FireEye
SECURITY REIMAGINED

Endpoint Security

Detect and Protect Against Unknown Attacks with Integrated Threat Intelligence

DATASHEET

HIGHLIGHTS

- Extend integrated FireEye Threat Intelligence from core to endpoint for comprehensive protection against advanced threats
- Conduct detailed endpoint investigations to identify and contain IOCs, and create event timelines with Triage Viewer.
- Detect, identify, and contain threats on tens of thousands of endpoints (connected or not) in minutes with Enterprise Security Search
- Respond rapidly to known and unknown threats with critical contextual information
- Protect all endpoints whether on- or off-premise, outside the network or behind NAT
- Contain threats and compromised devices with a single click, yet still allow remote investigation to continue.

Overview

Today's skilled attackers bypass traditional defenses most security teams have relied on for years to protect their endpoints. Even when a traditional defense stops a known threat, it can't determine what that threat was trying to do.

With FireEye Endpoint Security (HX series), organizations can proactively inspect, analyze, and contain known and unknown threats at any endpoint. Endpoint Security helps your security team hunt down and stop advanced threats with features such as Triage Viewer to view known indicators of compromise (IOCs), Enterprise Security Search to rapidly scan for and contain threats, and Data Acquisition for in-depth endpoint inspection and analysis.

Extend Threat Intelligence to Every Endpoint

To be effective, threat intelligence must be present at the point of attack. Endpoint Security seamlessly extends the threat intelligence capabilities of other FireEye products to the endpoint. If a FireEye product detects an attack anywhere in the network, endpoints are automatically updated and inspected for IOCs.

Attain Enhanced Endpoint Visibility

Visibility is critical to identifying the root cause of an alert and enables you to conduct deep analyses of the threat. The lookback cache in Endpoint Security allows you to inspect and analyze present and past network alerts (including those from a SIEM) at the endpoint. Triage Viewer provides you with an automatically collected timeline of events for any endpoint.

Get Complete Endpoint Coverage

On-site and remote endpoints outside the corporate network are key vulnerabilities. Endpoint Security covers all endpoints, pushing intelligence on IOCs to them regardless of Internet connection type. This enables you to investigate and contain endpoints anywhere in the world, without requiring additional VPN connections.

Contain Compromised Endpoints and Prevent Lateral Spread

Attacks that start at an endpoint can spread quickly through your network. After you identify an attack, Endpoint Security lets you immediately isolate compromised devices to stop the attack and prevent lateral spread—all with a single click. You can then conduct a complete forensic investigation of the incident without risking further infection.

How Endpoint Security Works

FireEye Endpoint Security uses threat intelligence to correlate alerts generated by FireEye network platforms, log management, and network security products with IOCs on any endpoint. Once a threat has been validated, Endpoint Security can investigate tens of thousands of endpoints in minutes, and isolate compromised endpoints with a single click while you assess further potential risks.

With Endpoint Security you can figure out:

- Which vectors an attack used to infiltrate your system
- If the attack spread laterally to other systems
- If an attack occurred on a specific endpoint and whether it persists
- How long an endpoint(s) has been compromised
- If IP has been exfiltrated
- Which endpoints and systems to contain to prevent further compromise

Endpoint Security Requirements

Endpoint Security requires a 1 Ghz or higher Pentium-compatible processor and at least 300 MB of free disk space. It works with the following operating systems:

Operating System	Minimum System Memory (RAM)
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1 or newer	1 GB (32-bit), 2 GB (64-bit)
Windows 2008 R2	2 GB (64-bit)
Windows 7	1 GB (32-bit), 2 GB (64-bit)
Windows 2012 (Including R2)	2 GB (64-bit)
Windows 8	1 GB (32-bit), 2 GB (64-bit)
Windows 8.1	1 GB (32-bit), 2 GB (64-bit)
Windows 10	1 GB (32-bit), 2 GB (64-bit)

Hardware Appliance Specifications

Endpoint Security currently requires a hardware appliance for communication and threat intelligence. An appliance, as specified below, supports up to 100k endpoints.

Specification	HX 4402/HX 4400D
Storage Capacity	4x 1.8 TB 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
Power Consumption Maximum (watts)	313 watts
MTBF (h)	35,200 h
Appliance Alone	32 lb. (15 kg)

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com