



Boost your McAfee[®] ePolicy Orchestrator[®] (ePO[™]) Performance

How to Stabilize and Improve the McAfee Experience

How to Stabilize and Improve the McAfee Experience

Table of Contents

Introduction	3
Promisec Complements ePO	3
Complete	4
Accurate	4
On-demand	4
Dynamic and Updated.....	6
Promisec Solutions	6
Custom McAfee Config Settings	7
Processes.....	7
Services.....	7
Success Stories	8
Large Northern Hospital System	8
Conclusion	8

How to Stabilize and Improve the McAfee Experience

Introduction

McAfee® ePolicy Orchestrator® (ePO) is a popular enterprise-class management platform designed to centrally manage systems, networks, data and compliance across an organization. According to McAfee, “ePO software helps more than 35,000 customers manage security on nearly 60 million nodes, reducing costs, improving protection and increasing visibility into security and compliance postures.” Promisec complements ePO by managing the unmanaged endpoints, monitoring the endpoints and providing the ability to start and stop services.

Utilizing unique and proprietary agentless technology, Promisec helps organizations maximize their investment in ePO and achieve the full potential of the ePO platform by:

- ▶ Providing unmatched 100% accurate visibility of the endpoint landscape
- ▶ Discovering endpoints that are not being managed by the console including rogue devices
- ▶ Discovering endpoint agents that have been disabled, tampered or failed to report into the ePO console
- ▶ Independent validation that policies for required services and processes are enforced
- ▶ Reducing cost of controlling AV endpoints
- ▶ Enabling powerful and simple remediation to resolve issues

Promisec Complements ePO

Like most endpoint management solutions, ePO’s architecture relies on agents installed on every managed endpoint in the organization, which must be configured accurately for the solution to be available and effective. Unfortunately, agent based technologies are all susceptible to a common weakness: agents themselves can be disabled or missing, rendering the associated solution uselessly unavailable. The problem is common affecting 23% of endpoints in a typical organization according to recent Promisec research where one or more of an organization’s 3rd party agents will fail a health check audit.

Promisec complements ePO through an ability to monitor and report on services and processes, and remediation capabilities that include stopping or starting services as necessary to ensure system health -functionality not available within ePO.

While it is likely that most IT organizations have good compliance coverage of their ePO deployment, odds are high that it is not perfect and anything less than 100% coverage represents a magnitude of risk and inefficiency within the organization.

Self-monitoring doesn’t work. If McAfee is missing a specific endpoint, that blind spot extends to their dashboard. Promisec provides an independent platform to ensure that if you have purchased and deployed ePO, the solution is distributed to 100% of your computers.

How to Stabilize and Improve the McAfee Experience

Complete

Like all agent based solutions, ePO is subject to 3 types of weaknesses:

Weakness	Implication
Agents not deployed	<ul style="list-style-type: none">▪ In many organizations, there are branches or specific endpoints where the company is unaware that ePO is not deployed (outside the domain, workgroup, etc)▪ In others, the IT organization does not even know where the solution is not deployed because of false positives or missed computers
Agents are disabled	<ul style="list-style-type: none">▪ Users unintentionally or intentionally turn off or disable the agents
Agents are not updated	<ul style="list-style-type: none">▪ For a variety of reasons, agents may not be running the latest upgrade or service, meaning the endpoint is not fully protected

Promisec resolves all of these weaknesses by identifying endpoints that are missed by the ePO console. In most cases, Promisec can deploy agents on endpoints that have been missed by the deployment engine. While Promisec does not claim to be a full deployment platform, for specific defined deployments of software, Promisec is often the most expedient solution.

Furthermore, Promisec also identifies, reconfigures and restarts or reconfigures agents that are deployed but disabled or not configured properly, and identifies and remediates missing updates or any other detected irregularity.

Accurate

Promisec inspections query a number of different APIs and objects on each endpoint, providing cross-check and 100% accuracy.

On-demand

IT organizations often need quick answers for specific tasks or problems. Promisec provides ad-hoc reporting capability using a simple interface, which can be deployed in less than one hour for most environments.

