Trellix

DATA SHEET

Trellix Endpoint Security (ENS)

Purpose-built security for proactive threat management and proven security controls

Key benefits

- **Advanced defenses for advanced threats:** Machine learning, credential theft defense, and rollback remediation complement Windows desktop and server systems' basic security capabilities.
- **No additional complexity:** Manage Trellix technologies, Windows Defender Antivirus policies, Defender Exploit Guard, and Windows Firewall settings using a single policy and console.
- **Actionable threat intelligence:** Respond immediately to potential active campaigns that are prioritized according to whether they are targeting your sector or geographies with a leading actionable security intelligence solution available today. Trellix Insights will predict which endpoints are lacking protection against the campaigns and offer prescriptive guidance on how to improve the detection. This is the only endpoint security solution to concurrently prioritize, predict, and prescribe actions.

Endpoint security that aligns with your priorities

The endpoint solution you depend on should align with the priorities that matter most to you. Whether you're focused on business continuity and security strategy or in protecting the network and endpoints, Trellix Endpoint Security (ENS) aligns to your specific critical needs—from preventing threats and hunting them to tailoring security controls.

With Trellix ENS and Trellix Insights you can protect your organization before an attack by using specific threat priorities. The solution enables you to ensure system uptime for users, find more opportunities for automation, and simplify complex workflows.

Ensure uptime and visibility

Trellix ENS enables customers to respond to and manage the threat defense lifecycle with proactive defenses and remediation tools. Automatic rollback remediation returns systems to a healthy state to keep users and administrators productive. This saves time that you might otherwise spend waiting for system remediation, performing recovery, or reimaging an infected machine.

Global threat intelligence and real-time local event intelligence are shared between endpoints and Trellix Endpoint Detection and Response (EDR) to collect threat event details, detect and prevent threats attempting to evade detection, and map them to the MITRE ATT&CK framework for further investigation.

Management is simple with a centralized console that comes with a choice of local software as a service or virtual environment deployments. Trellix Insights offers unique visibility and control into potential priority threats with high propensity to attack and determines whether your organization's security posture will protect against the threat. This ensures an advanced level of protection against a critical threat and outmaneuvers the attackers before they strike.

