# Boost your Symantec™ (SEP11) Endpoint Protection Performance

**How to Stabilize and Improve the Symantec Experience**

PROMISEC
Securing The Internal Network

## Table of Contents

## Introduction

Symantec™ Endpoint Protection (SEP11) is a popular enterprise-class solution combining Symantec Antivirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single agent and management console, increasing protection and helping lower total cost of ownership. Promisec complements SEP11 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 SEP11 and achieve the full potential of the SEP11 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 SEP11 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 Symantec Endpoint Protection

Like most endpoint management solutions, SEP11's architecture relies on an agent installed on every managed endpoint in the organization. These agents must be configured accurately on each endpoint for the solution to be available and effective. Unfortunately, agent based technologies are 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.

Promisec complements SEP11 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 SEP11.

While it is likely that most IT organizations have good compliance coverage of their SEP11 deployment, anything less than 100% coverage represents a magnitude of risk and inefficiency within the organization. The only way to reach 100% coverage is to have agentless validation.

Self-monitoring doesn't work. If Symantec 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 SEP11, the solution is distributed to 100% of your computers.

**Complete**

Like all agent based solutions, SEP11 is subject to 3 types of weaknesses:

| Weakness | Implication |
|---|---|
| Agents not deployed | ▪ In many organizations, there are branches or specific endpoints where the company is unaware that SEP11 is not deployed (outside the domain, workgroup, etc).<br>▪ Frequently, the IT organization does not even know where the solution is not deployed because of false positives or missed computers. |
| Agents are disabled | ▪ Users unintentionally or intentionally turn off or disable the agents. |
| Agents are not updated | ▪ 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 SEP11 console. In most cases, Promisec can deploy agents on endpoints that have been missed by the deployment engine. While Promisec does not replace a software 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 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.

**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.

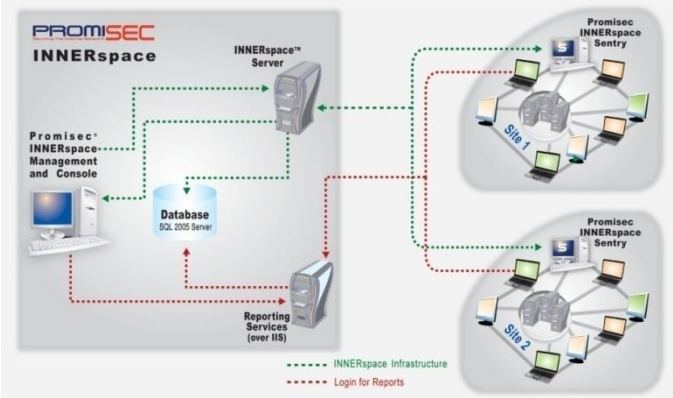
Promisec is specifically designed to have no tangible network impact and zero endpoint impact, such that it can be run at all times, providing timely and accurate updated reporting.

## 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.

## Custom Symantec Configuration Settings

Promisec has pre-packaged a custom inspection baseline that covers critical processes and services required for successful SEP11 delivery. In addition to monitoring for states, Promisec can be configured to automatically enable and start services or reconfigure services based on your policy.

**Registry Settings**

There are twenty-seven registry objects associated with SEP11:

| Object | Example Details | Description |
|---|---|---|
| ClientGroup | | The Symantec Group the client belongs to |
| DefaultHomePage | http://www.symantec.com/enterprise/security_response/index.jsp | Default website |
| DisableSplashScreen | 1 | Disable and Enable Symantec's Splash Screen |
| GUID | AF8C7EF8448A3843B1A055CED1F45CB4 | Unique Identifier used by Symantec to identify the client |
| HomeDirectory | D:\Program Files\Symantec AntiVirus\ | Directory where the product is installed |
| InstalledProducts | 1 | Product Installation Information for Symantec Endpoint Protection |
| LogFileRollOverDays | 14 | Number of days before log file is rolled over to another name |
| MyProcessID | 1388 | The process id that is used to execute the product |
| RebootStatus | 1 | Determine the reboot status of the client |
| ScanEngineVendor | NAV | |
| ServerName | | The Server that manages the client |

| | | |
|---|---|---|
| TimeOfLastScan | 28071F1100370000 | Date and time of last scan performed |
| VirusEngine | I2ldvp3.dll | Name of the dll file used for the virus engine |
| DebugLogOn | 0 | Debug switch |
| DebugLogLevel | 0 | Debug log levels for the firewall |
| DebugLevel | 0 | Debug log levels for antivirus |
| ProductVersion | 11.0.6100.645 | Actual Client Version Number |
| DebugLogFileSize | 20000 | Size of the log file before it's rolled to another name |
| DumpSylink | c:\sylink.log | Name of the log file created and used for troubleshooting |
| EnableScriptDebug | 0 | The Host Integrity is performed on the agent machine by a .JS javascript file included in the policies downloaded from the policy manager. Normally this script is deleted once HI is done, but by setting this registry key the file will not be deleted so that you can review the script for troubleshooting. |
| DefinitionVersion | DA07080000001F0000000000000000000002000000 | Version of the virus definition file the client is currently using |
| IPSSignature | C:\PROGRA~1\COMMON~1\SYMANT~1\SymcData\CNDCIP~1\20100827.001 | IPS Signature Symantec Endpoint Protection is using |
| SMCEngineStatus | 1 | To check the Network Threat Protection is installed and on |
| LUSchedulingEnabled | 1 | Determine if scheduling is enabled for LiveUpdate |
| LUEnableProductUpdate | 1 | Determine if LiveUpdate is enabled or disabled |
| QuarantineAgeLimit | 30 | Number of days quarantine information will be retained |
| SysPlant Start | 4 | Determine if device and application control is enabled or disabled |

**Processes**

There are four processes associated with SEP11:

| Displayed Process | Defined Process | Description |
|---|---|---|
| Rtvscan Process | Rtvscan.exe | The Rtvscan.exe runs the real time scanning feature of the Symantec Endpoint Protection and is responsible for detecting malicious code embedded on possible viruses and other malware processes. |
| Sygate Secure Enterprise | Smc.exe | A component of Sygate Secure Enterprise that implements firewall protection. |
| Sygate Protection Agent | SmcGui.exe | Sygate Protection Agent 5.0 build 6144 allows local users to obtain management control over the agent by executing the GUI |
| LiveUpdate | LuCallBackProxy.exe | LiveUpdate process |

**Services**

There are eight services associated with SEP11:

| Service Name / Display Name | Description |
|---|---|
| Symantec Endpoint Protection 11.0 | Provides virus scanning for Symantec Endpoint Protection |
| Symantec Antivirus | Provides virus scanning for Symantec Endpoint Protection |
| Symantec Event Manager | Event propagation and logging service |
| Symantec Management Client | Provides communication with the Symantec Endpoint Protection Manager. It also provides network threat protection and application and device control for the client |

| | |
|---|---|
| Symantec Settings Manager | Setting storage and management service |
| Symantec SymSnap VSS Provider | Symantec SymSnap VSS Provider |
| Symantec Network Access Contr* | Checks that the computer complies with the define security policies and communicate with the Symantec Enforcers to allow your computer to access the corporate network |
| LiveUpdate | This is the services the updates the client with the latest definition file and systems updates for Symantec Endpoint Protection |

## Conclusion

Promisec independently identifies the core stress points associated with optimized SEP11 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 without 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 SEP11 deployments. The solution allows our customers maximize their investment in SEP11, 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 Symantec 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

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