DATA SHEET

FireEye Endpoint Security

Stop attacks with knowledge from frontline responses

HIGHLIGHTS

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

Every day brings a new cyber attack, a new vulnerability or a new ransomware target. Security teams find it increasingly difficult to keep up with the threats to their users, company data and intellectual property and don't always bring in extra help. Responders are burdened with too many tools that do not work together and create more noise than useful signals. Systems in place do not always provide adequate detection and response of these advanced threats.

FireEye Endpoint Security defends against today's cyber attacks by enhancing the best parts of legacy security products with FireEye technology, expertise and intelligence. Using a defense-in-depth model, the modular architecture of Endpoint Security unites default engines and downloadable modules to protect, detect and respond, and manage endpoint security.

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. For attacks on exploits in common software and browsers, ExploitGuard uses a behavioral analysis engine that determines if an exploit is being used and stops it from executing. In addition, FireEye continuously creates modules to detect against attack techniques and accelerate responses to emerging threats. For example, Process Guard was developed to stop credential exfiltration.

> 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

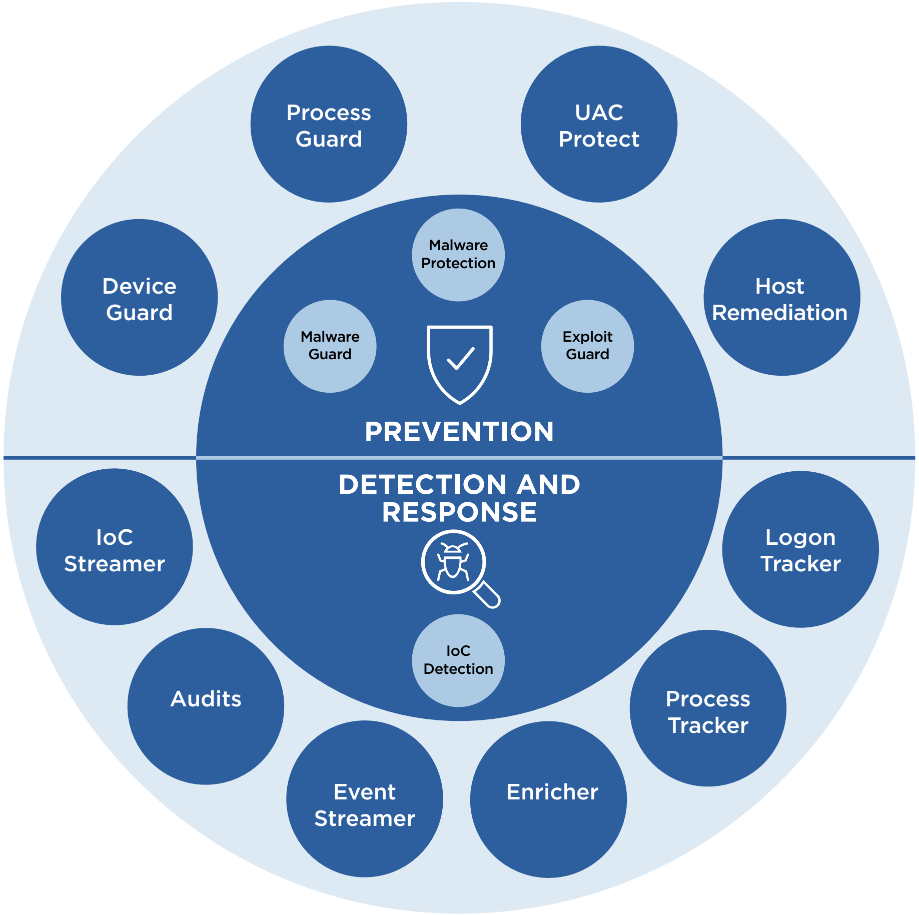
Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, Endpoint Security includes endpoint detection and response (EDR) capabilities that rely on real-time indicators of compromise (IOCs) developed with help from frontline responders. FireEye tools also:

- Search for and investigate known and unknown threats on tens of thousands of endpoints in minutes
- Identify and detail the 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

Modern threats do not stop at one endpoint, so remediating on a single endpoint will not solve most breaches. Full remediation efficiently communicates and points to all devices where a threat may be hiding and correlates this information in real time. Endpoint Security is a component of FireEye XDR, which seamlessly connects all FireEye technologies and services to detect and respond to all the most sophisticated threats.

Figure 1.

FireEye Endpoint Security core engines (center) and available modules (outer ring).



> 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 using defense in depth to minimize configuration and maximize detection and blocking
- Integrated workflow to analyze and respond to threats within Endpoint Security
- Malware protection with antivirus (AV) defenses, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility
- Component of FireEye XDR to fully remediate all threats in an organization

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	Windows 7, 8, 8.1, 10, 11 Server 2008R2, 2012R2, 2016, 2019, 2022
Mac	10.9 - 10.15, 11, 12
Linux	RHEL 6.8 - 6.10, 7.2 - 7.9, 8.0 - 8.3 CentOS 6.8 - 6.10, 7.2 - 7.7, 8.0 SUSE 11 SP3, SP4, 12 SP2 - SP5, 15 GA Open SUSE Leap 15.1, 15.2 Ubuntu 14.04, 16.04, 18.04, 19.04, 20.04 LTS Amazon Linux AMI 2018.3, AM2, Amazon Linux 2 Oracle Linux 6.10, 7.6, 8.1, 8.2

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

FireEye Endpoint Security is part of FireEye XDR
Learn more at **www.FireEye.com/XDR**

FireEye, Inc.
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

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 to eliminate the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.