SOLUTION BRIEF

FireEye

Disrupt attack chains to reduce business risk

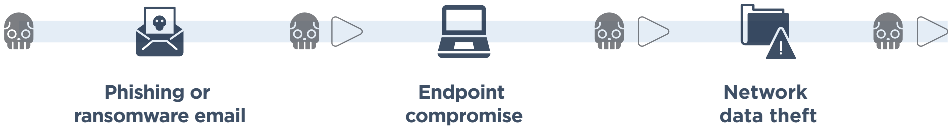
With FireEye Security Suite

91%

of cyber attacks begin with a spear-phishing email.[1]

The challenge of the cyber attack chain

Different types of threat actors have different motivations, but in the end, they all want the same thing: access to your data. Data is the currency of the 21st century. Your data is at core of every attack mission and the execution of that mission follows a standard attack chain. Security professionals work to disrupt attacks at any point in the chain — not with siloed, point products, but with an integrated, complete view to piece together clues and prevent significant business impact.



Email remains the primary method used to initiate an advanced attack or deliver ransomware because it can be highly targeted and customized to increase the odds of exploitation. While legacy anti-spam filters and antivirus software are good at catching traditional, mass phishing threats with known malicious attachments, links and content, they cannot catch the sophisticated and targeted spear-phishing and impersonation attacks designed to bypass them.

Traditional endpoint security is not effective against modern threats; it was never designed to deal with sophisticated or advanced persistent threat (APT) attacks. To keep endpoints safe, a solution must quickly analyze and respond to such threats.

Over 68% of malware is unique to an organization, and 80% of that malware is used just once,[2] making signature-based defenses ineffective against targeted attacks. Legacy and next-generation firewalls, intrusion prevention systems (IPS), and secure web gateways (SWG) are based on knowing attacker

[1] PhishMe (2016). "Enterprise Phishing Susceptibility and Resiliency Report."
[2] Joshua Goldfarb (September 19, 2016). "Detection Innovations."

methods and techniques. They struggle to detect and prevent advanced, targeted and evasive attacks. Today, common cyber criminals have access to advanced capabilities used to evade legacy network security. They can steal your data and establish a persistent presence, sometimes for months or years before they're discovered.

Attack chain disruption

Although attacks usually start with a malicious email, they can also first appear on an endpoint device or with suspicious outbound network traffic. Integrated visibility is needed to disrupt attacks at any point along the chain. 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 your core business with all the capabilities of FireEye Email Security, FireEye Endpoint Security and FireEye Network Security.

Protect your email

FireEye Email Security delivers advanced threat protection against sophisticated spear-phishing and impersonation attacks, and unknown malware to prevent unauthorized access and loss or compromise.

