FIREEYE™

SOLUTION BRIEF

Meet the Challenge of Evolving Network Threats

Be prepared for attacks that others miss

Today's Security Challenges

Advanced, targeted and other evasive attacks make it extremely difficult for organizations to effectively prevent cyber breaches:

- Cybercriminals use advanced attacks to evade next-generation firewalls, IPS and antivirus solutions, and hide in organizations for months (320 days on average in 2015 when notified externally)[1]
- 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
- Over 80% of alerts generated by signature- and policy-based security are unreliable[3] taking resources away from focusing on critical alerts

Today's business-driven IT transformation is adding to this challenge by expanding the organizational attack surface:

- By 2020, public cloud applications will be more than two thirds of enterprise spending.[4] Cloud-based operations increase an organization's inbound and outbound Internet traffic — and potential threats — by 40%.[5] All of this traffic must be inspected
- Non-Windows devices supported by 96% of organizations today[6] traditionally haven't been well protected
- Direct-to-Internet link adoption by 40% of branches[5] increases their exposure to attacks outside of the strongly protected central office

Four Requirements for Cyber Breach Protection

To minimize the risk of a costly cyber breach, organizations of all sizes need a solution that effectively protects against attacks. It must:

1. Detect and stop threats traditional security products miss
2. Rapidly respond and contain the impact of incidents
3. Continually adapt to the evolving threat landscape
4. Scale and remain flexible as the organization grows or the delivery mode of IT services changes

FireEye Network Security

FireEye Network Security helps organizations of all sizes minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. At the core of FireEye Network Security is the Multi-Vector Virtual Execution™ (MVX) and Intelligence-Driven Analysis (IDA) technologies. MVX is a signature-less, dynamic analysis engine that inspects suspicious objects to identify targeted, evasive and unknown threats. The IDA engines detect and block malicious objects based on machine-, attacker- and victim-intelligence.

[1] FireEye (February 2016). M-Trends 2016.

[2] Joshua Goldfarb (September 19, 2016). "Detection Innovations."

[3] Ponemon Institute LLC (January 2015). "The Cost of Malware Containment."

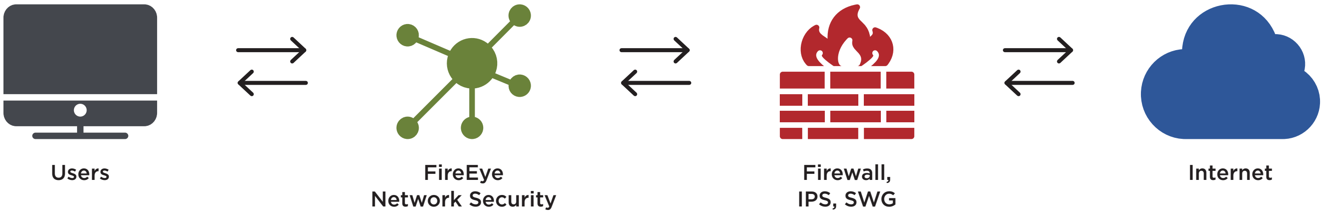
[4] Forrester (September 2016). "The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020."

[5] IDC (February 2016). "Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services."

[6] JAMF Software (2015). 2015 Survey: Managing Apple Devices in the Enterprise

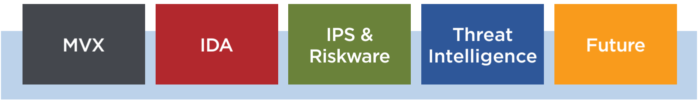
FireEye Network Security is available in a variety of form factors and deployment models. It is typically placed in the path of Internet traffic behind traditional network security appliances such as next-generation firewalls, IPS and secure web gateways (SWG) (Fig. 1).

Figure 1. Typical configuration — Network Security solutions.



To effectively protect organizations of all sizes against cyber breaches, FireEye Network Security provides:

- **Accurate detection:** MVX and IDA technologies detect attacks with high accuracy while generating a low rate of false alerts. These technologies also correlate events across multiple flows and threat vectors to protect against multistage attacks that other solutions cannot detect or stop.
- **Immediate and resilient protection:** Inline blocking of inbound exploits and malware and outbound multi-protocol callbacks immediately stop attacks. A high-availability option provides added resilience and protection when a network link or device fails.
- **Actionable insights:** Alerts include concrete evidence and contextual intelligence gained on the frontline to quickly respond to, prioritize and contain a threat.
- **Ingestion of indicators:** The Structured Threat Intelligence eXpression (STIX) format enables custom intelligence ingestion into the IDA engines.
- NEW **Extensible architecture:** Software and system design enable delivery of multiple threat protection technologies as software modules.



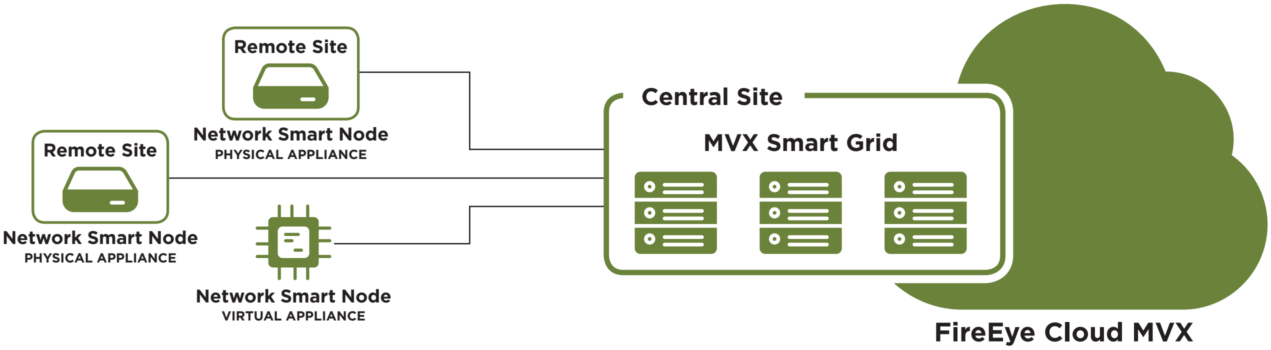
- **Comprehensive protection:** Supports diverse environments including the most common Microsoft Windows and Apple OS X operating systems, over 140 different file types and thousands of operating system, service pack and application combinations to cover a wide attack surface
- **Response workflow integration:** Alert validation, riskware categorization and pivot to packet capture for in-depth investigation automate and accelerate alert response workflows

