Trellix

SOLUTION BRIEF

Trellix® Endpoint Security Suite

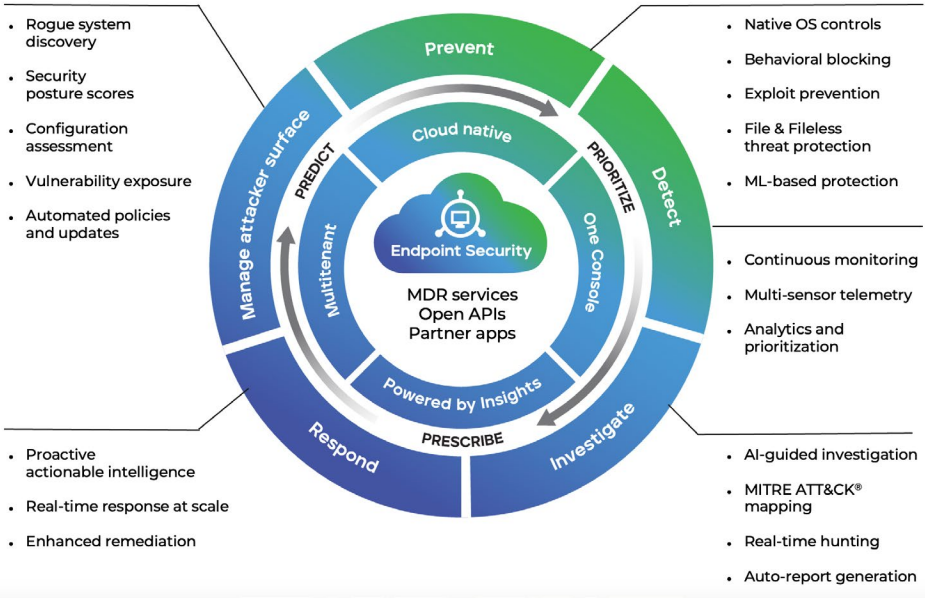
From detection to defense: Unmatched accuracy and comprehensive breach prevention

The Trellix Endpoint Security Suite is a comprehensive and unified set of solutions that protects devices and endpoints across your hybrid network, empowering your organization to address complex, distributed security issues thoroughly, efficiently, and quickly. It uses analytics and machine learning to achieve industry-leading threat protection, all while offering the flexibility to connect to products from other vendors. The solution helps you unify your data and threat defenses from device to cloud, for integrated security.

As Trellix® unifies threat protection, detection, and response from device to cloud, we are building a future where security is an integrated system—simpler, smarter, and broader than anything that's ever come before. The Trellix Endpoint Security Suite learns and evolves to protect your changing business needs in a dynamic threat landscape.

The Trellix Endpoint Security Suite includes Trellix Endpoint Security and Trellix Endpoint Detection and Response with Forensics and Trellix Wise™.

Future-proof your defenses with intelligence-driven endpoint security, threat detection, and response



Prevent, detect, investigate, and respond to threats while efficiently managing your attack surface. We help you predict, prioritize, and prescribe your most effective threat response leveraging AI, the most comprehensive threat research and intelligence, and simple-to-use forensic capabilities. In addition, we provide managed detection and response (MDR) services for more resource-constrained organizations.

Support your remote workforce with industry-leading endpoint security and a unified defense, along with comprehensive, proactive threat intelligence and defenses across the entire attack lifecycle.

Trellix Endpoint Security Suite is a comprehensive threat protection, detection, investigation, and response for your devices that uses analytics and artificial intelligence to secure your organization's hybrid environment—including the flexibility to connect to security products from other vendors.

Get adaptive, proactive defenses with AI-driven integrated endpoint protection, detection, and forensics

Comprehensive endpoint protection from advanced threats

Gain visibility and control of all your endpoints with robust threat prevention, detection, investigation, and response:

- Protect against emerging and advanced threats, including ransomware, while securing your remote workforce with powerful threat detection and response
- Go deeper to unearth hidden threats and comprehensively eradicate the full the scope of the attack

Simplify investigations, improve analyst productivity, and save time with Trellix Wise investigations

“In our environment, the Trellix integrated ecosystem replaced seven different security tools and six vendors’ management consoles. The difference in ease of management was night versus day.”

— M.T., information security analyst at a major American convenience store chain

Simplified management with a centralized console

Easily scale and manage hundreds of thousands of endpoints to:

- Streamline and accelerate your security effectiveness while easily protecting hundreds of thousands of endpoints and eliminating security gaps
- Enforce and manage security from a single view and access automated workflows from anywhere

Proactive risk management to stay ahead of adversaries

Use our solution capabilities to help protect your organization, so you can:

- Reduce and manage your attack surface to preempt attacks
- Proactively prioritize threats with advance knowledge of those targeting your industry or geographic location
- Easily support customized detections to reduce noise and false positives
- Use predictive security assessments and proactively prescribe security actions

Complete and proactive endpoint protection

Prevent security breaches with multi-layered protections

Uncover and protect against fileless and script-based attacks while defending against ransomware, greyware, and credential theft attacks with enhanced remediation and dynamic application containment technologies.

