ENDPOINT SECURITY

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

Today's skilled attackers bypass traditional endpoint protection platforms (EPP) because those EPPs focus on single elements to identify threats. By integrating AV and anti-malware protection, threat intelligence, behavior analysis and endpoint detection and response (EDR) capabilities, FireEye Endpoint Security offers a far more robust EPP option to detect and prevent multiple threat characteristics. It enables more security automation while enabling active inspection and analysis to find and eliminate suspicious activity. Its capabilities include:

- Triage Viewer and Audit Viewer to inspect and analyze threat indicators
- Enterprise Security Search to rapidly search for, find and determine actions of suspicious activity and threats
- Data Acquisition for in-depth endpoint inspection and analysis
- Exploit Guard to detect, alert on and prevent attacks that try to exploit endpoints and applications

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

Detect and prevent hidden endpoint exploit processes

When it comes to exploit detection, traditional EPP capabilities are limited because exploits don't conform to a simple signature or pattern. FireEye Endpoint Security provides a flexible, data-driven exploit behavioral intelligence via a feature called Exploit Guard. This feature also delivers EDR by gathering detailed information on areas traditional endpoint solutions miss. It uses detailed FireEye-exclusive intelligence to correlate multiple discrete activities and uncover exploits.

Extend threat intelligence to every endpoint

To be effective, threat intelligence must be present at the point of attack. The EDR capabilities offered by Endpoint Security seamlessly extend 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 analyst can quickly inspect and gather details with Triage and Audit Viewer on every endpoint for IOCs.

Attain enhanced endpoint visibility

Complete endpoint visibility is critical to identifying the root cause of an alert and conducting deep analyses of a threat to determine its threat state. The lookback cache in Endpoint Security allows you to inspect and analyze present and past alerts at any endpoint for thorough forensic investigation and the best response.

HIGHLIGHTS

- Deploys as on-premise appliances and endpoint agent software to detect and prevent exploits and monitor activity on remote and networked endpoints enabling rapid response to known and unknown threats
- Offers new AV (detection only until Q3) capability integrated with Advanced Threat Intelligence and endpoint behavioral analysis in a single endpoint agent
- Helps conduct detailed endpoint investigation with cohesive activity timelines within a single workflow to identify and contain IOCs
- Searches for, detect, identify and contain threats on tens of thousands of endpoints (connected or not) in minutes
- Easily assesses all endpoint activities with Triage and Audit Viewer within a single interface to identify and stop incidents for analysis with a single click for containment for more timely response decisions

FireEye

Get complete endpoint coverage

Onsite and remote endpoints outside the corporate network can be more vulnerable to attack. Endpoint Security covers all endpoints, pushing intelligence to them regardless of their Internet connection type. This enables you to detect and prevent threats, as well as 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 with a single click to stop an attack and prevent it from spreading laterally or becoming a greater threat in some other way. You can then conduct a complete forensic investigation of the incident without risking further infection.

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 FireEye Dynamic Threat Intelligence to correlate alerts generated by FireEye and network security products and security logs to validate a threat and 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

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 (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)
Windows Server 2016	2GB
Mac OS 10.9+	1GB

Hardware appliance specifications

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

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

ABOUT FIREEYE, INC.

FireEye is the leader in intelligence-led security-as-a-service. 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 has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

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

www.FireEye.com

FireEye