Perfect for Your Organization

FireEye Network Security offers flexible and scalable deployment options up to 8 Gbps for the needs and budgets of midsize to large organizations.

- **Integrated Network Security:** a standalone, all-in-one hardware appliance that uses the MVX service to secure a single Internet access point
- NEW **Distributed Network Security:** Network Smart Nodes and the shared MVX service extend protection across an entire organization (Fig. 2)
  - **Network Smart Node:** physical or virtual appliances deployed at Internet access points to identify and protect against suspicious activity
  - **MVX Smart Grid or FireEye Cloud MVX:** On-premise or cloud-based MVX service that conducts further analyses to detect advanced attacks and make security teams more efficient

Figure 2. Distributed Network Security.



FireEye Network Security Essentials offers cost-effective, integrated and distributed deployment options ranging from 10 Mbps to 2 Gbps for small to midsize organizations.

Table 1. FireEye Network Security deployment options.

	Integrated appliance	Network smart node	MVX Smart Grid Requires network smart nodes	FireEye Cloud MVX Requires network smart nodes
FireEye Network Security for midsize-to-large organizations	On premise	Physical or virtual	On premise and distributed	Cloud-based and distributed
FireEye Network Security Essentials for small-to-midsize organizations	On premise	Physical or virtual	Not available	Cloud-based and distributed

Fast Payback Period

Designed to meet the needs of single-site and distributed multisite organizations, FireEye Network Security minimizes the risk of cyber breaches and reduces the payback period.

According to a recent Forrester Consulting study,[7] FireEye Network Security customers can expect a 152% ROI from cost savings over three years, and payback on their initial investment in just 9.7 months. Present and future cost savings can be achieved by:

- Focusing security team resources on real attacks to reduce operational expenses
- Optimizing capital spend with options to share MVX capacity and a large variety of performance points to right size the deployment
- Future proofing investment by allowing incremental capacity expansion when the number of branches or the amount of Internet traffic grows
- Protecting existing investment by allowing cost-free migration from integrated to distributed deployment
- Lowering future capital outlays with modular and extensible architecture

Why Choose FireEye Network Security?

The FireEye MVX engine is the original and most successful advanced[8] threat protection solution on the market:

- Since 2013, FireEye has discovered more zero-day attacks actively exploited in the wild than all other solutions combined.
- In 2016, Frost & Sullivan recognized FireEye as the undisputed market leader with 56% market share, more than the next ten competitors combined.[9]
- FireEye Network Security has been a recipient of numerous awards from SANS Institute, SC Magazine, CRN and others.
- FireEye Network Security was the first security solution on the market to receive the US Department of Homeland Security SAFETY Act certification.

U.S. DEPARTMENT OF HOMELAND SECURITY
CERTIFIED
SAFETY ACT
www.safetyact.gov
SCIENCE AND TECHNOLOGY

[7] Forrester (May 2016). "The Total Economic Impact Of FireEye."

[8] IDC (2015). Worldwide Specialized Threat Analysis and Protection Market Shares.

[9] Frost & Sullivan (September 2016). "Network Security Sandbox Market Analysis."

Table 2. FireEye Network Security benefits.

CAPABILITY	BENEFIT
Detect and stop threats traditional security products miss	
Signature-less threat detection (MVX)	Detects multi-flow, multi-stage, zero-day, polymorphic, ransomware and other evasive attacks
Real-time and retroactive detection	Detects known and unknown threats in real time while also enabling back-in-time detection of threats
Multi-vector correlation	Automates validation and blocking of attacks across email, endpoint and file vectors
Multi-OS, multi-file and multi-application support	Supports heterogeneous endpoint environments for a wide range of applications
Hardened hypervisor	Provides evasion proofing
Rapidly respond and contain the impact of incidents	
Real-time inline blocking	Immediately stops attacks
Integrated security workflows	Pivots from detection to investigation and response
High availability (HA)	Resilient defense
Signature-based IPS detection with noise reduction	Automates and accelerates triaging of traditionally noisy alerts to eliminate manual overhead
Riskware detection and categorization	Categorizes critical and non-critical malware to prioritize response resources
Actionable contextual intelligence	Accelerates containment of advanced threats with in-depth information about the attack and attacker
Continually adapt to the evolving threat landscape	
Real-time threat intelligence sharing	Globally-shared real evidence to immediately block previously unknown attacks and accelerate response
NEW **Custom and third-party threat intelligence (STIX)**	Ingest FireEye and third-party indicators into the STIX-enabled IDA engines
Strategic threat intelligence	Enables a proactive assessment of threat landscape changes and empowers a lean-forward security posture
Scale and remain flexible as the organization grows or the delivery mode of IT services changes	
Supported bandwidths	10 Mbps – 8 Gbps
Supported scale	Single site to thousands of sites for distributed deployments
Supported form factors	Physical, virtual, cloud
Deployment models	Integrated Network Security and Distributed Network Security with Network Smart Nodes and MVX service 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

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. N-EXT-DS-US-EN-000030-02

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™