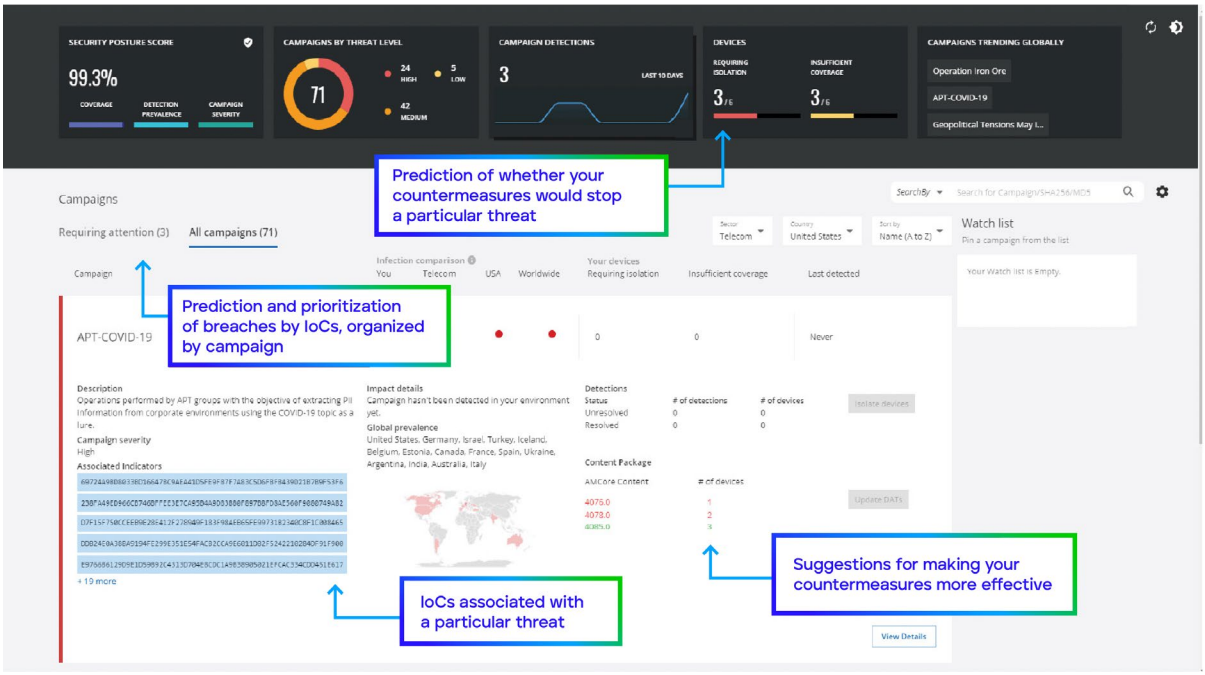

Figure 1. Trellix Insights dashboard (Insights requires Trellix Endpoint Security telemetry (opt-in) to function properly)

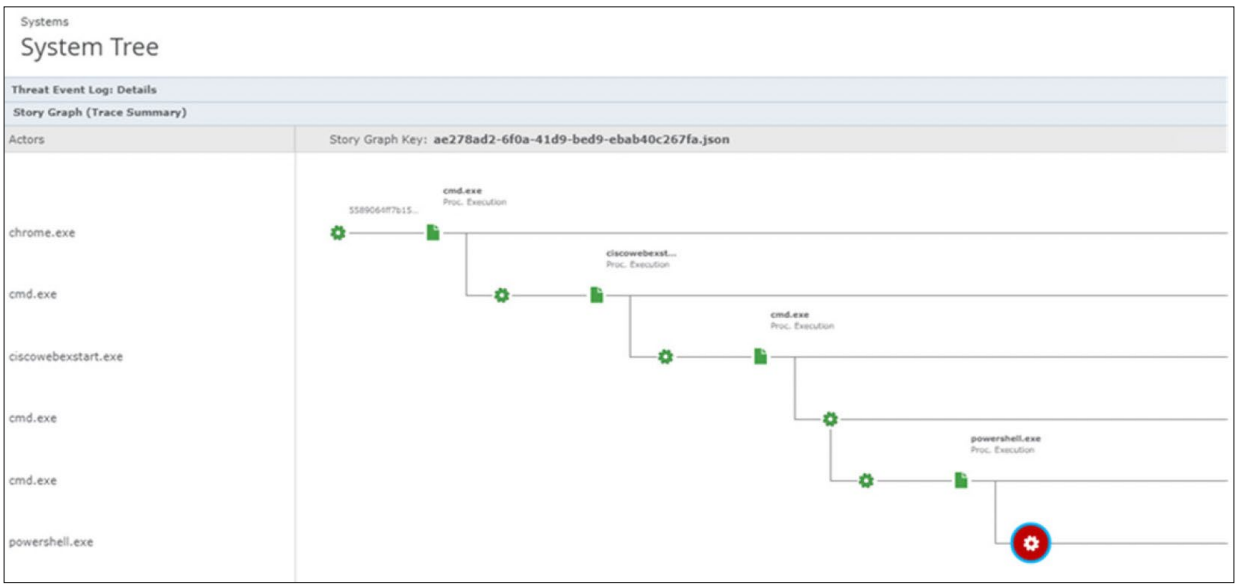

Figure 2. Story Graph

With Trellix Insights, you get alerts and notifications on prioritized potential threats likely to hit based on industry and region. In addition, Insights offers a local assessment of your security posture and whether it can protect against this threat. It also identifies endpoints that are vulnerable to the threat and offers prescriptive guidance on what to update. This increases proactive efforts to get ahead of adversaries who are likely to attack.

Trellix ENS gathers threat insights from multiple layers of engagement using a single software agent to remove redundancies caused by multiple point products. The result is an integrated approach to security that removes manual threat correlation. Threat details that require further investigation are elevated to incident responders automatically. Threat event data is presented in a simple, at-a-glance format via the Story Graph, which visualizes threat details and allows administrators to easily drill down and investigate the sources of malicious actors.

