FireEye
SECURITY REIMAGINED

HX Series

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

DATASHEET

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 within a single click workflow: 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.

Overview

Organizations invest millions of dollars on top-knotch security teams as well as security systems to prevent threats and keep attackers out. 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 traditional 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.

Extend FireEye Detection to Your Endpoints

Seamlessly extend the visibility of other FireEye® Threat Prevention Platforms, such as FireEye Network Threat Prevention Platform (NX Series), to the endpoint. The endpoint agents are updated automatically with indicators of compromise, providing integrated "defense in depth" for the most important threats: those that are occurring right now.

Validate Network Alerts

Confirm whether attacks seen on the network actually compromised an endpoint. For each alert from another FireEye product, identify all impacted endpoints. Analysts can further analyze what caused any network alert (including those from a SIEM) by viewing an automatically collected timeline of events from the impacted agent.

Complete Coverage with Agent Anywhere

Drive coverage to remote endpoints outside the corporate network using the Agent Anywhere technology no matter what kind of Internet connection they have. Indicators from current attacks are pushed to remote endpoints that aren't on networks protected by FireEye products. This allows analysts to investigate and contain endpoints anywhere in the world, with no additional VPN connection needed.

Contain endpoints

Security professionals can take immediate action to isolate compromised devices, thus denying attackers access to those systems to continue their attack. This allows the security team access to conduct a complete investigation of an incident without further risk of infection.

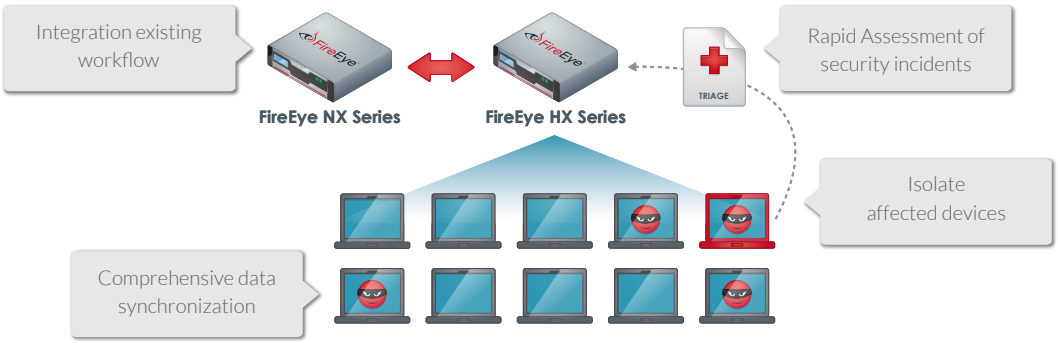
How it works

The Endpoint Threat Prevention Platform enables security operations teams to correlate network and endpoint activity. Organizations can automatically investigate alerts generated by FireEye Threat Prevention Platforms, log management, and network security products, apply intelligence from FireEye to continuously validate IOCs on the endpoints and identify if a compromise has occurred and assess the potential risk. Further, organizations can quickly triage the incident to understand the details and contain compromised endpoints with a single click and contain compromised devices within a single click workflow.

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.



Technical Specifications

	HX 4400/HX 4400D
Network Interface Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included
Front Panel LCD & Keypad	Included
PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel)	Included
USB Ports (rear panel)	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	4x 600 GB HDD, RAID 10, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
DC Power Supply	Not Available
Power Consumption Maximum (watts)	313 watts
Thermal Dissipation Maximum (BTU/h)	1068 BTU/h
MTBF (h)	35,200 h
Appliance Alone / As Shipped Weight lb. (kg)	32 lb. (15 kg) / 47 lb. (21 kg)
Safety Certifications	IEC 60950-1:2005 (Second Edition) + Am 1:2009 CSA C22.2 No. 60950-1/UL 60950-1, Second Edition CE Marking
EMC/EMI Certif ications	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE
Operating Temperature	10° C to 35° C
Operating Relative Humidity	10% to 85% (non-condensing)
Operating Altitude	5,000 f t.