McAfee ePolicy Orchestrator

Inspiring and empowering the security professional

Security management requires cumbersome juggling between tools and data, often with limited visibility into external threats. This puts the adversary at an advantage by having more time to exploit the gaps not seen between the tools so they can do more damage. The cybersecurity workforce is limited and needs to be empowered to simply orchestrate complex cybersecurity environments. They need to be less reactive and become more proactive to get ahead of adversaries.

Your organization needs to respond quickly to threats on any type of device to minimize the damage and when upper management demands evidence of security effectiveness. The McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform—available on premises and from the cloud (with two models to choose from: SaaS or IaaS)—helps eliminate the time-consuming effort and potential for human error. It also helps those responsible for managing security respond proactively, faster, and with higher efficacy. Unique to the McAfee ePO console is McAfee® MVISION Insights, the first technology to proactively prioritize threats and campaigns before they hit you, predict if your countermeasures can withhold the threat, and prescribe what you need to do to counter the threat concurrently.

Fundamental Security

Let's start with the must-haves. 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 out as a necessity. The McAfee ePO console allows you to gain critical visibility to help you set and automatically enforce policies that ensure a healthy security posture across your enterprise. It

Key Advantages

- Industry-acclaimed centralized management with unique, integrated single pane of glass for great simplicity—available from the cloud or on premises
- Proactive actionable intelligence to get ahead of the adversary
- Automated workflows to streamline administrative duties and achieve higher efficiency
- Open and comprehensive platform integrates McAfee and more than 150 third-party solutions for faster and more accurate responses
- Common security management for the largest share of devices on the market
- Leverages and enhances native controls built into operating systems like Windows Defender
- Scales to hundreds to thousands of devices with coverage from device to cloud

Connect With Us

eliminates the complexity of orchestrating multiple products with policy management and enforcement for your entire enterprise through a single console. The MVISION Insights extension offers proactive hardening recommendations and capabilities, along with actionable intelligence. This essential security management capability is fundamental to your IT security compliance.

Proven Advanced Security Management—Simplified

More than 36,000 businesses and organizations trust the McAfee ePO console to manage security, streamline and automate compliance processes, and increase overall visibility across devices, networks, and security operations. Large enterprises rely on the McAfee ePO console's highly scalable architecture, which allows them to manage hundreds of thousands of nodes from an integrated, single pane of glass. This dashboard view helps you prioritize risk and provides you with a summary of your security posture over your entire digital terrain in one graphical view within a new protection workspace. Additionally, with MVISION Insights, you uniquely gain a proactive view into outside anticipated threats that matter to your organization and 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. In addition, there is a Security Resource area, where the latest threat information and research is available at your fingertips.

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. The McAfee ePO console simplifies policy maintenance for enterprise security administrators. Additionally, it pulls in third-party threat intelligence, leveraging 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.

The Support Center enables easy access to information on McAfee products and provide an overview of McAfee ePO server health in customer environments. This is available for the on-premises McAfee ePO console and the McAfee ePO console on Amazon Web Services (AWS). You can proactively receive support and product notifications, search across McAfee content repositories, and access best practices and how-to resources from within the McAfee ePO console. You can also manage the health of your McAfee ePO infrastructure by easily assessing the health status and receive recommended steps to take to improve the health status.

Industry analysts call out McAfee ePO software as the reason customers adopt and stay with McAfee.

Advantages of an Integrated Platform
Organizations with integrated platforms are better protected and achieve faster response times than their counterparts without integrated platforms.

Organizations with integrated platforms

- 78% suffered less than five breaches last year.
- 80% discovered threats in eight hours.

Organizations without integrated platforms

- Only 55% suffered less than five breaches last year.
- Only 54% discovered threats in eight hours.

(Source: 2016 Penn Schoen Berland)

Open Platform Efficiency Conquers Sprawl

ESG research shows 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 product usage creates complexity and multiplies the operational payoff of a unified management experience—from installation through reporting. More than half of organizations estimate more than 20% improvement by integrating security tools (source: MSI Research 2018).

