McAfee MVISION ePO

Simple, single point of visibility and control from anywhere

Security management is complex. It requires unwieldy maneuvering between tools and data. In addition, cybersecurity professionals cannot be consumed with managing and updating security infrastructure. Instead, they need to focus on critical security tasks such as detection and enforcement—otherwise, adversaries will take advantage of the time they spend away from these important tasks and cause significant damage. McAfee® MVISION ePolicy Orchestrator® (McAfee MVISION ePO™) eliminates the need for maintenance of an on-premises security infrastructure, allowing the security professional to focus exclusively on security. Simply access from a browser with your credentials and manage your security.

With the pool of cybersecurity professionals so scarce, your current staff needs to be empowered to simplify the orchestration of cybersecurity. They also need to respond quickly to threats on any type of device to minimize damage. To do so, they need a strong understanding of your organization's security posture, which is paramount to risk management. McAfee MVISION ePO is a global, multitenant enterprise Security-as-a-Service (SaaS) version of McAfee ePO software, our proven and unique security management platform.

McAfee MVISION ePO eliminates time-consuming maintenance of an on-premises security management infrastructure. This helps reduce the potential for errors and enables your security team to manage security more efficiently and with higher efficacy from anywhere.

McAfee MVISION ePO even includes the ability to manage native controls built in Microsoft Windows operating system in conjunction with McAfee® MVISION Endpoint technology.

Essential Security Management Made Simple

The ability to monitor and control devices and data is core to any security approach and fundamental to IT security compliance. 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 cybersecurity infrastructures as a requirement for sound security.

Key Advantages

- Industry-acclaimed centralized management
- Removes the complexity of on-premises security platform maintenance
- Comprehensive platform that manages McAfee products and native controls in operating systems like Windows Defender
- Automated workflows for efficient administrative duties
- Streamlined incident investigation and remediation
- Common security management for largest share of devices on the market
- Scales to hundreds to thousands of devices, with coverage from device to cloud

Connect With Us

The McAfee MVISION ePO console allows you to gain critical visibility and to set and automatically enforce policies in order to ensure a healthy security posture across your enterprise from anywhere. Now you can eliminate the complexity of orchestrating multiple products with an integrated single pane of glass for policy management and enforcement across the entire enterprise.

To manage risk more effectively, a protection workspace helps prioritize risk and provides a summary of your security posture over your entire digital terrain in one graphical view. Administrators can drill down on specific events to gain more insight. This summary view reduces the time needed to create reports and rationalize the data at hand and removes the potential for error if manual intervention was needed. As a SaaS

Industry analysts say that McAfee ePO software is the reason many organizations buy from and stay with McAfee.

