DATA SHEET

# FireEye Network Security

## Effective protection against cyber breaches for midsize to large organizations

**Overview**

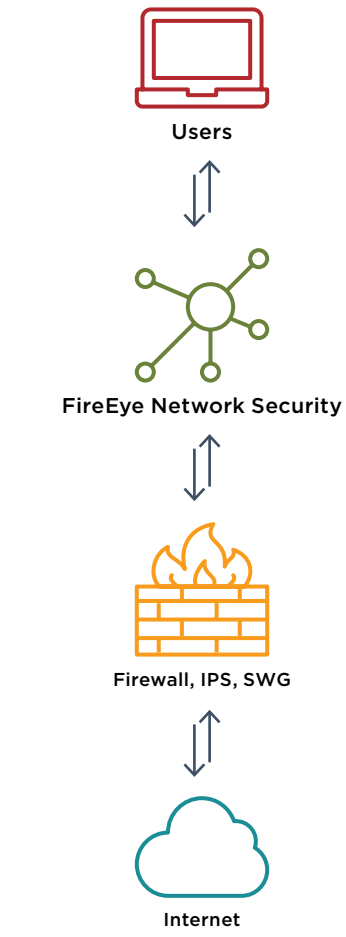
FireEye Network Security is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. It facilitates efficient resolution of detected security incidents in minutes with concrete evidence, actionable intelligence and response workflow integration. With FireEye Network Security, organizations are effectively protected against today's threats whether they exploit Microsoft Windows, Apple OS X operating systems, or application vulnerabilities; are directed at the headquarters or branch offices; or are hidden in a large volume of inbound Internet traffic that has to be inspected in real time.

At the core of FireEye Network Security are the Multi-Vector Virtual Execution™ (MVX) and dynamic machine learning and artificial intelligence (AI) technologies.

MVX is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. Multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time and retroactively, based on the latest machine-, attacker- and victim- intelligence. FireEye Network Security also includes intrusion prevention system (IPS) technology to detect common attacks using conventional signature matching.

FireEye Network Security is available in a variety of form factors, deployment and performance options. 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). FireEye Network Security supplements these solutions by rapidly detecting both known and unknown attacks with high accuracy and few false positives, while facilitating an efficient response for each alert.

**Figure 1.** Typical configuration — Network Security solutions.



| Capabilities | Benefits |
|---|---|
| **Detection** | |
| Accurate detection of advanced, targeted and other evasive cyber attacks | Minimizes risk of costly cyber breaches |
| Modular and scalable security architecture | Provides investment protection and supports business growth. |
| Consistent level of protection for multi-OS environments and all Internet access points | Creates a strong defense across the entire organization for all types of devices |
| Integrated, distributed, physical, virtual, on-premise and cloud deployment options | Offers flexibility to align with organizational preferences and resources |
| Multi-vector correlation with Email and Content Security | Provides visibility across wider attack surface |
| **Prevention** | |
| Immediate blocking of attacks at line rates from 250 Mbps to 10 Gbps | Gives real-time protection against evasive attacks |
| Visibility into encrypted traffic | Built-in TLS 1.3 decryption support available on appliances without an additional license fee |
| **Response** | |
| Low rate of false alerts, riskware categorization and mapping to MITRE ATT&CK framework | Reduces operational cost of triaging unreliable alerts |
| Pivot to investigation and alert validation, endpoint containment and incident response | Automates and simplifies security workflows |
| Execution evidence and actionable threat intelligence | Accelerates prioritization and resolution of detected security incidents |

## Technical Advantages

### Accurate and Actionable Threat Detection and Insights

FireEye Network Security uses multiple analysis techniques to detect attacks with high accuracy and a low rate of false alerts:

- **Multi-Vector Virtual Execution™ (MVX) engine** detects zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.
- **Multiple, dynamic machine learning, AI and correlation engines** detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights gathered on the front lines from thousands of hours of incident response experience. It stops infection, compromise and intrusion phases of the cyber attack kill chain by identifying malicious exploits, malware, phishing attacks and command and control (CnC) callbacks. It also extracts and submits suspicious network traffic to the MVX engine for a definitive verdict analysis.
  In addition to client-side protection, engines support server side detections, lateral movement detection and detection on post-exploitation traffic.
- Alerts generated by FireEye Network Security include concrete real-time evidence to quickly respond to, prioritize and contain targeted and newly discovered attacks. Detected threats can also be mapped to the MITRE ATT&CK framework for contextual evidence.