McAfee embraces these requirements with an open platform approach to security management that allows you to consolidate the sprawl while protecting the breadth of your assets, supporting threat intelligence, managing open source data, and integrating third-party products. McAfee provides centralized control for compliance and management across a range of security products. Analysts can quickly pivot across products to find the critical data and take the necessary policy action. The McAfee ePO console 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 integrations approaches (scripting, application programming interfaces (APIs), no-API, and minimal effort with open source DXL messaging fabric), allowing you to choose the approach that best meets your needs without heavy customization or services. Through the McAfee® Security Innovation Alliance program, we accelerate the development of interoperable security products, simplify the integration of these products with complex customer environments, and provide a truly integrated and connected security ecosystem to maximize the value of existing customer security investments. The McAfee Security Innovation Alliance program currently has more 150 partner integrations.

In addition, 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 McAfee ePO console is a key component for managing our robust open platform.

Expanded Device Security: Manage Native Security Tools

The extensible McAfee ePO platform manages many 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, while allowing organizations to take advantage of native Microsoft system capabilities. The McAfee ePO console manages McAfee® MVISION Endpoint, which combines specifically tuned advanced machine learning capabilities for Microsoft operating system (OS)-native security, while avoiding the additional complexity and cost of an additional management console. McAfee ePO software 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.

Save Time

Recent MSI Research 2018 notes that customers believe they will save up to 20% time if they security tools are integrated.

The Value of Integration

- Increases efficacy of tools and processes: 61%
- Reduces complexity and manual efforts, allowing security professionals to focus on tasks that require critical thinking: 61%
- Improves visibility by showing data in patterns and context: 58%
- Streamlines workflows for faster response: 57%

(*Source: MSI Research 2018)*

Consistency Through Automated Workflows

The McAfee ePO 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 single console. MSI Research, commissioned by McAfee in 2018, found that organizations expect to be able to save roughly 25% of time per day by automating repeatable or repetitive tasks.

With McAfee ePO software, 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 McAfee ePO 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 McAfee ePO platform allows you to create automated workflows between your security and IT operations systems to quickly remediate issues. You can use the McAfee ePO console to trigger remediation actions by your IT operations systems, like assigning stricter policies. Leveraging its web application programming interfaces (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.

A distinct proactive automated workflow unfolds in MVISION Insights. From the common view, outside and unknown threats and campaigns are automatically alerted and prioritized from the MVISION Insights dashboard based on industry and geographical intelligence. This provides a predictive assessment on whether your current security posture can hold against this threat. More importantly, specific actions are offered such as update the .DAT or isolate.

Common use cases

- Save time and eliminate redundant and labor-intensive efforts by scheduling security compliance reports to meet the needs of each stakeholder.
- Be proactive and gain actionable insights on anticipated threats, how they are tracking in your industry or region, if they can be countered with your current security posture, and, if not, what needs to be done, all through leveraging MVISION Insights.
- Easily integrate the McAfee ePO console into your existing business processes and functions by leveraging its robust set of APIs to gain more insight and accelerate workflows. For example, the McAfee ePO console integrates with ticketing systems, web applications, and self-service portals.
- Maintain your security posture by deploying agent or machine learning security solutions as new machines are added to your corporate network by syncing the McAfee ePO console with Microsoft Active Directory.

"McAfee ePO [software] is **one of the forefathers of integrated security automation and orchestration.** ...today's security professionals require the power of traditional [McAfee] ePO [software], 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

Rapid Mitigation and Remediation

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

Common use cases for automatic response

- Notify administrators of new threats, failed updates, or high-priority errors via email or SMS based on predetermined thresholds.
- Apply policies based on client or threat events, such as a policy to prevent external communications when a host may be compromised (to deny command and control activities) or blocking data exfiltration/outbound transfer until the administrator resets the policy.
- Tag systems and run additional tasks for remediation, such as on-demand memory scans when threats are detected.
- Trigger registered executables to run external scripts and server commands, like generating a ticket in the service desk or integrating into other business processes.
- Automatically quarantine the workload or container (any device) with more restricted policies.

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 by eliminating the cost and maintenance of an on-premises infrastructure. The McAfee ePO console can be implemented from the cloud from anywhere, anytime via two alternative deployment options: McAfee ePO software on AWS or McAfee® MVISION ePO™. Both of these can be up and running in less than an hour.

- McAfee ePO software on AWS allows organizations to leverage many native AWS services, such as auto-scaling and Amazon RDS, removing the need to purchase and manage a separate database. This allows administrators to focus on critical security tasks, not the infrastructure. McAfee ePO software on AWS manages McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, DXL, and third-party solutions that are integrated into McAfee ePO software.
- MVISION ePO builds on the advantages of McAfee ePO as a Software-as-a-Service (SaaS) offering. This dramatically simplifies the management of the platform, allowing you to attend to critical security tasks. Updates to the platform 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 enforcement against threats. This allows enterprises to manage McAfee MVISION Endpoint and DXL from a single console from anywhere.

