



## DATA SHEET

# FireEye Endpoint Security

Stop attacks with knowledge from  
frontline responses



### HIGHLIGHTS

- Prevent the majority of cyber attacks against the endpoints of an environment
- Detect and block breaches that occur to reduce the impact of a breach
- Improve productivity and efficiency by uncovering threats rather than chasing alerts
- Use a single, small-footprint agent for minimal end-user impact
- Protections and functionality through downloadable modules
- Comply with regulations, such as PCI-DSS and HIPAA
- Deploy to onsite or in the cloud

Traditional endpoint security is not effective against modern threats; it was never designed to deal with sophisticated or advanced persistent threat (APT) attacks. To keep endpoints safe, a solution must quickly see the threat and respond with the most effective technology.

FireEye Endpoint Security combines the best of legacy security products, enhanced with FireEye technology, expertise and intelligence to defend against today's cyber attacks. Based on a defense in depth model, Endpoint Security uses a modular architecture with default engines and downloadable modules to protect, detect and respond and manage agents.

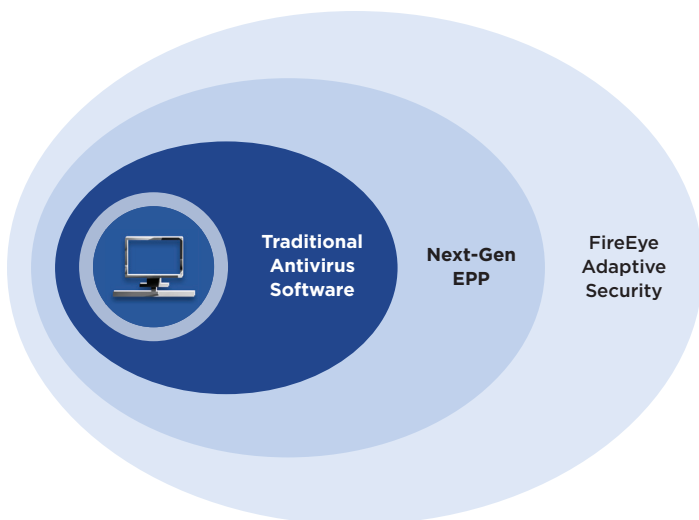
To prevent common malware, Endpoint Security uses a signature-based endpoint protection platform (EPP) engine. To find threats for which a signature does not yet exist, MalwareGuard uses machine learning seeded with knowledge from the frontlines of cyber attacks. To deal with advanced threats, endpoint detection and response (EDR) capabilities are enabled through a behavior-based analytics engine. A real-time indicators of compromise (IOC) engine relies on current, frontline intelligence to help find hidden threats. To add new engines and features, you can download modules from the FireEye Market.

Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, Endpoint Security provides tools to:

- Search for and investigate known and unknown threats on tens of thousands of endpoints in minutes
- Identify and detail vectors an attack used to infiltrate an endpoint
- Determine whether an attack occurred (and persists) on a specific endpoint and where it spread
- Establish timeline and duration of endpoint compromises and follow the incident
- Clearly identify which endpoints and systems need containment to prevent further compromise

IT is a strategic enabler that drives our ability to effectively educate our students. Utilizing FireEye Endpoint Security ensures that our IT assets are available, highly functioning, and secure, which is critical to achieving our mission.

— James D. Perry II  
Chief Information Security Officer, University of South Carolina



**Primary Features**

- Single agent using defense in depth to minimize configuration and maximize detection and blocking
- Single integrated workflow to analyze and respond to threats within Endpoint Security
- Fully integrated malware protection with antivirus (AV) defenses, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility
- Triage Summary and Audit Viewer for exhaustive inspection and analysis of threats

**Additional Features**

- Enterprise Security Search to rapidly find and illuminate suspicious activity and threats
- Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific time frame
- End-to-end visibility that allows security teams to rapidly search for, identify and discern the level of threats
- Detection and response capabilities to quickly detect, investigate and contain endpoints to expedite response
- Easy-to-understand interface for fast interpretation and response to any suspicious endpoint activity

Often, management thinks any virus is almost the end of the world. With FireEye, I can bring real evidence to display about the nature of the issue and that we've been able to manage and contain it. Making all of those unknowns known quickly helps to take the pressure down for everybody in the organization.

— **Michael Hennessy**, Director Technology Services  
Alpha Grainer Manufacturing, Inc

**Supported Operating Systems and Environments**

<b>Windows</b>	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
<b>Mac</b>	OS X 10.9+
<b>Linux</b>	RedHat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 & 7.6

**Deployment options:** onsite physical appliance, onsite virtual appliance, FireEye Cloud Service



To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

**FireEye, Inc.**

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

©2020 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. EP-EXT-DS-US-EN-000018-05

**About FireEye, Inc.**

FireEye is the intelligence-led security company. 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.

