



Managing Security Policy and System Protection

Centralized Management for the Enterprise

Table of Contents

Introduction	3
Executive summary	3
Core offering	3
Agent-based system	3
Deployment options	3
Bring systems easily up to speed	4
Scalable to any size environment	4
Tackling the task of monitoring 24/7	4
Protecting against rogue systems	4
Microsoft patch compliance	4
Protecting mobile and remote users	5
Extending McAfee ePO to third-party solutions	5
User experience	5
Conclusion	5

Centralized Management for the Enterprise

Introduction

The landscape of corporate security has changed dramatically over the years. Once viruses held the position of public enemy number one and it was a race to put out new virus definitions in order to clean infected systems in a timely manner. Over the years, the threat model has changed dramatically. End users are not only faced with threats from macro viruses, but now must contend with worms, Trojans, malicious Web content, and application vulnerabilities that leave many feeling overwhelmed by the amount of work needed to secure machines from these threats.

This paper examines how McAfee® ePolicy Orchestrator® (ePO™) helps organizations create, manage, and maintain security policies and applications without a large increase in IT hours.

Executive summary

ePolicy Orchestrator, the cornerstone of the McAfee security portfolio, provides an organization with the central point to create, define, and deploy security policies across an enterprise environment. Features such as rapid anti-virus deployment, system policy enforcement and compliance, rogue system detection, spyware protection, and extensive reporting built on top of a robust and efficient updating repository provide the tools necessary to combat today's rapidly changing threats.

Core offering

ePO is a centralized server solution to install, configure, manage, and report on threat mitigation tools deployed throughout the enterprise network. ePO deploys agents on desktops, laptops, and servers to enforce and monitor system security policy compliance and assist in deploying and updating anti-virus, anti-spyware, host intrusion prevention (HIPS), and desktop firewall (DTFW) applications.

Available for Microsoft® Windows® and Novell NetWare, ePO provides centralized management of threat prevention technology and security policy enforcement. ePO was built

for IT administrators who are responsible for maintaining the security policy of an enterprise network.

The ePO console provides a single interface for managing deployment and reporting of McAfee System Protection Solutions—McAfee VirusScan® Enterprise, McAfee Anti-Spyware Enterprise, McAfee Entercept® (HIPS), McAfee Desktop Firewall™, and McAfee WebShield® SMTP. ePO also provides features specific to its agents, such as rogue system detection, notification, and the system compliance profiler. Building on the strength of these products, ePO grants IT administrators the ability to transition their policies and designs from theory into reality.

The foundation of ePO is a central server that functions as a repository for policies and reports. ePO provides a hierarchical structure for systems managed within the enterprise. The server itself runs on Windows 2000/2003 server platforms with the agents running on a wide variety of platforms. An MS-SQL database is used for data storage; Crystal Reports is utilized for report generation.

Agent-based system

ePO utilizes a common agent installed on servers, desktops, and laptops throughout your environment. Agents check the system and enforce compliance to the policies established by the ePO server. The agents continually monitor the security software installed on the system to provide real-time enforcement of the enterprise network security policy.

Deployment options

The network-wide deployment of ePO is simplified into three stages. The first phase is the installation of the ePO server. This server should be installed on a stand-alone server with a static IP address. The ePO server can be placed anywhere within your environment, as long as the ePO agents can find an IP route back to the server.

The second phase involves establishing the security policies you want to exist within your network. These policies can contain a number of factors, such as what security software will be installed, which users can make modifications to security settings, and frequency of virus definition updates.

It is possible to set these policies to a very granular level, even down to the specific user level within ePO, but most administrators take advantage of Microsoft Active Directory

(AD) integration. ePO can leverage key investments already made in AD, ensuring simplified change control and directory consistency throughout the enterprise. Microsoft AD integration allows the scheduled import of systems from AD into the ePO directory and also, where appropriate, provides the capability to identically mirror AD groupings within the ePO directory.

The final phase of deployment involves installing the agents to the systems within your network. Using embedded administrative credentials, ePO agents can be deployed to any system on your network. It is also possible to install via login scripts, reconfigured install packages, or third-party tools. Given the ease of use and scalability, most administrators will use the built-in deployment option.

Once an agent has been installed, it will immediately communicate to the ePO server to retrieve the latest policies and begin policy enforcement. The agent then begins collecting information from the host, such as anti-virus definitions, OS patch level, and network identification to send to the ePO server. The agent also collects incident information from security software installed on the host to send to the ePO server for collection and reporting.

Bring systems easily up to speed

At customizable intervals, the ePO agent checks into the ePO server and looks for updates or configuration changes. Since the agent initiates the communication, it is less likely to miss an update or change due to network latency or interruption. If an agent checks in and does not have the appropriate software or is in need of an anti-virus update, it will automatically pull down the appropriate code and install it. The IT administrator simply defines in the policy what the ePO agent is to watch for and ePO handles the installation and updating. It is also possible to send the agent a “wakeup” call and have it check in immediately instead of waiting for the next scheduled check.