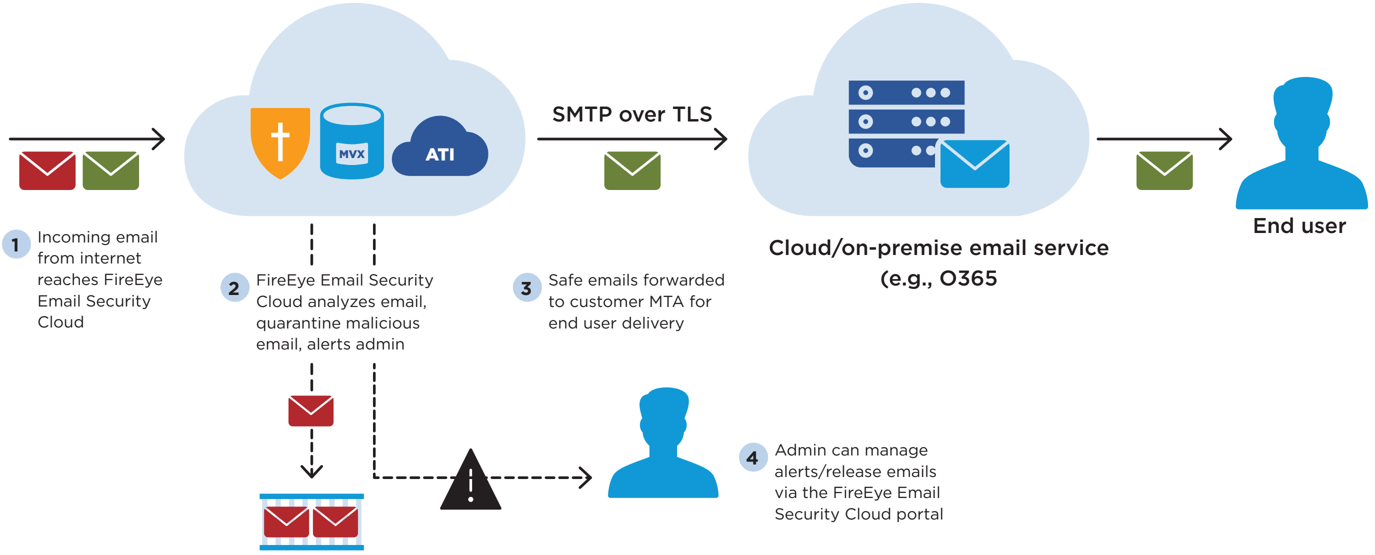

MVX
ATI
SMTP over TLS
End user
Cloud/on-premise email service
(e.g., O365
1 Incoming email from internet reaches FireEye Email Security Cloud
2 FireEye Email Security Cloud analyzes email, quarantine malicious email, alerts admin
3 Safe emails forwarded to customer MTA for end user delivery
4 Admin can manage alerts/release emails via the FireEye Email Security Cloud portal

Figure 1. Inline blocking with FireEye Email Security.

Protect your endpoints

FireEye Endpoint Security defends all entry points to your environment against common and advanced threats. Combining a signature engine, endpoint detection and response (EDR) and threat intelligence, Endpoint Security detects and blocks simple and sophisticated attacks.

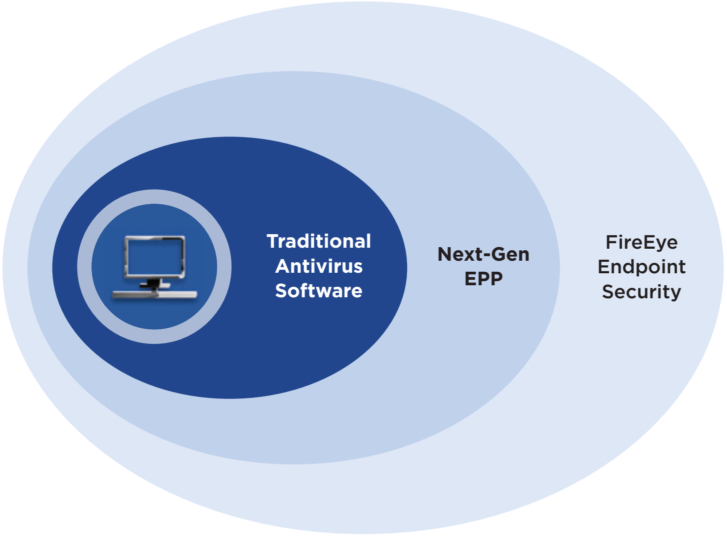


Figure 2. Expanded protections with FireEye Endpoint Security.

Protect your network

FireEye Network Security blocks advanced attacks and provides visibility into the world's most sophisticated attacks. Built on the patented multi-vector virtual execution (MVX) engine, Network Security can analyze traffic in ways no other company can match.

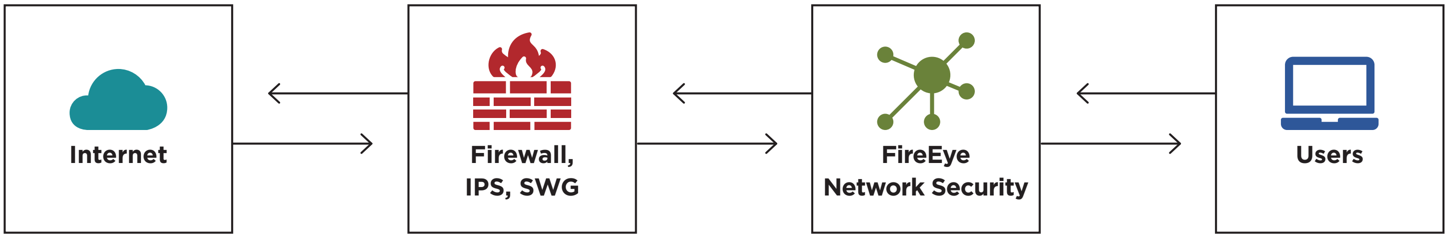


Figure 3. Reinforced defensive layer from FireEye Network Security.