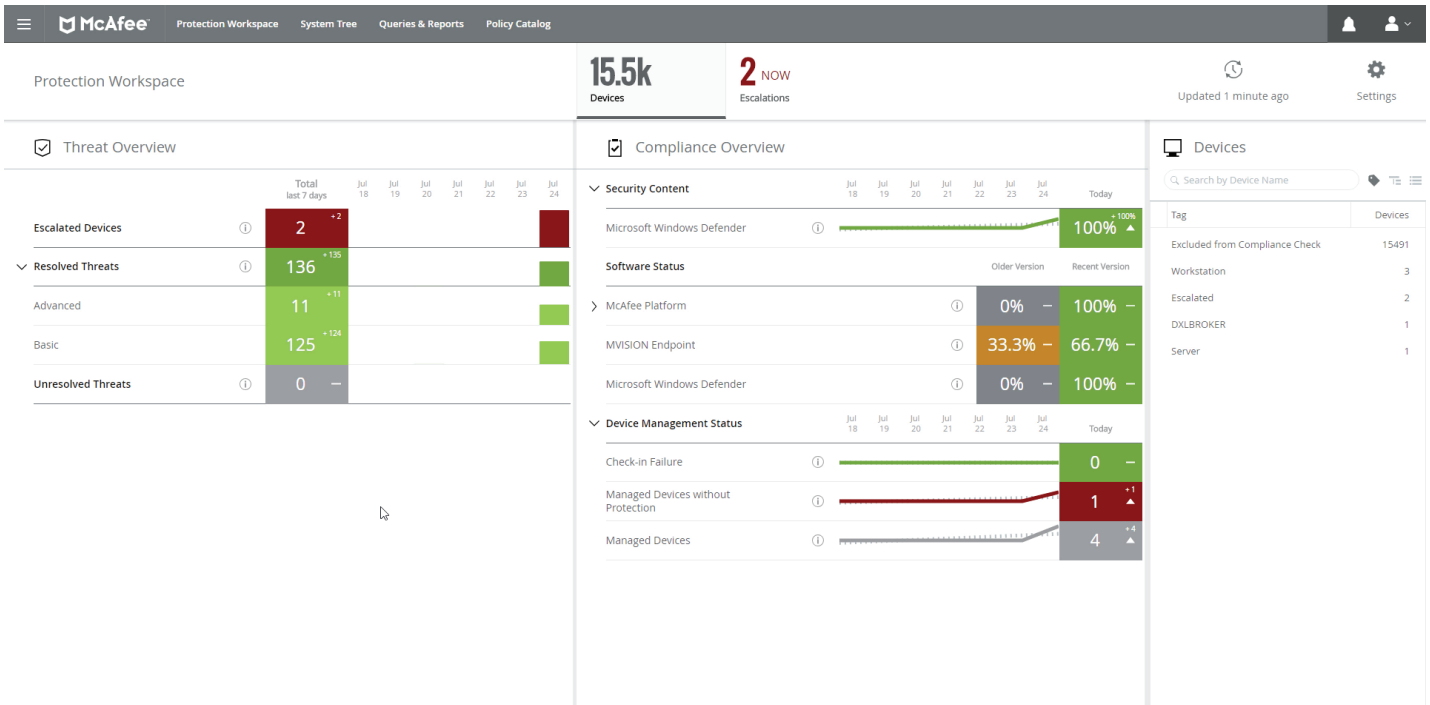

Figure 1. The McAfee ePO protection workspace.

offering, McAfee MVISION ePO removes the setup and maintenance of security infrastructure, allowing you to focus exclusively on monitoring and controlling all devices. Updates to the platform are continuous and transparent. Device security is automatically deployed across the enterprise, eliminating manual efforts to install or update security for each device and assuring stronger enforcement against threats. McAfee MVISION ePO is built on a proven track record of over 36,000 McAfee ePO software customers who manage security, streamline, and automate compliance processes and want to increase visibility across all devices in the enterprise.

Boost Threat Analysis

McAfee MVISION ePO is designed to unify security management in order to achieve better efficiency and efficacy. McAfee MVISION ePO brings risk management and incident analysis together. This enables your devices to provide critical insights to your security information and event management (SIEM) solution, ensuring that critical information is at your analysts' fingertips for improved threat hunting and remediation efforts.

Broad Device Security: Manage Native Security Tools

McAfee MVISION ePO's extensible platform manages multiple devices, including devices with native controls. McAfee enhances and co-manages the security that's already built into Microsoft Windows 10 to provide optimized protection. This allows organizations to take advantage of native Microsoft system capabilities. McAfee MVISION ePO manages McAfee MVISION Endpoint, which combines advanced machine learning capabilities specifically tuned for Microsoft OS-native security. This also avoids the complexity and cost of an additional management console. McAfee MVISION ePO 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.

Stability and Time Savings with Automated Workflows

MSI Research, commissioned by McAfee in 2018, found that organizations expect to be able to save roughly 25% of time per day by automating repetitive tasks. McAfee MVISION ePO delivers agile, automated management capabilities so that you can rapidly identify, manage, and respond to vulnerabilities, changes in security posture, and known threats—all from a single view. From this single view, you can simply deploy and enforce security policies by clicking a few sequential steps.

Pertinent context is made available as administrators work through the task and see each step and how it relates to others, removing the complexity and the possibility of error. 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 assuring quality control.

"McAfee ePO is **one of the forefathers of integrated security automation and orchestration.** ...today's security professionals require the power of traditional ePO, but delivered as a simplified experience, making them both efficient AND effective... as a SaaS-delivered workspace, MVISION combines analytics, policy management and events in a manner that enterprise and midmarket can appropriate."

—Frank Dickinson, Research Vice President, Security Products, IDC

Contextual routing directs alerts and security responses based on the type and criticality of security events for your environment, policies, and tools. The McAfee MVISION ePO platform allows you to create automated workflows between your security and IT operations systems to quickly remediate issues.

Common use cases

- Be consistent and save time by deploying policies to all devices, including those with native controls.
- Save time and eliminate redundant and labor-intensive efforts by scheduling security compliance reports to meet the needs of each stakeholder.
- Maintain your security posture by deploying agent or machine-learning security solutions as new devices are added to your corporate network by syncing the McAfee MVISION ePO console with Microsoft Active Directory.

Swift Mitigation and Remediation

The McAfee MVISION ePO platform has advanced capabilities to increase the efficiency of the security operations staff when they mitigate a threat or make a change to restore compliance. McAfee MVISION ePO's automatic response can automatically trigger an action based on an event that occurs. Actions can be simple notifications or approved remediation.

Common use cases for automatic response

- Notifying administrators of new threats, failed updates, or high-priority errors via email based on predetermined thresholds
- Applying policies based on client or threat events, such as a policy to prevent external communications when a host may be compromised (which would deny command and control activities) or blocking data exfiltration/outbound transfer until the administrator resets the policy
- Tagging systems and running additional tasks for remediation, such as on-demand memory scans when threats are detected
- Automatically quarantining the workload or container (any device) with more restricted policies
- Once a system is tagged, the escalation status is automatically shown on the Protection Workspace dashboard

Key Features

- Graphical security posture Dashboard
- Role-based access control
- Two-factor authentication
- Custom reports and queries
- Zero downtime upgrades
- Migration assistance tool for McAfee® Endpoint Security and McAfee® VirusScan® Enterprise

McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure.

McAfee does not control or audit third-party benchmark data or the websites referenced in this document. You should visit the referenced website and confirm whether referenced data is accurate.

4076_0718
JULY 2018

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com