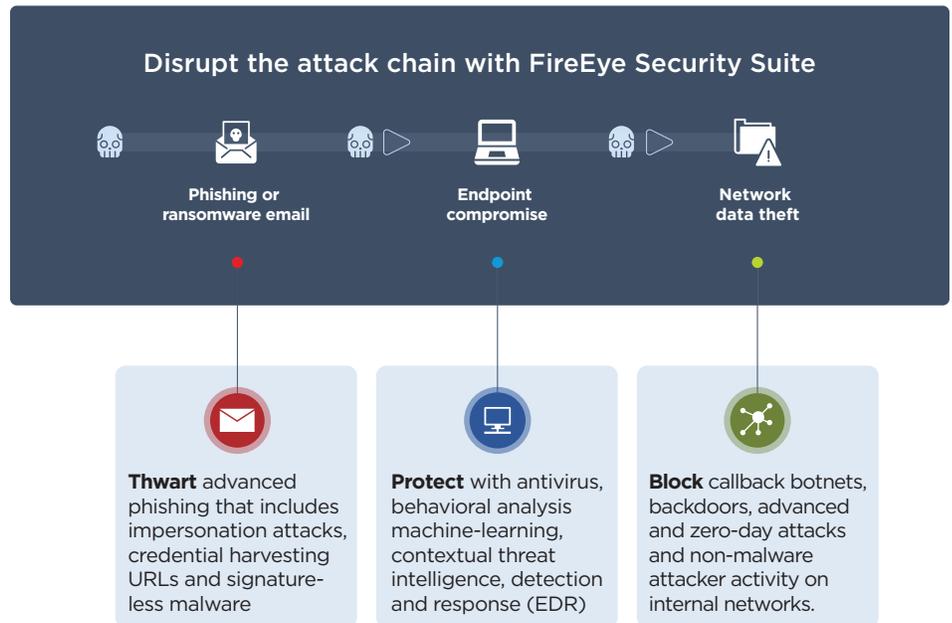# FireEye Security Suite

## Many attacks. One solution.

**HIGHLIGHTS**

- Single-console security management to protect networks, emails, and endpoints from sophisticated and targeted attacks

- Antivirus and anti-spam engines for emails and endpoints included

- Tools to investigate and rapidly respond to potential security breaches

**BUSINESS BENEFITS**

- Focus on growing your business, not managing your security

- Accelerate discovery of serious incidents to reduce risk of business impact

- Increase operational efficiency through vendor consolidation and a tightly integrated platform

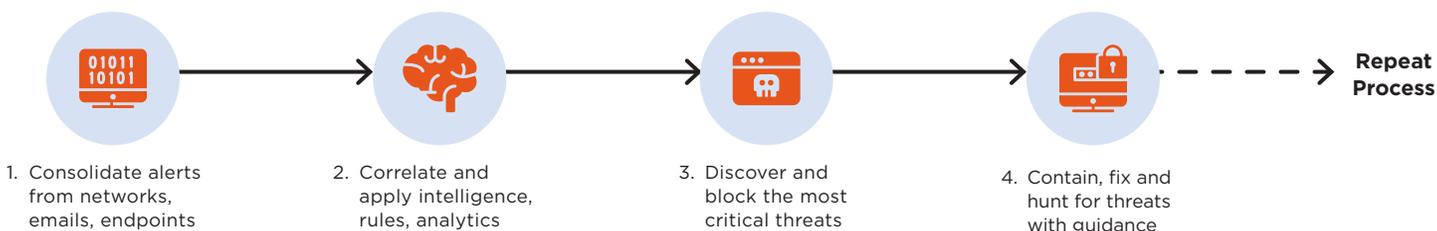- Control costs with simplified procurement and per-user pricing

Inevitably, someone in your organization will inadvertently become a link in the chain of events leading to a cyber attack. An individual may open a malicious email, but threats can also enter through endpoints and travel through your network, escalating privileges, conducting reconnaissance and stealing data.

**Disrupt the attack chain with FireEye Security Suite**

Phishing or ransomware email

Endpoint compromise

Network data theft

**Thwart** advanced phishing that includes impersonation attacks, credential harvesting URLs and signature-less malware

**Protect** with antivirus, behavioral analysis machine-learning, contextual threat intelligence, detection and response (EDR)

**Block** callback botnets, backdoors, advanced and zero-day attacks and non-malware attacker activity on internal networks.