### Immediate and Resilient Protection

FireEye Network Security offers flexible deployment modes including:

- Out-of-band monitoring via a TAP/SPAN, inline monitoring or inline active blocking. Inline blocking mode automatically blocks inbound exploits and malware and outbound multi-protocol callbacks. In inline monitoring mode, alerts are generated and organizations decide how to respond to them. In out-of-band prevention mode, FireEye Network Security issues TCP resets for out-of-band blocking of TCP or HTTP connections.
- Selected models offer an active high availability (HA) option to provide resilience in case of network or device failures.

### Wide Attack Surface Coverage

FireEye Network Security delivers a consistent level of protection for today's diverse network environments:

- Support for most common Microsoft Windows and Apple Mac OS X operating systems.
- Analysis of over 160 different file types, including portable executables (PEs), active web content, archives, images, Java, Microsoft and Adobe applications and multimedia.
- Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations.
- Protection against advanced attacks and malware types that are difficult to detect via signatures: web shell uploads, existing web shells, ransomware, cryptominers.

### Validated and Prioritized Alerts

In addition to detecting genuine attacks, FireEye MVX technology is also used to validate alerts detected by conventional signature-matching methods and to identify and prioritize critical threats:

- Intrusion prevention system (IPS) with MVX engine validation reduces the time required to triage signature-based detection that is traditionally prone to false alerts
- Riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response

### Response Workflow Integration

FireEye Network Security can be augmented in several ways to automate alert response workflows:

- **FireEye Central Management** correlates alerts from both FireEye Network Security and FireEye Email Security for a broader view of an attack and to set blocking rules that prevent the attack from spreading further
- **FireEye Network Forensics** integrates with FireEye Network Security to provide detailed packet captures associated with an alert and enable in-depth investigations
- **FireEye Endpoint Security** identifies, validates and contains compromises detected by FireEye Network Security to simplify containment and remediation of affected endpoints

### Flexible Deployment Options

FireEye Network Security offers various deployment options to match an organization's needs and budget:

- **Integrated Network Security:** standalone, all-in-one hardware appliance with integrated MVX service to secure an Internet access point at a single site. FireEye Network Security is an easy-to-manage, clientless platform that deploys quickly without requiring rules, policies or tuning.
- **Distributed Network Security:** extensible appliances with centrally shared MVX service to secure Internet access points within organizations
  - **Network Smart Node:** physical or virtual appliances that analyze Internet traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis
  - **MVX Smart Grid:** on-premise, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance and automated load balancing
  - **FireEye Cloud MVX:** FireEye-hosted MVX service subscription that ensures privacy by analyzing traffic on the Network Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.
  - **Protection on-premise or in the cloud:** In addition to stand-alone and virtual appliances, FireEye offers Network Security in the Public Cloud with availability in both Amazon and Azure.

**Figure 2.** Examples of Integrated Network Security include NX 2550, NX 3500, NX 5500, NX 10550.

**Figure 3.**

Distributed deployment models for Network Security.

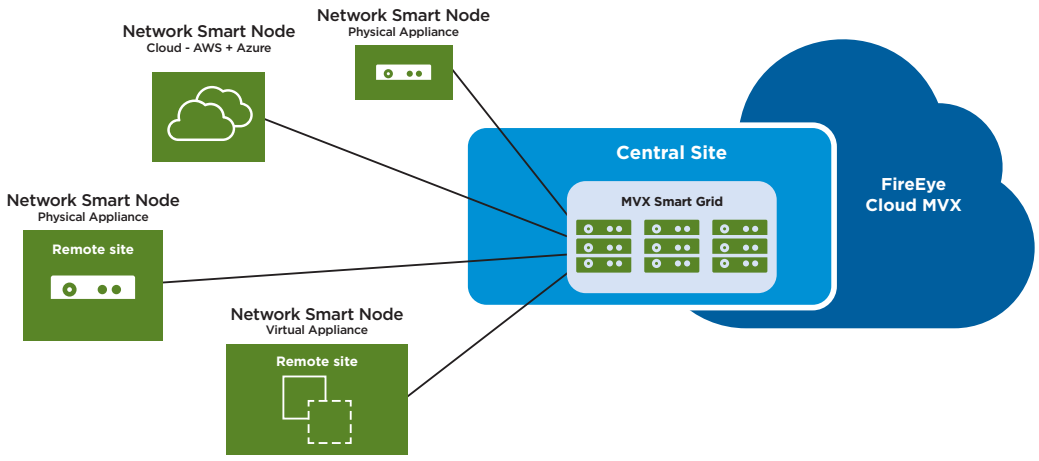
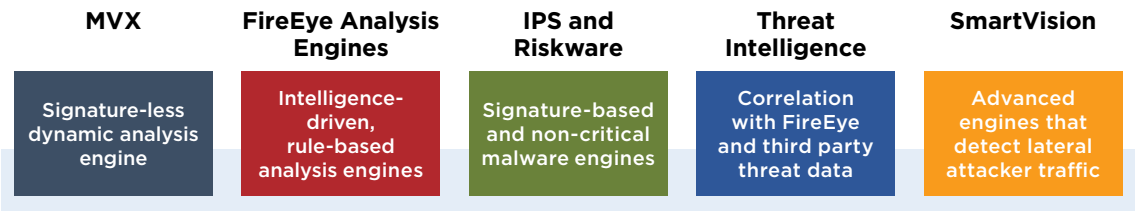