With Promisec, the report is defined within minutes and data can be collected immediately and accurately with absolutely no impact to the day-to-day operations. Within just a couple of hours, Promisec can report and remediate

How to Stabilize and Improve the McAfee Experience

up to 10,000 endpoints.

Promisec inspections take under 6 seconds per endpoint and require absolutely no agents on endpoints. This allows Promisec to run inspections 24/7 with no disturbance to employees' regular work. With Promisec, all reports are updated regularly, meaning that managers can see current status and trends.

The following is representative of the type of ePO data Promisec can quickly retrieve from all endpoints within an organization:

Host	Object	Details
192.168.1.11	DAT Version Date	2010/09/03
192.168.1.11	McAfee VS Version	8.7.0.570
192.168.1.11	McAfee Spy Version	8.7.0.129
192.168.1.11	Agent Version	4.0.0.1180
192.168.1.11	McAfee Protection Setting	Standard
192.168.1.11	Quarantine Directory Location	C:\QUARANTINE\
192.168.1.11	McAfee DAT Version	6094.0000
192.168.1.11	Engine Version	5400.1158
192.168.1.11	Last Agent Checkin	20100903105145
192.168.1.11	AP/BO DAT Version	499
192.168.1.11	Microsoft Product	Windows Server (R) 2008 Enterprise
192.168.1.11	Microsoft Product ID	92516-082-2500885-76760
192.168.1.11	Pending System Reboot	none
192.168.1.11	Windows Installer Version	C:\Windows\Installer\45b80.msi
192.168.1.11	VS Engine	Running
192.168.1.11	TaskManager	Running
192.168.1.11	FrameWork	Running

How to Stabilize and Improve the McAfee Experience

192.168.1.11	On Access Scanner	Running
192.168.1.11	Validation Service	Running

Dynamic and Updated

Promisec was created to monitor and remediate each endpoint in a 24/7 manner for IT, security and compliance purposes. Promisec performs these functions in 4-6 seconds per machine, without overloading the network while being transparent to the endpoint. As a result, ALL Promisec functionality can be performed during working hours without interference, even in highly sensitive environments, such as financial trading, where every second is critical. Promisec provides all of its functionality from one console with no dedicated expertise on the side of the customer.

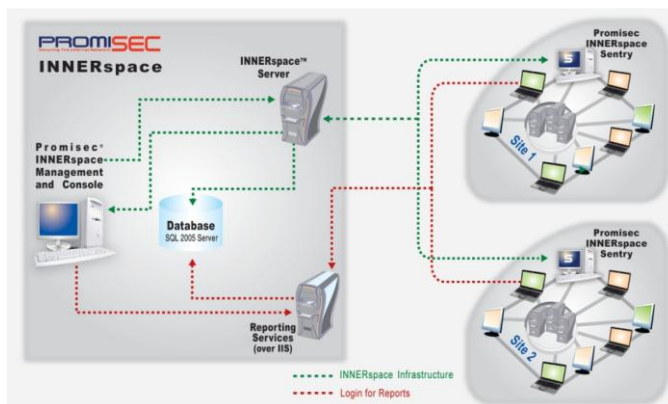
Promisec is specifically designed to have no tangible network impact and zero endpoint impact, such that it can be run at all times, providing timely and accurate updated reporting.

Promisec Solutions

Promisec provides software applications that utilize unique and proprietary agentless technology to deliver unmatched visibility into 100% of your systems' endpoints. Our unique agentless technology allows IT executives to drive out the cost of controlling your endpoints by optimizing your existing IT solutions and processes. By knowing what you have previously not known about your endpoints, we make it faster and easier to resolve known problems as well as fix unknown problems.

The immediate, continuous visibility and independent control offered by our products enable you to manage many kinds of corporate policies...including IT compliance, security, inventory, operations, licensing and power management.

Utilizing your existing management credentials, Promisec's agentless capabilities leverage published and unpublished APIs to inspect and remediate endpoints within your environment with negligible impact on your network. Promisec inspections allow independent, focused, and dynamic exception-based control and management of your endpoints without WMI, ActiveX or dissolvable agents.



