Trellix

DATA SHEET

Trellix ePO – On-prem

Centralize security management of all your endpoints in-house

Highlights

- **In-house:** Supports organizational requirements in which security infrastructure must be on-premises and managed in-house
- **Hybrid log-ins:** Single sign-on option helps you test your move to cloud and how it would work for your organizational security posture
- **Disaster recovery:** DR-Bourne, the snapshot, and a SQL back-end helps recover data and lets your security posture remain intact in case of a disaster
- **Certified:** Federal Information Processing Standards (FIPS) Certified
- **Open platform:** Our platform orchestrates policies and information for Trellix products and supported partner network, offering true integration

Overview

Security management requires constant juggling between tools and data, often with limited visibility into external threats. You need to see and plug gaps between various tools. To stay ahead of the curve, your cybersecurity workforce must be empowered to orchestrate complex cybersecurity environments simply and easily, with a proactive and not reactive, approach.

Trellix ePO – On-prem helps you simplify your security management when security infrastructure must be hosted in-house to meet industry or organizational requirements. It eliminates the time-consuming task of managing various disparate tools, ensures better visibility by bringing together data from various sources to a single pane of glass, and helps you focus on managing your security posture.

With the ever-increasing demands on cybersecurity professionals, your staff needs to respond quickly to threats on any type of device, to minimize damage. To do this, they need a strong understanding of your organization's security posture, which is paramount to risk management.

This is where Trellix ePO – On-prem can make a difference by simplifying your security management experience. In fact, the more complex the security environment, the stronger ePO – On-prem will be. It helps reduce the potential for errors and enables your security team to manage security more efficiently, proactively, and with higher efficacy. Trellix ePO – On-prem also lets you manage native controls built into the Microsoft Windows operating system, in conjunction with Trellix endpoint technology.

Key Benefits

- Industry-acclaimed centralized management with a unique, integrated single pane of glass for simplicity
- Proactive actionable intelligence to get ahead of the adversary
- Automated workflows to streamline administrative duties and achieve higher efficiency
- Open platform that integrates Trellix and other supported third-party solutions for accurate responses
- Common security management for the largest share of devices on the market
- Ability to use enhanced native controls built into operating systems, like Windows Defender
- Scalability up to thousands of devices with coverage from device to cloud

Fundamental security

Core to any security architecture is the ability to monitor and control the health of devices and systems. Industry standards, such as the Center for Internet Security (CIS) Controls and Benchmarks and the National Institute of Standards Technology (NIST) SP 800-53 security and privacy controls, call out the need to monitor and control a security infrastructure as a necessity. Use the Trellix ePO – On-prem console to gain critical visibility and eliminate the complexity of multiple product orchestration with policy management and enforcement for your entire enterprise through a single console.

You can use the built-in threat isolation engine (TIE) integrations to get some proactive threat intelligence. Furthermore, the Trellix Insights extension offers proactive hardening recommendations and capabilities, along with actionable intelligence. These security management capabilities are fundamental to your IT security compliance.

Advanced security management—simplified

About 36,000 plus businesses and organizations worldwide trust the Trellix ePO – On-prem console to manage security, streamline and automate compliance processes, and increase overall visibility across devices, networks, and security operations. Large enterprises rely on the highly scalable architecture of ePO – On-prem, which allows them to manage hundreds of thousands of nodes from an integrated platform.

The dashboard view helps you prioritize risk by providing a summary of your security posture across your entire digital terrain, in one graphical view within a new protection workspace. Administrators can drill down on specific events to gain additional insight. This summary view reduces the time to create and rationalize the data at hand and eliminates the potential for error, even if manual intervention is needed.

With Trellix Insights, you uniquely gain a view into outside anticipated threats that matter to your organization and get preemptive guidance on what you need to do. This advances your endpoint security to be more proactive and less reactive, making security management less stressful. Use the Security Resource area any time you want a summary of the latest threat information and research available at your fingertips.

True integrations lead to better management

Streamline policy maintenance for enterprise security administration with the Trellix ePO – On-prem console. It pulls in third-party threat intelligence using Trellix Data Exchange Layer (DXL), our industry-leading messaging fabric. It also integrates policies bi-directionally with an array of products. These operational efficiencies cut down process and data-sharing overhead, enabling a faster, more precise response.

Use Support Center for easy access to information on Trellix products and an overview of Trellix ePO server health in data center environments. This feature is available in the ePO – On-prem and Trellix ePO – IaaS variant for Amazon Web Services (AWS). You can proactively receive support and product notifications, search across Trellix content repositories, and access best practices and how-to resources from within the ePO – On-prem console. You can also use it to manage the health of your ePO – On-prem infrastructure with recommended steps to improve the health status.

Open platform efficiency conquers sprawl

Research conducted by ESG found that 40% of organizations use 10 to 25 tools, while 30% use 26 to 50 tools to manage billions of new threats and devices. This diversity of products creates complexity and multiplies the operational payoff of a unified management experience—from installation through reporting. More than half of organizations estimate seeing a greater than 20% improvement by integrating security tools.