FireEye Security Suite provides enterprise-grade protection to secure networks, emails and endpoints for organizations of all sizes. It defends against advanced attacks, accelerates incident response and safeguards the core business.

FireEye Security Suite is designed for organizations with 100-2000 users. It protects multiple attack vectors to break the chain of events that often leads to data loss and business disruption.

## How FireEye Security Suite works



1. Consolidate alerts from networks, emails, endpoints

2. Correlate and apply intelligence, rules, analytics

3. Discover and block the most critical threats

4. Contain, fix and hunt for threats with guidance

**Repeat Process**

### Protect your network
- Block advanced signature-less malware such as zero-day exploits and multi-flow attacks
- Discover and stop hard-to-find internal attacker activity that doesn't use malware
- Identify and disrupt callbacks to threat servers used to maintain a malicious presence

### Protect your email
- Stop viruses, spam and advanced impersonation attacks such as CEO fraud, also known as business email compromises (BECs).
- Prevent advanced URL threats that include zero-day, low-volume, spear phishing attacks.
- Easy cloud deployment and ideal for securing cloud email providers

### Protect your endpoints
- Engage a single agent that unifies an antivirus engine, behavioral analysis and machine-learning.
- Use the latest indicators of compromise (IOCs) from real-time threat intelligence.
- Conduct investigations quickly with detection and response tools (EDR).

### Simplify security operations
- Highlight and quickly respond to alerts that matter
- Apply contextual intelligence, rules and analytics to alerts correlated across network, email and endpoints.
- Automate tasks and create security synergies that address real-world threats.
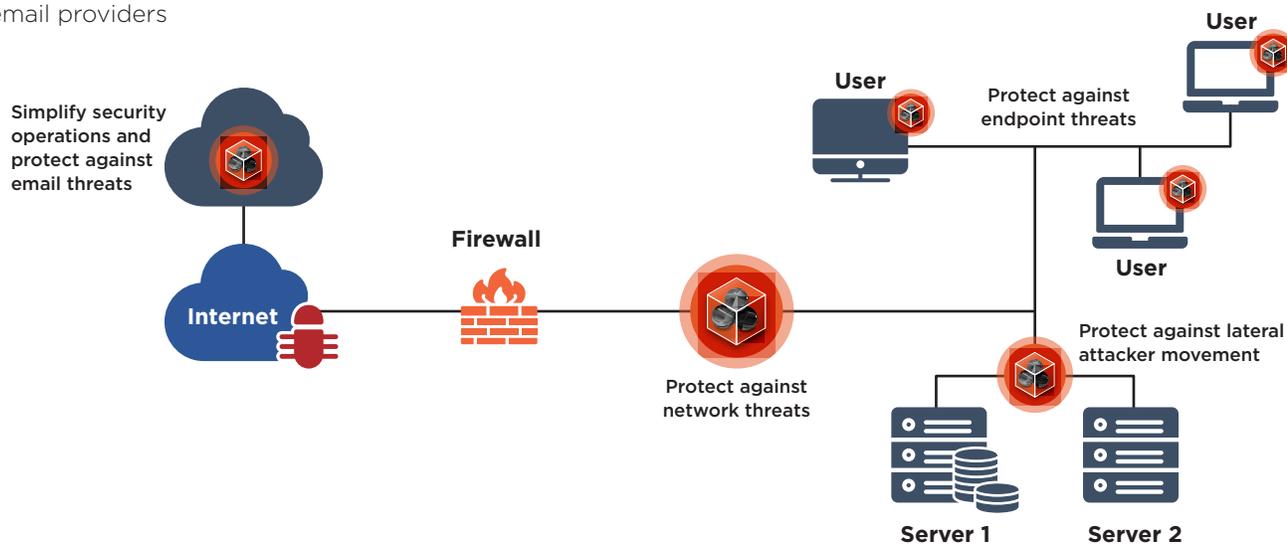


**Figure 1.** Security Suite as part of your security architecture.

## To learn more about FireEye, visit: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About FireEye, Inc.**
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.