How to Stabilize and Improve the McAfee Experience

Custom McAfee Config Settings

Promisec has pre-packaged a custom inspection baseline that covers critical processes and services required for successful ePO delivery. In addition to monitoring for states, Promisec can be configured to automatically enable and start services or reconfigure services based on your policy.

Processes

Displayed Process	Defined Process	Description
VS Engine	engineserver.exe	McAfee Engine Service
VS TaskManager	vstskmgr.exe	Allows scheduling and updating of tasks
FrameWork	frameworkservice.exe	Shared component framework for McAfee
On Access Scanner	mcshield.exe	Provides McAfee On-Access scanning protection
Validation Service	mfevtps.exe	Provides validation trust protection services

Services

Service Name	Services Display Name
McTaskManager	McAfee Task Manager
McAfeeEngineService	McAfee Engine Service
McShield	McAfee McShield
McAfeeFramework	McAfee Framework Service
Mfevtp	McAfee Validation Trust Protection Service

How to Stabilize and Improve the McAfee Experience

Success Stories

Large Northern Hospital System

The Challenge:

- ▶ Struggling to keep current with diverse A/V infrastructure
- ▶ Required to use a specialized DAT to mitigate risk to enterprise to maintain high quality of healthcare

The Solution:

- ▶ Utilizing Promisec Spectator, In less than one hour, the endpoint team and server team had resolved over 50 percent of the endpoint issues during a proof of concept

The Results:

- ▶ Validated specialized DAT deployment on endpoints, which was critical to mitigate risk
- ▶ Inspected 1,000 computers in less than 12 minutes
- ▶ Reported specialized DAT deployment coverage (not available in their current A/V console) to confirm compliance
- ▶ Remediated endpoints that could not get updates from A/V console
- ▶ Validated all A/V processes as operating and repaired unoperable processes on the fly
- ▶ Inspected P2P/Remote-Control applications so removal occurred in minutes and not days
- ▶ Reported MS Service Pak deployment.

Conclusion

Promisec independently identifies the core stress points associated with optimized ePO posture. Because the solution is agentless and independent, Promisec identifies problems in the foundation, and can resolve issues immediately or simply report on them.

Promisec provides an independent framework for the most accurate, comprehensive, and reliable solution for monitoring and reporting of corporate policy deviations. Through its unique, agentless approach, Promisec provides solutions that are unmatched in providing IT and security executives with the right information, at the right time, and with the least amount of effort.

No other solution can provide such a comprehensive approach while not requiring any configuration changes to the network or endpoint, having no impact on the network and taking only 4-6 seconds per endpoint for inspection and remediation. Only Promisec can provide this kind of holistic framework because of its agentless architecture. Most other solutions on the market are vendor-based or agent-based, meaning they have intrinsic limitations. Whether those limitations are in the amount of time they take to inspect, the bandwidth they require to allocate, their legacy technology that overload the CPU or in the scope of the inspections they perform, the results they offer do not address the fundamental infrastructure flaws of the operating system.

Promisec has proven to be a valuable and complementary component of many successful ePO deployments, helping

How to Stabilize and Improve the McAfee Experience

our customers maximize their investment in ePO, while significantly improving the effectiveness of this mission critical component of their security and management posture.

Contact us today to learn more about how we might help your organization stabilize and improve your McAfee experience.

About Promisec®

Promisec, Inc. delivers Agentless Endpoint Management software solutions that eliminate threats and optimize corporate internal networks with unprecedented visibility and control over the endpoints. Promisec's patented technology allows IT managers to identify and resolve security, compliance and policy issues in a matter of minutes, without making any changes to the network or endpoints.

Founded in 2004 by former military intelligence experts, Promisec's management team brings broad high-level executive experience in the network security industry.

Promisec is a privately held company with headquarters in Israel and offices in New York, Tokyo and Paris. Our customers include Forbes Global 2000 companies and other organizations in the manufacturing and service industries as well as government and health care institutions.

For more information visit www.promisec.com.

For More Information

Promisec

Email: sales@promisec.com

Internet: www.promisec.com

Copyright© Promisec 2009. All Rights Reserved.



2009 Red Herring 100 Award Winner honoring Promisec as "one of the top 100 most promising tech companies."