Get actionable threat intelligence with machine-learning to detect zero-day threats in near real time.

Quickly detect advanced and emerging threats

Simplify detection and response for sophisticated advanced persistent threats (APTs) with endpoint detection and response (EDR) with deep forensics and with Trellix Wise AI. Trellix Wise automatically identifies related breaches, identifies key artifacts, explains why artifacts are important and/or suspicious, and automatically maps to MITRE ATT&CK.

Trellix EDR with Forensics and Trellix Wise eliminates manual work by generating a summary email and executive report with just a single click.

Use automation and AI to accelerate threat investigations

Cut through alert noise and enable analysts to focus on high-priority alerts with AI-guided investigations and alert triage.

This provides a set of questions and responses based on the MITRE associated attack patterns to maximize the resources, and minimize mean time to response (MTTR) of a threat.

Respond to threats with confidence and speed

With the Trellix Endpoint Security Suite you get proactive protection across endpoints to contain and stop threats in real time at scale. Our enhanced remediation capabilities save you valuable time otherwise spent reimaging systems. Enable junior analysts to be more effective through simplified and context-driven user experience, thereby accelerating detection and investigation efforts.

Manage your attack surface with unparalleled threat intelligence

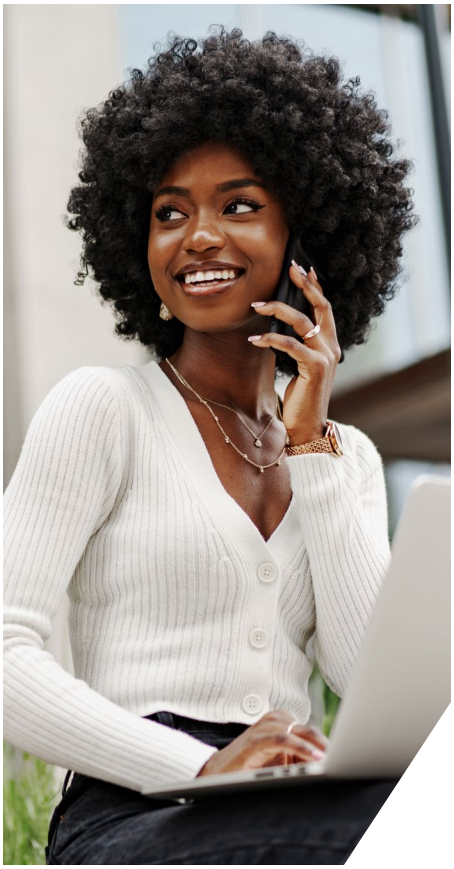
Use Trellix Insights* to intelligently preempt attacks with proactive threat prioritization, predictive assessments of your security posture, and preemptive security action prescriptions. Trellix Insights delivers prioritized risk intelligence on which threats and campaigns are most likely to target your organization, while Trellix Global Threat Intelligence enhances your situational awareness and helps you accurately understand the constantly changing risk landscape.

Orchestrate with a cloud-delivered, unified platform

Easily scale across hundreds of thousands of endpoints to meet business needs and remove security gaps. You can automate security and compliance workflows and accelerate responses with real-time sharing and trigger actions. When business needs require it, you can gain a unified view across all your security needs by extending protection across endpoints, network, and cloud.

Gain access to an extensive partner ecosystem for a unified defense

We collaborate with leading software vendors to improve security outcomes for our customers. Our open platform helps you integrate your existing security solutions easily. You also get fewer management consoles for a more streamlined, automated experience.



Trellix Endpoint Security Suite components

Trellix Endpoint Security (ENS)

The endpoint solution you depend on should align with the priorities that matter most to you. Regardless of your role, Trellix Endpoint Security aligns to your specific critical needs—from preventing threats and hunting them to tailoring security controls. Use the solution to ensure system uptime for users, find more opportunities for automation, and simplify complex workflows.

Trellix Endpoint Detection and Response with Forensics (EDR with Forensics)

Trellix EDR with Forensics and Trellix Wise AI reduces reduces alert fatigue by automating alert investigation and correlation for analysts of all skill levels. It proactively contextualizes threats to improve productivity and investigate more effectively, while continuously monitoring and gathering data to provide the visibility and context needed to detect and respond to additional threats.

Trellix Endpoint Solution bundles

	Essentials	Core	Enterprise
CAPABILITIES			
ePO On-Prem / IaaS / SaaS	✓	✓	✓
Next Gen AV	✓	✓	✓
Host Firewall	✓	✓	✓
Web & Device Control	✓	✓	✓
Adaptive Threat Protection	✓	✓	✓
Native Security Protection	✓	✓	✓
Trellix Insights		✓	✓
Threat Intelligence Exchange (TIE)		✓	✓
IVX Cloud Submissions		✓	✓
Application Control for PCs		✓	✓
EDR for Critical Assets (5%)		✓	
Trellix EDR + Forensics			✓

* Trellix Insights requires Trellix Endpoint Security telemetry (opt-in) to function properly; if you do not want to provide this telemetry, you should not choose this product, as you won't be able to receive full value.

Request a demo

To learn more, visit trellix.com