FireEye Endpoint Security

Comprehensive single-agent security solution to protect on-premise and remote endpoints against known and unknown threats

OVERVIEW

Traditional endpoint protection leaves gaps as it tries to address modern threats. FireEye Endpoint Security improves security visibility and the quality and relevance of your threat data to address these gaps and give you:

- Fully integrated malware protection (antivirus (AV) defenses), remediation, behavior analysis, intelligence and endpoint visibility
- Triage and Audit Viewer to conduct exhaustive inspection and analysis of threat indicators with integrated
- Enterprise Security Search to rapidly find and illuminate intention of suspicious activity or threat
- Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over specific time frame
- Exploit Guard to detect, alert, and prevent attacks attempting to misuse or exploit applications

The combination of endpoint detection and response (EDR) and other capabilities into a single integrated FireEye solution gives analysts the fastest possible way to inspect, search and analyze any suspicious activity on any endpoint enabling them to adapt a defense based on detailed threat information in real time.

Detect and prevent hidden endpoint exploit processes

When it comes to exploit detection and prevention, traditional endpoint protection 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 works with Endpoint Detection and Response (EDR) with detailed information traditional endpoint solutions miss with FireEye-exclusive intelligence to correlate multiple discrete activities to uncover exploit activity.

Extend threat intelligence to every endpoint

To be effective, threat intelligence must be present at the point of attack. The endpoint detection and response (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

- Available to deploy in on-premise, cloud or virtual environments along with endpoint agent to detect, prevent and monitor local or remote endpoint activities
- Fully integrated inspection and analysis workflow with a single endpoint agent that includes threat intelligence, behavioral analysis and malware detection, prevention and remediation
- Allows detailed endpoint investigation with complete activity timelines within a single workflow so staff can quickly identify and contain IOCs and other threats or suspicious activities
- Search for, identify and contain threats on tens of thousands of endpoints (connected or not) in minutes
- Single interface to easily assess all endpoint activities, identify and analyze incidents and contain them with a single click to eliminate risk of infection

FireEye

Get complete endpoint coverage with malware protection

Provides integrated protection to onsite and remote endpoints with a tamper proof agent as well as on-access scanning (real-time) of all file types using signatures, heuristics, generic detection and emulation (sandbox) and on-demand (scheduled) scans for full, quick memory and MBF scanning.

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 and take remediation action based on detailed investigation and analysis of threat action.

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:

- Identify and detail vectors an attack used to infiltrate an endpoint
- Determine whether an attack occurred (and persists) on a specific endpoint
- Ascertain whether lateral spread occurred and to which endpoints
- Establish time line and how long an endpoint(s) has been compromised
- Follow the incident to identify whether and what intellectual property may have been exfiltrated
- Clearly identify which endpoints and systems need containment 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:

Table 1. 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)
Windows Server 2016	2GB
Mac OX 10.9+	1GB
Red Hat Enterprise Linux (RHEL) 6.8, 7.2, 7.3	2GB

Deployment Options

Endpoint Security can be deployed through the cloud or as a virtual or on-premise hardware appliance (listed below) that protects up to 100,000 endpoints. The HX4502 can be used for either core or DMZ deployment — the only difference is the license state of each device; the hardware is identical.

Table 2. Deployment Options

SPECIFICATION	HX 4502	HX 4502D
Storage Capacity	4x 4TB HDD RAID10 8TB Effective	4x 4TB HDD RAID10 8TB Effective
Enclosure	1RU, Fits 19-inch Rack	1RU, Fits 19-inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)
CPU	1 Intel E3-1240 4-Core 3.5GHz	1 Intel E3-1240 4-Core 3.5GHz
Memory	64GB	64GB
NIC	2x 1GigE, 2x 1GigE (MB)	2x 1GigE, 2x 1GigE (MB)

Table 3. Endpoint Security virtual appliance

COMPONENT	HX2500V (D)	HX2502V	HX4500V (D)	HX4502V
CPU	4 cores	4 cores	8 cores	8 cores
Memory	16 GB RAM	16 GB RAM	64 GB RAM	64 GB RAM
Disk	512 GB Disk	1200 GB Disk	1200 Disc	3600 GB Disk
Virtual NICs	2 vmxnet3 interfaces	2 vmxnet3 interfaces	2 vmxnet3 interfaces	2 vmxnet3 interfaces
Max Endpoints Supported	15,000	15,000	100,000	100,000

Note: The features of Endpoint Security virtual appliances are detailed below.

Virtual appliance requirements

Endpoint Security virtual appliances require the following VMware resources:

- VMware ESXi host version 6.0 or later. Earlier ESXi versions are not supported
- VMware vSphere Client
- VMware VCenter Server (recommended). When you use vSphere Client to add virtual appliances to vCenter Server, the Deploy OVG Template wizard provides an easy way to enter your activation code. Otherwise, you must type it in the virtual appliance console, because you cannot paste into this console.
- VMXNET 3 network drivers
- Standard virtual switch created for the monitoring ports of the virtual appliances, and attached to a physical network adapter on the ESXi server.

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

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

www.FireEye.com

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