FireEye™

Datasheet

HX Series

Endpoint Threat Prevention Platform that Detects, Analyzes, and Resolves Security Incidents on the Endpoint

Highlights

- **Integrated network and endpoint security:** Validate and analyze network alerts by finding matching activity on endpoints.
- **Reach endpoints anywhere:** Innovative Agent Anywhere technology reaches remote endpoints outside the corporate network and behind NAT.
- **Detect threats using robust threat intelligence:** Apply threat intelligence from FireEye to find advanced threats in your IT environment.
- **Contain compromised devices with a single click:** Isolate compromised devices with a single mouse click to deny attackers access to systems while still allowing remote investigation.
- **Quickly investigate all endpoints:** Investigate tens or hundreds of thousands of endpoints in a matter of minutes.

Organizations spend millions of dollars investing in top-notch security teams and in building secure networks to prevent threats and keep attackers out of their IT environment. Despite these investments, determined attackers still manage to compromise organizations and steal their intellectual property and financial assets. The Endpoint Threat Prevention Platform equips security teams to confidently detect, analyze, and resolve incidents in a fraction of the time it takes when using conventional approaches.

Search for advanced attackers and APTs

Host-based detection Indicators of Compromise (IOCs) identify threats missed by AV, including advanced attackers and advanced persistent threats (APTs). Users are immediately notified when an IOC identifies a compromised device.

Integrate endpoint security with your network security

Seamlessly integrate with existing network security devices, such as FireEye® Network Threat Prevention Platform (NX series), to learn about current attacks and search for compromised endpoints, including those outside your corporate network using Agent Anywhere™ technology.

Accelerate triage of suspected incidents

Automatically collect evidence from endpoints involved in events seen by FireEye Threat Prevention Platforms for immediate review of host and network evidence.

Understand what happened without forensics

Agents continuously monitor and record key events so organizations can establish a timeline for suspected incidents without time-consuming disk acquisition or forensic analysis.

Contain endpoints

Take non-destructive action to isolate compromised devices and deny attackers access to systems while still allowing remote investigation.

How it works

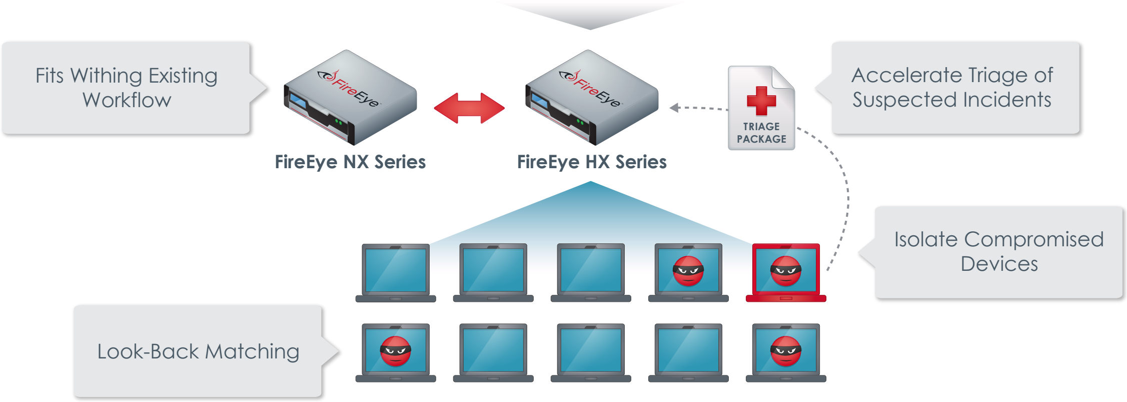
The Endpoint Threat Prevention Platform enables security operations teams to connect the dots between what's happening on their network and on their endpoints. Organizations can automatically investigate alerts generated by FireEye Threat Prevention Platforms, log management, and network security products, apply proprietary intelligence from FireEye, or sweep for IOCs, to identify the devices that have been compromised and assess the potential risk. Further, organizations can quickly triage the incident to understand the details of compromise. When a suspected incident is confirmed, the endpoints can be contained with a single click to deny the attacker access while still allowing network-based investigation to continue.

Automatically investigate alerts from network devices—Create IOCs automatically from alerts generated in network devices. Confirm threat alerts at all endpoints to identify critical issues.

Rapid interrogation of all endpoints—Investigate tens or hundreds of thousands of endpoints in a matter of minutes.

Agent Anywhere—Investigate any endpoint even when they're not on your network.

Easy to understand interface—Transform front-line analysts into investigators by making it simple and straightforward to quickly interpret data and follow up appropriately.


Fits Withing Existing Workflow
FireEye NX Series
FireEye HX Series
TRIAGE PACKAGE
Accelerate Triage of Suspected Incidents
Isolate Compromised Devices
Look-Back Matching

Technical Specifications

	HX 4000	HX 4000D
CPU	6-core, 2.5 GHz	6-core, 2.5 GHz
Memory	16 Gb	16 Gb
Disk	(4) 2 TB (RAID 10)	(4) 2 TB (RAID 10)
Number of Endpoints	Up to 100,000 Endpoints	Up to 100,000 Endpoints
Network Interfaces	(4) 10/100/1000 BASE-T Ports (2 active)	(4) 10/100/1000 BASE-T Ports (2 active)
Dimensions (WxDxH)	17.2" x 27.5" x 1.7" (43.7 x 69.9 x 4.3 cm)	17.2" x 27.5" x 1.7" (43.7 x 69.9 x 4.3 cm)
Power Supply/RAID	Dual, Hot-swap	Dual, Hot-swap
Max Power	700 W	700 W

Note: All performance values vary depending on the system configuration and traffic profile being processed.