McAfee ePolicy Orchestrator

Centrally get, visualize, share, and act on security insights

Security management requires cumbersome juggling between tools and data. This puts the adversary at an advantage by offering more time to exploit the gap not seen between the tools and do damage. In addition, the cybersecurity workforce is limited and needs to be empowered to manage cybersecurity complexity. The McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform removes the time-consuming and potential human error effort and inspires those responsible to manage security quicker and with higher efficacy.

Fundamental Security

Start with the fundamentals. Core to any security architecture is the ability to monitor and control the health of endpoints and systems. Industry standards such as Center for Internet Security **(CIS)** Controls and National Institute of Standards Technology **(NIST) SP 800 153** security and privacy controls call this out as a must. The McAfee ePO console allows you to gain critical visibility and set and automatically enforce policies to ensure a healthy security posture across your enterprise. Policy management and enforcement across security products for your entire enterprise is accomplished from a single console, removing the complexity of managing multiple products. This essential security is fundamental to your IT security compliance.

Proven Advanced Security Management

More than 30,000 businesses and organizations trust the McAfee ePO console to manage security, streamline and automate compliance processes, and increase overall visibility across endpoint, network, and security operations. Big companies rely on the McAfee ePO console's highly scalable architecture, allowing large enterprises to manage hundreds and thousands of nodes from a single console. The McAfee ePO console provides an enterprise security administrator with the opportunity to simplify policy maintenance, pull in third-party threat intelligence leveraging Data Exchange Layer (DXL), and integrate policies bi-directionally with an array of products. These operational efficiencies cut down process and data-sharing overhead, allowing a faster, more precise response.

Connect With Us

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 use creates complexity and multiplies the operational payoff of a unified management experience—from installation through reporting. McAfee embraces these requirements with a "Together is power" 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 command and control for compliance and management across a range of security products. You 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.

A Sample List of Products Managed by McAfee ePO

McAfee Products	Third-Party Products
McAfee Endpoint Protection (Threat Prevention, Firewall, Web Control)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
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	

Use Case Examples: How the McAfee ePO Console Creates Centralized Management of Security Products

Product and Technology	Sample Centralized Management Use Case	Benefit
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 in one common management interface.	Quick containment of a bad endpoint
McAfee ePO McAfee DLP 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 enforcement

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 (the McAfee ePO console). Cisco ISE can isolate the host until it is deemed acceptable.	Increased proactive protection
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Deploy and manage the industry-leading, privilege management solution, Avecto Defendpoint, from McAfee ePO. Avecto Defendpoint configuration changes are informed by McAfee Threat Intelligence Exchange application reputation data.	Reduction in complexity No additional infrastructure, lowering TCO Privilege access changes based on threat intelligence
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO shares assets list to Nexpose. This enables you to gain an understanding of 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 shared with the DXL community.	Decrease time to detect Block and remediate attacks

Organizations with integrated platforms are better protected and achieve faster response times than their counterparts without integrated platforms.

	Integrated Organizations	Not Integrated Organizations
Suffered less than five breaches last year	78%	55%
Discovered threats in eight hours	80%	54%

2016 Penn Schoen Berland

Extensible Workflows Streamline Processes

The McAfee ePO database provides flexible, automated management capabilities so you can rapidly identify, manage, and respond to vulnerabilities, changes in security postures. and known threats from single console. You 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. 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.

Common Use Cases

- Save time and eliminate redundant and labor-intensive efforts by scheduling security compliance reports to meet the needs of each stakeholder.
- 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, integrate with ticketing systems, web applications, or self-service portals).
- Maintain your security posture by deploying agent and security solutions as new machines are added to your corporate network by syncing the McAfee ePO console with Active Directory.

"The most powerful endpoint management platform on the market today, McAfee ePolicy Orchestrator, this product is the underlying management tool for all of the company's security products, and it offers the power and flexibility that enterprise buyers desire. The security capabilities are broad and tightly integrated through a common policy engine and intelligence stream."

—Forrester Wave: Endpoint Security Suites 2016

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. McAfee ePO 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

- Notifying administrators of new threats, failed updates, or high-priority errors via email or SMS 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 (this 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
- Triggering registered executables to run external scripts and server commands, like generating a ticket in the service desk or integrating into other business processes
- Automatically quarantining the endpoint with more restricted policies

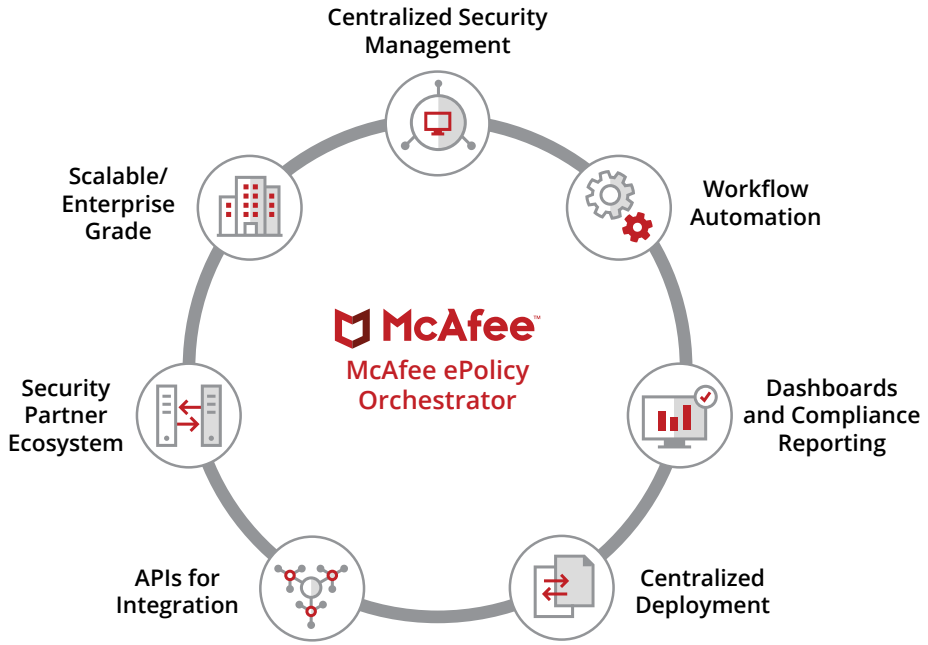

Figure 1. Centralized security management using the McAfee ePO console.

Secure Across Your Organization with the McAfee ePO Console

Centrally manage security

- Distinctive single console for centralized management and visibility into up to hundreds of thousands of nodes across the enterprise
- Open framework for broad security management of systems secure by McAfee and third-party solutions
- Extensible platform integrates with and leverages your existing IT infrastructure to reduce operational friction

Accelerate response times with confidence

- Comprehensive views and insight to proactively address internal and external security issues
- Swift centralized deployment of security updates and definitions to ensure that endpoints are protected from the latest threats
- Accelerated response times through actionable dashboards and advanced query and reporting capabilities

Reduce complexity and streamline processes

- Ability to get up and running quickly with guided configuration, automated policy management work streams, and predefined dashboards
- Tag-based policy assignment to precisely target application of predefined security profiles to individual or groups of systems based on their business roles or risk status
- Task catalog and automated management capabilities to streamline administrative processes and reduce overhead
- Single agent to manage multiple endpoint products reduces your risk of endpoint conflicts

Scale for enterprise deployments

- Enterprise-class architecture to support managing hundreds of thousands of devices with a single server
- Supported and proven within complex, heterogeneous IT environments
- Enterprise reporting, which aggregates a comprehensive view of your security posture and compliance

"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

McAfee Together is power.

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