Trellix

DATA SHEET

Trellix® Endpoint Forensics (HX)

Highlights

- Collect forensics data from thousands of endpoints in minutes
- Detect and block breaches to reduce their impact
- Improve productivity and efficiency by uncovering threats rather than chasing alerts
- Use a single, lightweight agent for minimal performance impact
- Gain added protections and functionality through downloadable modules
- Comply with regulations including GDPR, PCI-DSS, and HIPAA
- Deploy onsite or in the cloud

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 Forensics (HX) provides a modular architecture that unifies multiple engines and downloadable modules to protect, detect, investigate, and respond to threats, and collect salient forensics data to accurately scope an incident.

Trellix Endpoint Forensics provides a signature based engine to prevent malware. To find threats for which a signature does not yet exist, Endpoint Forensics uses machine learning built off knowledge from thousands of incident response engagements. For attacks on exploits in common software and browsers, a behavioral analysis engine determines if an exploit is being used and stops it from executing. In addition, Trellix continuously develops methods to defend against attack techniques and accelerate responses to emerging threats. For example, we developed a mechanism to see and stop credential exfiltration.

Trellix Endpoint Forensics provides a signature based engine to prevent malware. To find threats for which a signature does not yet exist, Endpoint Forensics uses machine learning built off knowledge from thousands of incident response engagements. For attacks on exploits in common software and browsers, a behavioral analysis engine determines if an exploit is being used and stops it from executing. In addition, Trellix continuously develops methods to defend against attack techniques and accelerate responses to emerging threats. For example, we developed a mechanism to see and stop credential exfiltration.

Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, Endpoint Forensics 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 scope the potential spread
- Establish timeline and duration of endpoint compromises and follow the incident

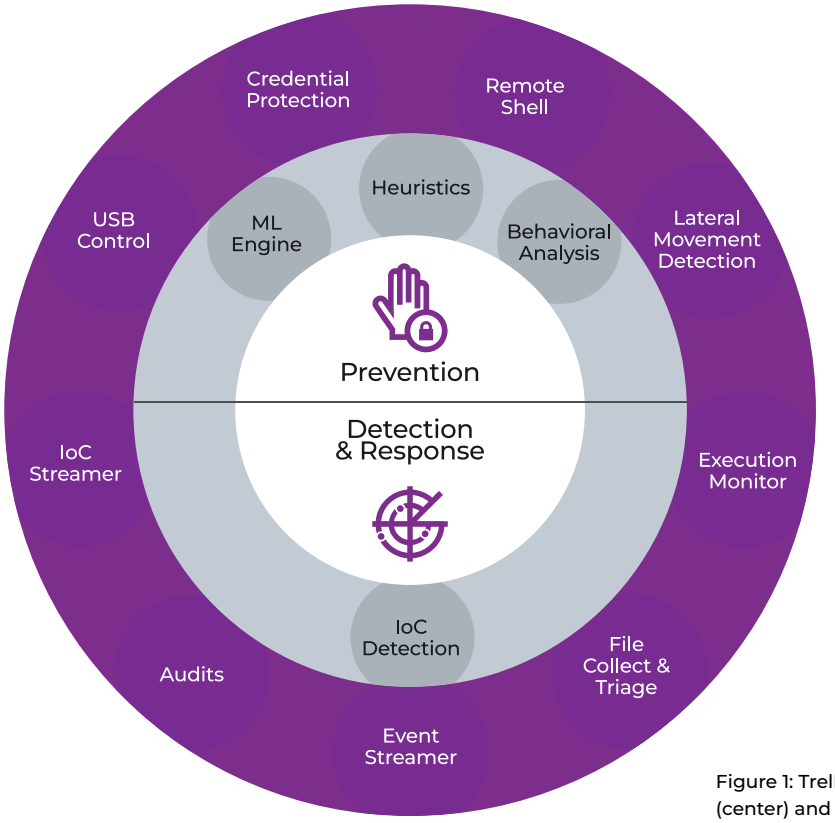

Figure 1: Trellix Endpoint Forensics core engines (center) and available modules (outer ring).

Modern threats do not stop at one endpoint, and reimaging a single endpoint rarely contains the breach. Full remediation efficiently communicates and points to all devices where a threat may be hiding and correlates this information in real time. Endpoint Forensics natively integrates with the rest of the Trellix Security Platform, which seamlessly connects all Trellix technologies and services to detect and respond to all the most sophisticated threats.

Primary Features

- Lightweight agent that stops threats and collects forensic data from endpoints on demand
- Malware protection using machine learning, behavior analysis, indicators of compromise (IoCs), and unparalleled visibility
- Integrated workflow to detect, investigate, analyze, and remediate threats
- Natively integrates with the Trellix Security Platform to gain complete visibility of threat activity across hybrid environments including air-gapped networks

Additional Features

- Easily discover and investigate suspicious activity with Enterprise Search
- Use rapid data acquisition to conduct in-depth endpoint analysis over a specific timeframe
- Gain end-to-end visibility that allows security teams to quickly search for, identify and discern the level of threats
- Quickly detect, investigate and triage endpoints using detection and response capabilities
- Leverage an 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.