Trellix embraces these requirements with an open platform approach to security management. Consolidate sprawl while protecting the breadth of your assets, supporting threat intelligence, managing open-source data, and integrating third-party products. Trellix provides the much-needed centralized control for compliance and management across a range of security products. It also allows you to invest in next-generation technologies and integrate them with existing assets within a single framework.

Our open platform offers a range of integration approaches—scripting, application programming interfaces (APIs), no-API, and minimal effort with open source DXL messaging fabric. It allows you to choose the approach that best meets your needs, without heavy customization or services. The DXL communication fabric connects and optimizes security actions across multiple vendor products, as well as internally developed and open-source solutions. With the Cisco pxGrid and DXL integration, you can have access to any data from 50 additional security technologies. The ePO – On-prem console is a key component for managing our robust open platform.

Expanded device security with native security tools management

The extensible Trellix ePO platform manages many devices, including devices with native controls. Trellix enhances and co-manages the security that's already built into Microsoft Windows 10 to provide optimized protection, while allowing organizations to take advantage of native Microsoft system capabilities. The Trellix ePO – On-prem console manages Trellix Endpoint Security, which combines specifically tuned advanced machine learning capabilities for Microsoft OS-native security, while avoiding the additional complexity and cost of an additional management console. Trellix ePO – On-prem provides a common management experience with shared policies for Microsoft Windows 10 devices and all devices across the heterogenous enterprise to ensure consistency and simplicity.

Consistency through automated workflows

The Trellix ePO – On-prem console provides flexible, automated management capabilities so that you can rapidly identify, manage, and respond to vulnerabilities, changes in security postures, and known threats from a single console.

Technically, with Trellix ePO – On-prem, you can easily deploy and enforce security policies from a single view by clicking through a few unfolding logical steps. The single-pane-of-glass view offers pertinent context as you work through tasks and see each step and how it relates to other steps. This reduces complexity and minimizes the possibility of errors. You can define how the Trellix ePO – On-prem console should direct alerts and security responses based on the type and criticality of security events for your environment and your policies and tools.

To support development operations and security operations, the Trellix ePO platform allows you to create automated workflows between your security and IT operations systems to quickly remediate issues. You can use the Trellix ePO – On-prem console to trigger remediation actions by your IT operations systems, like assigning stricter policies. Leveraging its web APIs reduces manual effort. You have the option to require an approval process before a new or updated policy or task is pushed out, reducing the risk of an error and ensuring quality control.

Rapid mitigation and remediation

The Trellix ePO platform has built-in, advanced capabilities to increase the efficiency of your security operations staff when they mitigate a threat or make a change to restore compliance. The console's Automatic Response feature can trigger an action based on an event. Actions can be simple notifications or approved remediation.

The next level—cloud-based security management

Organizations need to simplify and accelerate the deployment of advanced threat solutions. Many are seeing the efficiency value of cloud-based security management not only in terms of deployment but also by reducing the cost and maintenance of an on-premises infrastructure. This is where the Trellix ePO platform can change the equation. With Trellix ePO, you get a range of offerings starting with Trellix ePO – On-prem to Trellix ePO – IaaS, to Trellix ePO – SaaS.

While Trellix ePO – On-prem covers the in-house/on-premises offering of the Trellix ePO platform, Trellix ePO – IaaS is the infrastructure as a service offering and Trellix ePO – SaaS the multitenant SaaS offering. Both the latter offerings can be implemented in the cloud from anywhere, anytime, and can be up and running in less than an hour, depending upon infrastructure.

- Trellix ePO – IaaS* helps you leverage many native services offered by cloud service providers, such as auto-scaling and relational databases, removing the need to purchase and manage a separate database. This allows administrators to focus on critical security tasks, not the infrastructure. Trellix ePO – IaaS helps you manage Trellix Endpoint Security, Trellix Data Loss Prevention, Trellix Insights, DXL, and third-party solutions that are integrated into the Trellix ePO platform.
- Trellix ePO – SaaS enables you to dramatically simplify your management experience, so you can attend to critical security tasks. Updates to the offering are transparent, with a continuous delivery model. Device security is automatically deployed across the enterprise once your agent is deployed, eliminating manual efforts to install or update security for each device and ensuring stronger threat enforcement. This allows enterprises to manage Trellix Endpoint and DXL from a single console from anywhere.

* Support available on Amazon AWS, Google Cloud, and Microsoft Azure

Summary

It is integral for us at Trellix to ensure that security management is a simple and comfortable experience for you. With that objective in mind, we introduced Trellix ePO – On-prem, one of industry's most extensible security management platforms. However, it's the depth of the Trellix ePO platform that ensures that you get to scale not only vertically (more nodes, more devices) but also horizontally (to the Trellix ePO – SaaS offering).

What's more, the Hybrid Log-in feature in every ePO – On-prem offering (OS version 5.10 and above) is a single-sign-on option for testing how your move to the cloud would work for your security posture. Once you're comfortable you can take the next few steps and take full advantage of the many efficiencies and benefits of a SaaS-based security management platform.

Learn more about Trellix ePO – On-prem at trellix.com.

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