"McAfee ePO software stands out compared to other solutions. It is a one-stop shop for our endpoint protection. I can see everything I need to see for all of our McAfee products from one pane of glass. Its easy-to-use dashboards and built-in functionality make everything—visibility, reporting, deployment, updating, maintenance, decision making—so much easier."

—Christopher Sacharok, Information Security Engineer, Computer Sciences Corporation

MVISION ePO enables your devices to provide critical insights to your security information and event management (SIEM) to ensure that relevant data is at your analysts' fingertips for improved threat hunting and remediation efforts. Additionally, existing on-premises or hybrid cloud McAfee ePO software customers can now quickly and easily migrate to MVISION ePO and take full advantage of the many efficiencies and benefits of a SaaS-based security management platform.

McAfee Products Managed by McAfee ePO Software

McAfee Products*
McAfee® Endpoint Protection (Threat Prevention, Firewall, Web Control)
McAfee® MVISION Endpoint complements Microsoft Windows Defender with Advanced Threat Protection
McAfee® MVISION Mobile
McAfee® MVISION Insights
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)
McAfee® Data Loss Prevention (McAfee® DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**For McAfee ePO software on premises.*

Flexible Deployments

Deployment	Primary Benefit
McAfee ePO on premises	Full control of data and feature set
McAfee ePO on AWS	Eliminates the need for hardware maintenance required by an on-premises solution
McAfee® MVISION ePO Software-as-a-Service*	Multi-tenant SaaS offering to eliminate all maintenance of infrastructure and upgrades

**Not all McAfee ePO software capability is available on McAfee MVISION ePO.*

Use Cases: How the McAfee ePO Console Enables Security Centralized Management

Product and Technology	Use Case	Benefit
MVISION ePO MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO software manages McAfee MVISION Endpoint, which augments Microsoft Windows 10 native controls with advanced protection. You can easily discover and manage advanced threats with a common management platform and consistent policies for Microsoft Windows and McAfee Endpoint Security.	Better protection for native controls for Microsoft Windows and more efficient proven management
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security discovers a known malicious file on an endpoint. The McAfee ePO console sets a stricter policy on the endpoint to quarantine it. This is done with one common management interface.	Quick containment of infected endpoints
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager detects significant data exfiltration on an endpoint and tags it in the McAfee ePO console. The McAfee ePO console applies data loss protection policies to block the data and advise the user that this is not in compliance.	Automatic data loss policy enforcements
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insight	McAfee MVISION Insights offers actionable information on prioritized and anticipated outside threats. MVISION Insights pivots to McAfee® MVISION EDR to offer indicators of compromise (IoCs) and search to determine if they exist in the environment with current investigations. If so, detailed information is available on a related campaign and what you can do.	Accelerate investigation and resolutions

Integration Examples

Product and Technology	Integrated Use Case	Benefit
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security flags a suspicious host. The McAfee ePO console can trigger additional scans. This is communicated to Cisco ISE via PxGrid and the DXL exchange (via the McAfee ePO console). Cisco ISE can isolate the host until it is deemed acceptable.	Increased proactive protection
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO shares the asset list with Nexpose. This enables you to gain an understanding of your risk posture from your McAfee ePO console and allows you to set policy accordingly. Vulnerability data is shared with the DXL community of vendors.	▪ Reduce complexity ▪ Gain a comprehensive and reliable posture and prioritize actions to minimize risk from one dashboard
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	This integration facilitates bi-directional and real-time intelligence sharing between the network and endpoints. Events are also shared with the DXL community. Check Point Anti-Bot software blade blocks command and control (C&C) traffic and alerts McAfee ePO software, as well as other integrated third-party security solutions over common DXL topics. With this intelligence, McAfee automatically initiates a relevant remediation workflow for endpoint devices. Check Point and McAfee can also detect and prevent zero-day attacks and convert them into known attacks, regardless of whether the attacks are coming from the network or the endpoint. By exchanging mission-critical intelligence in real time, the integration enables our respective products to detect, block, and remediate threats in an automated fashion.	▪ Decrease time to detect ▪ Block and remediate attacks

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