How FireEye Security Suite works

In addition to providing effective security, FireEye Security Suite simplifies and automates security operations. It achieves this by integrating alerts from FireEye security solutions for email, endpoints and networks into a single cloud-based platform, FireEye Helix.

1. FireEye email, endpoint, and network security solutions each specialize in detecting a range of sophisticated attacks, but alert consolidation centralizes information to build a complete threat narrative.
2. Developed by FireEye frontline experts, analytical correlation and contextual threat intelligence help streamline the process of surfacing alerts that matter and identifying risks.
3. FireEye security solutions can block the most critical threats it discovers at each of the main attack vectors.
4. While included tools can contain threats, you also need to confirm what data was stolen, and how. Using powerful detection and response tools, you can recreate the attack chain that led to compromise and answer the key questions of a breach investigation. With these same tools and intelligence, you can also proactively hunt for threats in the absence of specific alerts.

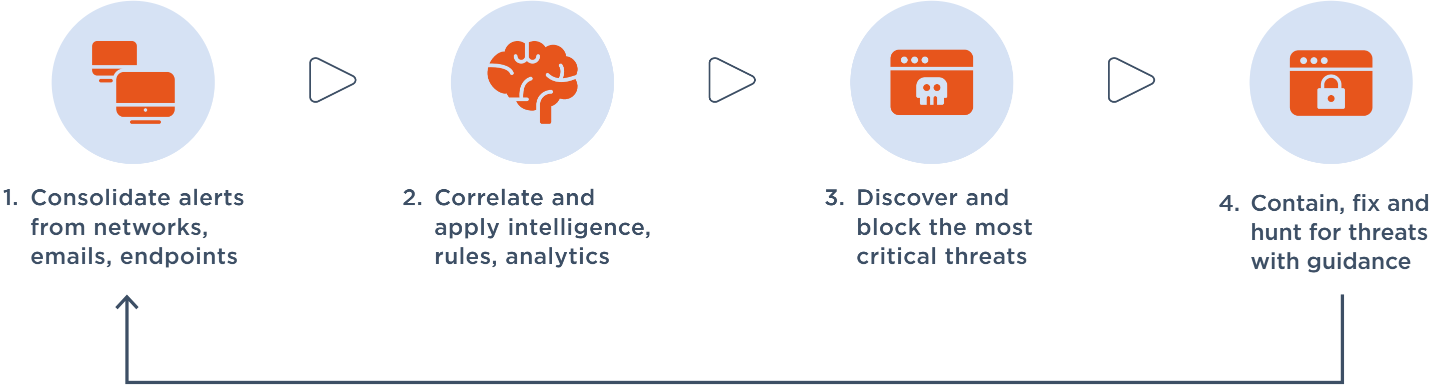

1. Consolidate alerts from networks, emails, endpoints
2. Correlate and apply intelligence, rules, analytics
3. Discover and block the most critical threats
4. Contain, fix and hunt for threats with guidance

Figure 4. Simplify and automate operations with FireEye Helix.

Get Value

FireEye Security Suite, created specifically for organizations with 100-2000 users, is designed to reduce the business risk related to loss of data confidentiality, integrity and availability. Vendor consolidation and per-user pricing means simplified procurement. It also means you can more quickly add and adopt advanced cyber security.

Control Cost

Simplify procurement with per user pricing

Improve Efficiency

Cover multiple threat vectors with vendor consolidation

Reduce Business Risk

Discover real threats faster

Case Studies

A supplier of aluminum rolled products in Malaysia with slightly fewer than 200 users was suffering from the effects of a phishing attack when they learned about FireEye Security Suite. Since this company supports large enterprise customers globally (including Germany, Australia and Japan), they needed to demonstrate a high level of cyber security proficiency and due diligence. FireEye's reputation and the Security Suite price point were critical factors in their purchase decision.

A retail organization of natural and organic food and health products in the Philippines with approximately 350 users recognized the sensitivity of the personal data of customers in their loyalty program. FireEye emerged as a candidate to protect their data and brand reputation. The capability of the FireEye Security Suite to comprehensively cover primary attack vectors factored heavily into their purchase decision.

A home-grown integrated public transportation company in Singapore provides one-stop solutions including design, assembly and maintenance of rolling stock, as well as financing and operational management services. A costly ransomware attack precipitated the need to prevent further security incidents. Because FireEye Email Security was able to detect what their incumbent email gateway missed, they decided to adopt FireEye Security Suite and future proof their entire security framework by protecting endpoints and the network as well.

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.

FireEye®