Trellix

SOLUTION BRIEF

# Trellix Endpoint Protection Platform

Overcome the adversary advantage

# Defenders are feeling the pressure to up their game

> The knowledge and capabilities gap between attackers and defenders is mandating fundamental changes to endpoint defenses

Organizations of all sizes are at risk from nation-state attackers, hacktivists, organized crime, and malicious and accidental insider threats. For adversaries, successful breaches provide the motivation and resources for further attacks. The knowledge and capabilities gap between attackers and defenders is mandating fundamental changes to endpoint defenses.

Security practitioners are under increasing pressure to defend their organizations. To overcome adversaries, endpoint defenses need to collaborate with each other and with other security technologies to quickly detect, analyze, block, and contain attacks in progress. They need to present forensic information quickly and intuitively. Moreover, they need to do all this without adding to the complexity of the environment for IT teams or impacting the productivity and performance of the users they protect.

# Trellix Endpoint Protection Platform helps you respond and adapt

Trellix Endpoint Protection Platform enables customers to respond to and manage the threat defense lifecycle. It delivers a collaborative, extensible framework to reduce the complexity of conventional multivendor endpoint security environments. It also provides administrators with visibility into advanced threats to speed detection and remediation response times. Global threat intelligence and real-time local event intelligence are shared between endpoints to further aid in rapid detection and response. Management is kept simple through a true centralized console and easy-to-read dashboards and reports.

Tellix Endpoint Protection Platform is built for real-time communication between threat defenses. Events and threat insights are shared with multiple technologies so your organization can take immediate actions against suspicious applications, downloads, websites, and files. Redundancies caused by multiple point products or defenses can be found and removed, while a common endpoint architecture integrates several layers of protection to share threat insights for faster convictions and analysis.

# 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 Protection Platform framework to help organizations defend against the very latest advanced threats.[1] DAC analyzes and takes action against greyware and other emerging malware, containing them to prevent infection.

Another available technology for advanced threats 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 and indicators of compromise. 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 and adding rules to identify similar future attacks using both static and runtime features. To immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint to the last known good state following a conviction.

1. Available with Trellix Complete Endpoint Threat Protection

# Intelligent endpoint protection lets you know what adversaries are doing now

Gathering and distributing local, community, and global security intelligence shrinks the time between attack discovery and containment to milliseconds

Better intelligence leads to better results. Trellix Endpoint Protection Platform 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, and target processes 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, Threat Intelligence Exchange technology empowers adaptive defenses to collaborate with other Trellix solutions, including gateways, sandboxes, and our security information and event management 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 (GTI), the Trellix Endpoint Protection Platform 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 they attempt to gain, such as registry or memory.

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

# Strong and effective performance helps you respond in time

Intelligent defenses are of little value if they impede users with slow scans, lengthy installations, or management complexities. Trellix Endpoint Protection Platform protects the productivity of users with a common service layer and our new antimalware core engine. This engine helps reduce the amount of 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 focusing resources on those that appear suspicious or come from unknown sources.

Trellix Endpoint Protection Platform possesses an integrated firewall that uses GTI to protect endpoints from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections.

# Improve security while reducing complexity and increasing sustainability

The rapid growth of security products with overlapping functionality and separate management consoles has made it difficult to get a clear picture of potential attacks. Trellix Endpoint Protection Platform delivers strong, long-term protection thanks to its open and extensible framework, which serves as the foundation to centralize current and future endpoint solutions management. This framework uses 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 your operating costs and management complexity.

Trellix ePolicy Orchestrator (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, other Trellix capabilities, and many third-party security solutions.

## Key features and why you need them

| Feature | Why you need it |
|---|---|
| **Real Protect** | • Machine-learning behavior classification detects zero-day threats in near real time, enabling actionable threat intelligence<br>• Automatically evolves behavior classification to identify behaviors and add rules to identify future attacks<br>• Repairs the endpoint to the last known good state to immediately prevent infection and reduce administrator burdens |
| **Endpoint protection for targeted attacks** | • Closes the gap from encounter to containment from days to milliseconds<br>• Trellix Threat Intelligence Exchange collects intelligence from multiple sources, enabling security components to instantly communicate with each other about emerging and multiphase advanced attacks |
| **Intelligent, adaptive scanning** | • Improves performance and productivity by bypassing scanning of trusted processes and prioritizing suspicious processes and applications<br>• Adaptive behavioral scanning monitors, targets, and escalates as warranted by suspicious activity |
| **Advanced antimalware protection** | • Protects, detects, and corrects malware fast with a new antimalware engine that works efficiently across multiple devices and operating systems |
| **Proactive web security** | • Ensures safe browsing with web protection and filtering for endpoints |
| **Dynamic Application Containment** | • Defends against ransomware and greyware and secures patient zero [2] |
| **Hostile network attack blocking** | • Integrated firewall uses reputation scores based on GTI to protect endpoints from botnets, DDoS, advanced persistent threats, and suspicious web connections<br>• Firewall protection allows only outbound traffic during system startup, protecting endpoints when they aren't on the corporate network |
| **Actionable threat forensics** | • Administrators can quickly see where infections are, why they're occurring, and the length of exposure to understand the threat and react quickly |
| **Centralized management (Trellix ePO platform) with multiple deployment choices** | • 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<br>• Process optimization and elimination of redundancies result in lower operational costs<br>• Seamless integration with other Trellix and third-party products reduces protection gap |

2. Available with Trellix Complete Endpoint Threat Protection

# Gain the advantage over cyberthreats

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

Trellix, the market leader in endpoint security, offers a full range of solutions that produce defense-in-depth by combining powerful protections with efficient management. Accelerated time to protection, improved performance, and effective management empower security teams to resolve more threats faster with fewer resources.

# Migration made easy

Environments with current versions of Trellix ePO, Trellix VirusScan Enterprise, and the Trellix agent can leverage our automatic migration tool to migrate existing policies to Trellix Endpoint Protection Platform in about 20 minutes or less.[3]

You'll also get these benefits from Trellix Endpoint Protection Platform:

- Zero-impact user scans for greater user productivity
- Stronger forensic data to help you harden your policies
- Performance improvements
- 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's ready to plug into our other advanced threat and endpoint detection and response solutions

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

**To learn more about Trellix, visit trellix.com.**

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