Trellix

DATA SHEET

Trellix Endpoint Security (HX)

Stop attacks with knowledge from front-line responses

Every day brings a new cyberattack, 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.

Trellix Endpoint Security (HX) defends against today's cyberattacks by using a defense-in-depth model. The modular architecture of Endpoint Security (HX) unites default engines and downloadable modules to protect, detect and respond, and manage endpoint security.

Highlights

- Prevent the majority of cyberattacks 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

To prevent common malware, Endpoint Security (HX) 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 cyberattacks. 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, Trellix continuously develops modules to detect against attack techniques and accelerate responses to emerging threats. For example, Process Guard was developed to stop credential exfiltration.

Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, Endpoint Security (HX) includes Endpoint Detection and Response capabilities that rely on real-time indicators of compromise (IOCs) developed with help from front-line responders. Trellix 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

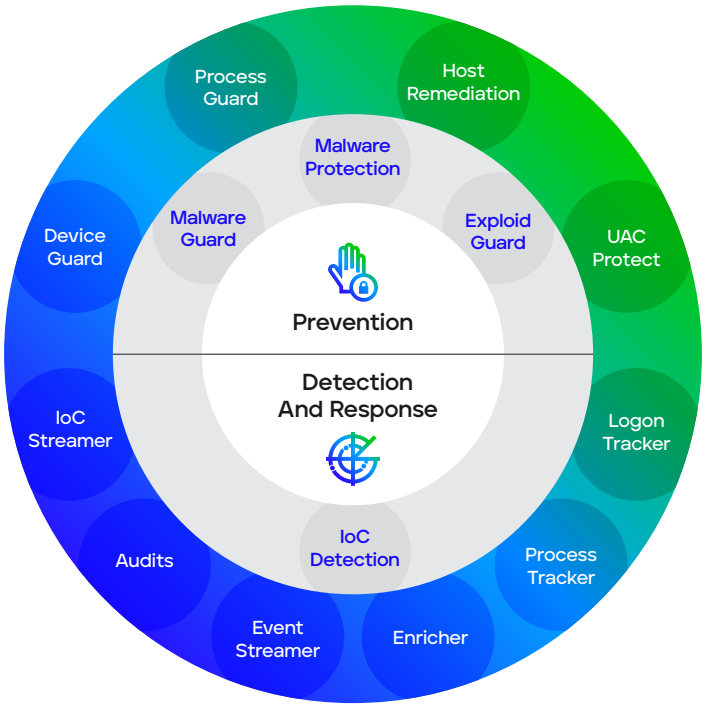

Figure 1: Trellix Endpoint Security (HX) core engines (center) and available modules (outer ring).

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 (HX) natively integrates with Trellix XDR, which seamlessly connects all Trellix technologies and services to detect and respond to all the most sophisticated threats.

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 (HX)
- Malware protection with anti-malware protection, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility
- Natively integrates with Trellix XDR for more visibility and control to fully remediate all threats in an organization

Additional Features

- Enterprise Search to rapidly find and illuminate suspicious activity and threats
- Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific timeframe
- 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
Mac	10.9 - 10.15, 11, 12, 13
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: physical appliance, virtual appliance, cloud-hosted appliance.

Visit Trellix.com to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.