ENDPOINT SECURITY

ON-PREMISE OR REMOTE ENDPOINT DEFENSE AGAINST UNKNOWN THREATS AND EXPLOITS

OVERVIEW

Today's skilled attackers bypass the traditional endpoint defenses (firewalls, antivirus software) that most security teams have relied on for years. Even when a traditional defense stops a known threat, it can't determine what that threat was trying to do. FireEye Endpoint Security (HX series) can be deployed on premise for endpoints inside and outside the corporate network. It helps your security team detect, contain and understand the nature and purpose of known and unknown threats using features such as:

- Triage Viewer and Audit Viewer to inspect and analyze threat indicators
- Enterprise Security Search to rapidly search for, find and contain threats
- Data Acquisition for in-depth endpoint inspection and analysis
- Exploit Guard to detect and alert on endpoint exploit processes

With FireEye Endpoint Security organizations can proactively inspect, analyze and contain known and unknown threats on any endpoint.

Extend threat intelligence to every endpoint

To be effective, threat intelligence must be present at the point of attack. HX Endpoint Detection and Response (EDR) 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 can be inspected for IOCs.

Attain enhanced endpoint visibility

Visibility is critical to identifying the root cause of an alert and conducting deep analyses of a threat. The lookback cache in Endpoint Security allows you to inspect and analyze present and past alerts at the endpoint. Triage Viewer also allows you to automatically build a timeline of events for forensic analysis.

HIGHLIGHTS

- Deploy Endpoint Security via on premise appliances with endpoint agent software to monitor corporate and remote endpoints
- Extend protection against advanced threats with FireEye Dynamic Threat Intelligence (DTI) from the core network to endpoints
- Conduct detailed endpoint investigation and create timelines to identify and contain IOCs
- Search for, detect, identify and contain threats on tens of thousands of endpoints (connected or not) in minutes
- Easily assess all endpoint activities from a single interface to identify exploits to analyze and make containment or response decisions
- Comply with both Common Criteria and FIPS government standards
- Centralize host-based workflows with a single location for current alerts, system details and acquisitions
- Respond rapidly to known and unknown threats with critical contextual information
- Protect all endpoints whether on- or off-premise, outside the network or behind network address translation (NAT)
- Contain threats and compromised devices with a single click while still allowing remote investigation
- Enhance workflow with Audit Viewer for complete threat analysis within Endpoint Security
- Customize Endpoint Security capabilities to address unique characteristics of an incident
- Support multiple DMZ deployments

FireEye
SECURITY REIMAGINED

Get complete endpoint coverage

On-site and remote endpoints outside the corporate network can be vulnerable to attack. Endpoint Security covers all endpoints, pushing intelligence 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.

Detect hidden endpoint exploit processes

When it comes to exploit detection, traditional endpoint protection (EPP) capabilities are limited by comparing signatures to a database. FireEye Endpoint Security provides flexible, data-driven exploit intelligence via a feature called Exploit Guard. This feature delivers Endpoint Detection and Response (EDR) capabilities and gathers detailed information on areas traditional endpoint solutions miss. It uses detailed FireEye-exclusive intelligence to correlate multiple discrete activities and uncover exploits.

How endpoint security works

Endpoint Security can search for and investigate known and unknown threats on tens of thousands of endpoints in minutes. It uses Dynamic Threat Intelligence to correlate alerts generated by FireEye endpoint and network security products and log management.

After validating a threat, you can determine:

- Which vectors an attack used to infiltrate an endpoint
- Whether an attack occurred (and persists) on a specific endpoint
- If lateral spread occurred and to which endpoints
- How long an endpoint(s) has been compromised
- If intellectual property has been exfiltrated
- Which endpoints and systems to contain to prevent further compromise

ENDPOINT SECURITY REQUIREMENTS

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 (Including 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)

Note: 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

HARDWARE APPLIANCE SPECIFICATIONS

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)

Note: The hardware deployment option for Endpoint Security uses a single appliance for communication and threat intelligence that supports up to 100,000 endpoints.

Connecting network-level alerts to endpoint threats

Read how FireEye Endpoint Security works with other FireEye deployments to equip security teams to provide more accurate decisions about potential security incidents.

For more information on FireEye, visit:
www.FireEye.com

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

www.FireEye.com

FireEye