Integrated advanced threat defenses automate and speed response times

Additional advanced threat defenses, like Dynamic Application Containment (DAC), are also available as part of the integrated Trellix Endpoint Security framework. These features help you protect your organization from the latest advanced threats.* For example, DAC will analyze and act against greyware and other emerging malware, containing them to prevent infection.

> To immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state.

Another technology for advanced threat is Real Protect, which uses machine-learning behavior classification to detect zero-day malware and improve detection. The signatureless classification is performed in the cloud and maintains a small client footprint while providing near real-time detection.

Actionable insights are delivered and can be used to create indicators of attack (IoAs) and indicators of compromise (IoCs). This can be particularly useful for lateral movement detection, patient-zero discovery, threat actor attribution, forensic investigations, and remediation. Real Protect also speeds future analysis by automatically evolving behavior classification to identify behaviors and adding rules to identify future attacks that are similar using both static and runtime features.

Lastly, to immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint, following a conviction, to the last known good state.

Intelligent endpoint protection lets you know what attackers are doing now

Better intelligence leads to better results. Trellix Endpoint Security shares its observations in real time with the multiple endpoint defense technologies connected to its framework. This collaboration accelerates identification of suspicious behaviors, facilitates better coordination of defenses, and provides better protection against targeted attacks and zero-day threats. Insights like file hash, source URL, AMSI, and PowerShell event data are tracked and shared, not only with other defenses but also with the client and management interfaces. This helps users understand attacks and provides administrators with actionable threat forensics.

In addition, Trellix Threat Intelligence Exchange technology empowers adaptive defenses to collaborate with other Trellix solutions including gateways, sandboxes, and our security information and event management (SIEM) solution. Gathering and distributing local, community, and global security intelligence shrinks the time between attack discovery and containment from weeks or months to milliseconds.

Combined with Trellix Global Threat Intelligence (Trellix GTI), the Trellix Endpoint Security framework leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time across all vectors—file, web, message, and network. The existing endpoint footprint and management system is enhanced with localized and global threat intelligence to combat unknown and targeted malware instantly. Automatic actions against suspicious applications and processes quickly escalate responses against new and emerging forms of attack while informing other defenses and the global community.

Customers using DAC and Real Protect get insights into more advanced threats and the behaviors they exhibit. For example, DAC provides information on contained applications and the type of access that they attempt to gain, such as registry or memory.

For organizations interested in collecting endpoint related threat insights to hunt malware and equip incident responders, Real Protect provides insights into behaviors that have been deemed malicious and classifies threats. These insights can be particularly helpful in uncovering file-based malware attempts to evade detection through techniques like packing, encryption, or misusing legitimate applications.

Strong and effective performance helps you accelerate response

Intelligent defenses are of little value if they impede users with slow scans, take a long time to install, or are complicated to manage. Trellix Endpoint Security protects the productivity of users with a common service layer. And our new anti-malware core engine reduces the resources and power required by a user's system. Endpoint scans won't impact user productivity because they only occur when the device is idle, and they resume seamlessly after a restart or shutdown.

An adaptive scanning process also helps reduce CPU demands by learning which processes and sources are trusted, and only focuses resources on those that appear suspicious or that come from unknown sources. Trellix Endpoint Security possesses an integrated firewall that uses Trellix GTI to protect endpoints from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections.

Relieve the pressure with reduced complexity and increased sustainability

The rapid growth of security products with overlapping functionality and separate management consoles has made it difficult for many to derive a clear picture of potential attacks. Trellix Endpoint Security delivers strong, long-term protection thanks to its open and extensible framework which serves as the foundation for centralizing current and future endpoint solutions.

This framework leverages the Trellix Data Exchange Layer for cross-technology collaboration with existing security investments. The integrated architecture seamlessly integrates with other Trellix products, further reducing security gaps, technology silos, and redundancies, while improving productivity by lowering operating costs and management complexity.