**Figure 4.**

Modular components of FireEye Network Security.




## High Performance and Scalability

FireEye Network Security protects Internet access points at line rate with performance options for a wide variety of branch and central office sizes:

The MVX Smart Grid and FireEye Cloud MVX scalable architecture allows the MVX service to support one Network Smart Node to thousands and scale seamlessly as needed.

| Form Factor | Performance |
|---|---|
| **Integrated Network Security** | 50 Mbps to 5 Gbps |
| **Physical Network Smart Node** | 50 Mbps to 10 Gbps |
| **Virtual and Public Cloud Network Smart Node** | 50 Mbps to 8 Gbps |

## Business Benefits

Designed to meet the needs of single-site and distributed multi-site organizations, FireEye Network Security delivers several benefits:

### Minimizes Risk of Cyber Breaches

FireEye Network Security is a highly effective cyber defense solution that:

- Prevents intruders from breaking into an organization to steal valuable assets or disrupt business by stopping advanced, targeted and other evasive attacks
- Stops attacks and contains intrusions faster with concrete evidence, actionable intelligence, inline blocking and response workflow automation
- Eliminates weak points from an organization's cyber defenses with consistent protection for various operating systems, application types, branches and central sites

### Short Payback Period

According to a Forrester Consulting study[1], FireEye Network Security customers can expect a 152% ROI savings over three years and payback on their initial investment in just 9.7 months. FireEye Network Security:

- Focuses security team resources on real attacks to reduce operational expenses
- Optimizes capital spend with a shared MVX service and a large variety of performance points to rightsize deployment to meet requirements
- Future-proofs security investment by scaling smoothly when the number of branches or the amount of Internet traffic grows
- Protects existing investments by allowing cost-free migration from an integrated to a distributed deployment
- Reduces future capital outlay with modular and extensible architecture

1 Forrester (May 2016). The Total Economic Impact of FireEye.

## Awards and Certifications

The FireEye Network Security product portfolio has been awarded a number of industry and government awards and certifications:

- In 2020, FireEye won first place in the Naval Information Warfare Systems Command (NAVWAR) Artificial Intelligence Cybersecurity Challenge[2]
- In 2020, KuppingerCole awarded FireEye the Leadership Compass for Network Detection and Response[3]
- In 2020, Forrester recognized FireEye as a large vendor for Network Analysis and Visibility[4]
- In 2018, Frost & Sullivan recognized FireEye as the undisputed market leader with 46% market share, more than the next ten competitors combined[5]
- FireEye Network Security holds certifications including Common Criteria, FIPS 140-2 and SOC 2
- 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


2 FireEye (January 6, 2021). Naval Information Warfare Systems Command (NAVWAR) Awards FireEye First Place in Network Threat Detection Challenge.
3 KuppingerCole (June 10, 2020). Leadership Compass Network Detection and Response.
4 Forrester (June 23, 2020) Now Tech: Network Analysis and Visibility, Q2 2020.
5 Frost & Sullivan (July 5, 2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.


FireEye Network Security is part of FireEye XDR
Learn more at **www.FireEye.com/XDR**

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



**About FireEye**

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™