Scalable to any size environment

ePO has been designed to support up to 250,000 agents from a single server. The management console also allows an administrator to manage multiple ePO servers from a single console. The streamlined updating structure of ePO allows for verifiable updates of 50,000 hosts in less than an hour. The administrator can use ePO to set up repository servers for remote locations to get updates locally instead of traversing the WAN. Updates can also be scheduled for non-peak hours to manage bandwidth impact.

Tackling the task of monitoring 24/7

ePO provides integrated alerting and notification on compliance, threat activity, and rogue system detection. Thresholds defined by your administrator enable critical alerts to be sent to specified individuals via e-mail, SMS, text pager, or SNMP trap. Alerts cover threat activity, anti-virus compliance levels, and rogue system detections.

A wide array of over 50 pre-defined reports in ePO makes it easier to locate non-compliant systems, trace an outbreak to its source, or determine effectiveness of security policies. All of the information is at your fingertips, ranging from one-page, executive security summaries to detailed information on virus policy and activity, desktop firewall policy, system vulnerabilities, anti-spam, and content filtering policies.

Customizing reports to suit your specific needs is just as easy. Your administrators may select from a variety of printable and exportable chart types, including three-dimensional bar charts, pie charts, line graphs, and tables.

Protecting against rogue systems

A single, unknown system lacking appropriately managed protection represents a significant threat to the entire network—introducing the risks of constant re-infection of known threats, new vulnerabilities, potential threat targets, or propagation points. Many companies have spent countless hours cleansing a network from a worm only to have it reintroduced by an unprotected system plugged into their network by a contractor, vendor, or careless employee.

ePO takes a unique approach to mitigating the risk of rogue, non-compliant systems. Using distributed sensors, ePO passively monitors the network for any LAN-based connections, quickly establishing whether they are currently managed by ePO and providing a range of policy-based responses to rogue systems not managed by ePO. This information can be used by administrators to quickly focus on these systems and bring them into compliance.

Microsoft patch compliance

The System Compliance Profiler (SCP) is an integral component of ePO, enabling administrators to quickly assess enterprise-wide system compliance, including the presence of vital Microsoft security patches. Profiling is based on rules, customized by the administrator or templates downloaded from McAfee, searching for a file, service, registry key, or specific Microsoft patch reference. Patch fingerprinting (utilizing MD5 hash codes) is also available to ensure absolute integrity of Microsoft security patches and prevent patch spoofing. Criticality of compliance is set by the administrator and easily monitored in the form of detailed, graphical compliance reports.

Protecting mobile and remote users

Given the increase in remote offices and mobile users, ePO includes features to account for systems that do not have direct continuous access to the ePO server. Software updates through ePO can be resumed if they are interrupted during the download process. Remote offices can also have a repository server at their location to reduce bandwidth costs. Multiple update sources can be added so that the ePO agent will download updates from the closest repository server or will look for an alternate server if the default server is unavailable. Administrators can also configure ePO to allow mobile users to defer updates to a time when they will be able to complete the update.

Extending McAfee ePO to third-party solutions

Not all environments have the option of being completely homogeneous when it comes to security software. ePO takes this into account by including the ability to manage third-party system security software in the same console that you manage McAfee's products. This allows for consolidated reporting, management, and metrics.

User experience

McAfee customers with experience in maintaining large enterprise networks have repeatedly cited ePO's ability to shift the administration from a reactive to a proactive state as a primary benefit of ePO. This helps them to dramatically decrease the time and resources spent recovering from attacks by worms and malicious code. Customers point to ePO's reporting features as integral to simplifying malicious threat management.

McAfee customers also routinely praise McAfee's consultants and technical support staff for helping them to quickly deploy and adapt ePO to their existing Windows domains and network architecture.

Conclusion

ePO provides a complete system security management solution designed to give IT and security administrators the power and flexibility to manage security threats and compliance throughout their network. Properly implemented, ePO can help reduce the number of security incidents, reducing expenses in man-hours for recovery and lost productivity due to security related outages.

ePO does this by focusing on the areas that have traditionally caused administrative headaches, such as creating and enforcing security policies and enforcing them at an enterprise level instead of at an individual level. With ePO, an IT administrator can easily manage vulnerabilities enterprise wide regardless of the number of systems or users on the network. Protecting large and small networks from new and varied attacks becomes an easily achievable goal with the rapid updating and configuration abilities of ePO.

ePolicy Orchestrator 3.6 is the industry-leading system security management solution —delivering a coordinated, proactive defense against malicious threats and attacks for the enterprise. As the central hub of McAfee security solutions, administrators can mitigate the risk of rogue, non-compliant systems, keep protection up-to-date, configure and enforce protection policies, and monitor security status, 24/7, from one centralized, enterprise-scalable console.