Trellix ePO software can further reduce complexity by providing a single pane of glass to monitor, deploy, and manage endpoints. Customizable views and actionable workflows in clear language provide the tools to quickly assess security posture, locate infections, and mitigate the impact of threats by quarantining systems, stopping malicious processes, or blocking data exfiltration. It also provides a single place to manage every endpoint, additional Trellix capabilities, and third-party security solutions.

Gain the advantage over cyberthreats

Trellix Endpoint Security provides what today's security practitioners need to overcome adversaries' advantages: intelligent, collaborative defenses and a framework that simplifies complex environments. With strong and efficient performance and threat detection effectiveness that is proven in third-party tests, your organization can protect your users, increase productivity, and create peace of mind.

As the market leader in endpoint security, Trellix offers a full range of solutions that produce defense in depth and proactive defense by combining powerful protections with efficient management. This empowers security teams to resolve threats faster with fewer resources.

Table 1. Key features and why you need them

Feature	Why you need it
Proactive threat detection and response (Trellix Insights)	▪ Predictively and preemptively detects potential threats based on your industry and region ▪ Locally assesses security posture against the potential threat and gives corrective guidance on how to improve ▪ Gets ahead of adversaries by setting protections before an attack occurs
Real Protect	▪ Machine-learning behavior classification detects zero-day threats in near real time, enabling actionable threat intelligence ▪ Automatically evolves behavior classification to identify behaviors and add rules to identify future attacks
Endpoint protection for targeted attacks	▪ Endpoint protection reduces the gap from detection to containment from days to milliseconds ▪ Trellix Threat Intelligence Exchange collects intelligence from multiple sources, enabling security components to instantly communicate with each other about emerging and multiphase advanced attacks ▪ AMSI and PowerShell event logging uncover and help protect against fileless and script-based attacks
Intelligent, adaptive scanning	▪ Performance and productivity are improved by bypassing scanning of trusted processes and prioritizing suspicious processes and applications ▪ Adaptive behavioral scanning monitors, targets, and escalates as warranted by suspicious activity
Rollback remediation	▪ Rollback remediation automatically reverts changes made by malware and returns systems to their last known healthy state and keeps your users productive
Proactive web security	▪ Proactive web security ensures safe browsing with web protection and filtering for endpoints
Dynamic Application Containment	▪ DAC defends against ransomware and greyware and secures "patient zero"*
Blocking of hostile network attacks	▪ The integrated firewall uses reputation scores based on Trellix GTI to protect endpoints from botnets, DDoS, advanced persistent threats, and suspicious web connections ▪ Firewall protection allows only outbound traffic during system startup, protecting endpoints when they are not on the corporate network
Story Graph	▪ Administrators can quickly see where infections are, why they are occurring, and the length of exposure in order to understand the threat and react more quickly
Centralized management (ePO platform) with multiple deployment choices	▪ True centralized management offers greater visibility, simplifies operations, boosts IT productivity, unifies security, and reduces costs
Open, extensible endpoint security framework	▪ Integrated architecture allows endpoint defenses to collaborate and communicate for a stronger defense ▪ This results in lower operational costs by eliminating redundancies and optimizing processes ▪ Seamless integration with other Trellix and third-party products reduces protection gaps

Migration made easy

Environments with current versions of Trellix ePO, Trellix VirusScan Enterprise, and Trellix Agent can leverage our automatic migration tool to migrate existing policies to Trellix Endpoint Security in about 20 minutes or less.**

You'll also get these benefits from Trellix Endpoint Security:

- Zero-impact user scans for greater user productivity
- Stronger forensic data that is mapped to the Story Graph for at-a-glance insights and simplified investigations, to help you harden your policies
- Rollback remediation to automatically reverse malware changes and keep systems healthy
- Proactive insights on prioritized potential threats a nd prescriptive guidance on tuning your countermeasures against the threats with Trellix Insights
- Fewer agents to manage, along with scan avoidance, to reduce manual entry
- Collaborative defenses that work together to defeat advanced threats
- A next-generation framework that is ready to plug into our advanced endpoint detection and response solution

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

* Available with most Trellix endpoint suites. Consult your sales representative for details.

** The migration time is dependent on your existing policies and environment.