Trellix

Trellix Endpoint Security (HX)

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.

Endpoint Security can be deployed as an on-premise hardware appliance that protects up to **100,000 endpoints**, a virtual appliance, or through a cloud instance.

Prevent cyber-attacks on the endpoint

- Identify attacker behavior and their tactics, techniques, and procedures.
- Analyze live memory—without downloading memory images—to discover hidden malware.

Detect malware and other signs of compromise on endpoints

- Sweep thousands of endpoints for evidence of compromise, including malware and irregular activities.
- Collect targeted forensic data with intelligent filtering to return only the data you need.
- Enable remote investigation securely over any network, without requiring access authorization.

Trellix Endpoint Security (HX)

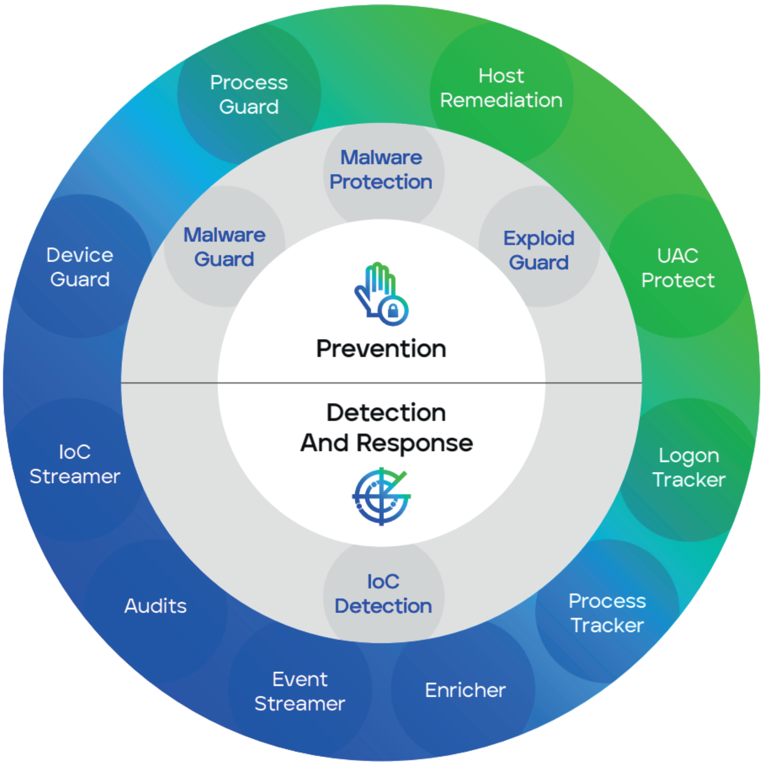
Respond to endpoint security incidents faster

- Provides the ability to remotely connect to endpoints command shell to analyze and remediate threats.
- Integrate with other detection systems to automate triage of hosts with suspicious activity.
- Automatically collect data and analyze suspicious activity based on alerts generated by your SIEM, ticketing system or other applications.
- Support open IOCs to allow security analysts to edit and share custom IOCs.

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.
- Determine whether an attack occurred (and persists) on a specific endpoint and where it spread.
- Identify and detail the vectors an attack used to infiltrate an endpoint.
- Establish timeline and duration of endpoint compromises and follow the incident.



Trellix Endpoint Security (HX)

Features

- Single agent using defense in depth to minimize configuration and maximize detection and blocking.
- Natively integrates with Trellix XDR for more visibility and control to fully remediate all threats in an organization.
- Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific timeframe.
- Malware protection with anti-malware protection, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility.
- Enterprise Search to rapidly find and illuminate suspicious activity and threats.
- End-to-end visibility that allows security teams to rapidly search for, identify and discern the level of threats.

CONTACTS:

trellix@bakotech.com

trellix.bakotech.com

Trellix | bako tech®

WE BRING SECURITY TO LIFE