



Protect what you value.

McAfee ePolicy Orchestrator (ePO)

The McAfee security risk management strategy enables intelligent security and compliance optimization, delivered by McAfee ePolicy Orchestrator

Security products once were mostly “set-and-forget” point products. Configurations were simple and protection occurred in the background, with little or no need for full-time administration. Now, more and more IT resources are needed to address an organization's security and compliance requirements. McAfee® is the first to offer a comprehensive and integrated security risk management (SRM) approach. With our SRM strategy, McAfee products are developed, enhanced, and integrated to leverage what you already have, providing unprecedented operational efficiencies and ROI.

KEY ADVANTAGES

Implement a strong SRM strategy

- ePO provides powerful cross-product integration, unified management, and reporting and auditing across our security and compliance products.

Lower costs through integration

- Deploying a single integrated agent and console across endpoint, data and network security products translates into lower TCO and faster ROI, a result of having less complexity in maintaining security product policies.

Identify problems quickly

- Get answers about infections and threat events faster. ePO provides data-level integration among endpoints, data, networks, web, and email, streaming threat and vulnerability information into a single, central management hub.

Accelerate response time

- ePO's unmatched updating speed allows IT administrators to update tens of thousands of systems in an hour or less—all verified via ePO's powerful reporting.

Achieve operational efficiencies and business benefits

- ePO customers benefit from significantly fewer deployed servers, and reduced number of total administrators spending less time per week administering and managing security products—all translating into measurably lower staff resources and operating cost.

McAfee ePolicy Orchestrator® (ePO™) is the most popular and respected security management technology with over 35,000 customers and managing nearly 58 million PCs and servers. ePO brings intelligent security that is automated and actionable, enabling organizations to make quick and effective decisions. ePO is the first centralized management console that manages security beyond the endpoint to include data and network protection that can significantly reduce costs and improve threat protection and compliance management.

Answer Your Three Core Questions—At All Times

- Am I secure?
 - Faster time to identify problems: “Are there infections out there, are there IPS events?”
- Am I compliant?
 - Faster time to response: “Is my security policy enforced properly? Are the point products up to date? Are my systems properly patched?”
- Am I at risk?
 - Faster time to confidence: “The number of point products needed to address the threats has risen to an unmanageable number.”

McAfee ePO Advantage—Integration Beyond the Endpoint

McAfee ePO enables companies to lower the cost of managing security while at the same time improving operational performance through enhanced integration. With ePO, McAfee delivers real-time information and application integration for endpoint, network and data security as well as compliance management.

ePO delivers four levels of integration and benefits:

- **Agent integration**—Use a single agent to manage multiple protection tiers
 - Cost savings result from less complexity in maintaining security product policies
- **Management integration**—Single management console provides policy configuration and editing, policy deployment, policy enforcement, and reporting for multiple endpoint, data, network security, and compliance management
 - Delivers centralized management to lower cost and improve visibility
- **Data integration**—Share data and report on policy compliance and event activity
 - Streamlines threat, vulnerability and security policy information to simplify compliance
- **Application integration**—Countermeasure awareness among network, compliance management, email, web, and endpoint security environments
 - Centralized information and actionable security enables faster response to outbreaks

SYSTEM REQUIREMENTS

ePO server

- CPU: Pentium III-class 1.0 GHz or better (1.5 GHz or better multi-processor or dual-core recommended)
- RAM: 1 GB minimum, 2 to 4 GB recommended
- OS: Microsoft® Windows® 2000 SP4/Windows Server 2003 SP1/2 and R2 (32-bit) only
- Disk space: 1.0 GB (1.5 GB if upgrading from ePO 3.6.x to ePO 4.0, 2 GB recommended)

Clients

- CPU: Pentium III-class 1.0 GHz or better
- Memory: 512 MB RAM minimum (1 GB recommended)
- OS: Windows 2000, XP, 2003, Vista

ePO web console

- CPU: Pentium III-class 1.0 GHz or better
- RAM: 512 MB minimum, 1 GB recommended
- OS: Windows 2000, XP, 2003, Vista
- Browser: Microsoft Internet Explorer 6.0 SP1 or higher, or Microsoft Internet Explorer 7.0

Virtualization platforms

- VMware Virtual Infrastructure 3 (ESX 3.0.x)
- Microsoft VirtualServer 2005 R2

Database software

- Microsoft SQL Server 2000 or SQL Server 2005 (including native mode)
- Local or remote install
- 32-bit and 64-bit (64-bit is only supported when used as a remote database)
- Microsoft SQL Server 2005 Express Edition is included for smaller environments (~500 nodes)

Key Features

Web-based console

- Anywhere access to console without having to install any software on the systems

Customizable dashboard

- Custom dashboard view presented at user login via a web browser
- Reports compiled to become dashboards
- Every report on the dashboard can be clicked on to view the details
- Dashboards can be created by each user and shared with other users

Microsoft Active Directory synchronization

- Greatly improved usability of managing systems within ePO
- Active Directory can be synchronized at any level within the directory
- Specific organization unit (OU) groups can be mirrored within ePO

Automate and actionable reports

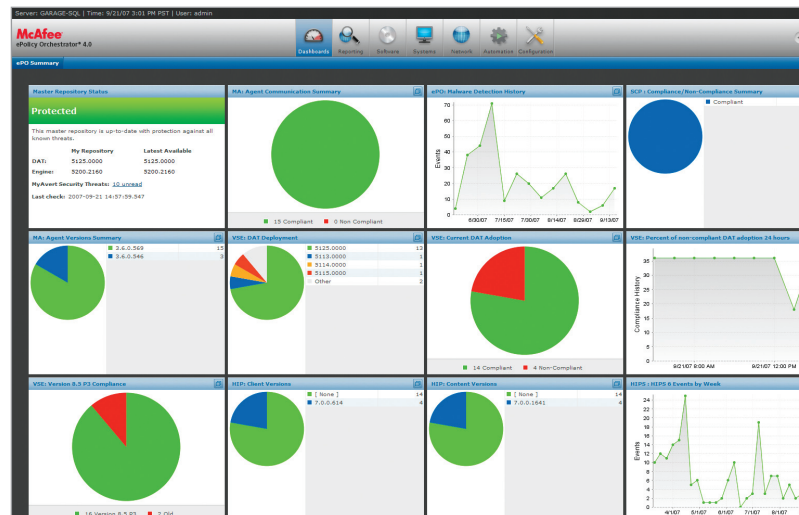
- Reports can be automated and scheduled to run at any time
- Reports can be automatically exported into many different formats, and emailed all in the same action
- Any report generated within ePO is actionable
- Users can select a system or a number of systems in the report summary table and take immediate action to resolve issues or perform tasks on targeted machines

Automate, report and enforce compliance

- Enforce security policies with regular policy updates or NAC
- Identify rogue systems that connect to your network with Rogue System Detection
- Measure, audit and report on policy and regulatory compliance

Granular role-based access control

- ePO allows more people within an organization to take advantage of the information in ePO
- Roles within ePO are defined by permission sets
- System access can be restricted at any group level, not just site levels
- Users with restricted system access cannot view other parts of the system, and their reports, queries, and dashboards will only report on the systems to which they have rights



ePO's configurable dashboard displays critical information in an easy-to-view format.

