DATA SHEET

FireEye Endpoint Security

Engage multiple defense engines with a single agent

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
- 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 analyze and respond to such threats.

FireEye Endpoint Security combines the best of legacy security products, enhanced with FireEye technology, expertise and intelligence to defend against today's cyber attacks. FireEye uses four engines in Endpoint Security to prevent, detect and respond to a threat.

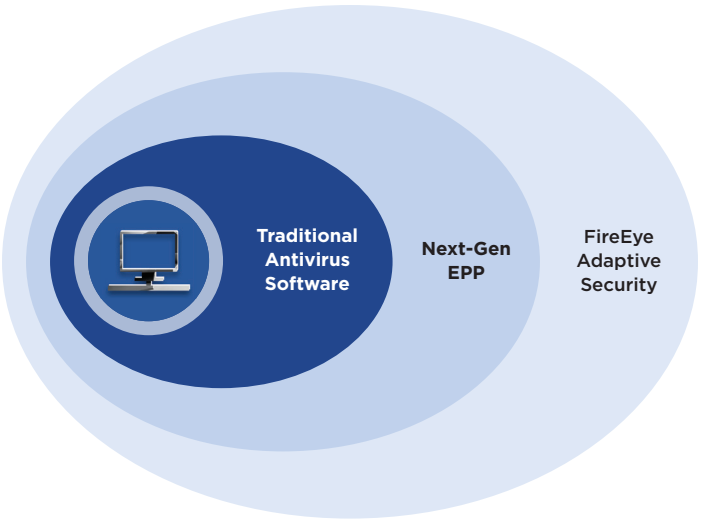
To prevent common malware, Endpoint Security uses a signature based endpoint protection platform (EPP) engine. To find threats for which a signature does not yet exist, MalwareGuard uses machine learning seeded with knowledge from the frontlines of cyber attacks. To deal with advanced threats, endpoint detection and response (EDR) capabilities are enabled through a behavior-based analytics engine. Finally, a real-time indicators of compromise (IOC) engine that relies on current, frontline intelligence helps find hidden threats. This defense in depth strategy helps protect vital information stored on customer endpoints.

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



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

Primary Features

- Single agent with three detection engines 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

Supported Operating Systems and Environments	
Windows	XP SP3, 2003 SP2, Vista SP1 and up, 2008, Win7, 2012, 8, 8.1, 10, Server 2016
Mac	OS X 10.9+
Linux	Red Hat Enterprise Linux 6.8+, 7.2 + CentOS 6.9+, 7.4+

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

ICSA labs CERTIFIED ANTI-VIRUS

vb 100 VIRUS virusbtn.com

To learn more about FireEye, visit: **www.FireEye.com**

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

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.

FIREEYE™