Product Brief

Symantec® Protection for SharePoint Servers 6.10

At A Glance

Scanning
• Performs real-time scans of files as they are uploaded to and downloaded from your SharePoint server(s).

• Off-box or On-box implementation

• Leverages the latest Symantec security stack

Reporting
• Allows administrators to obtain updates on virus activity within the SharePoint environment via regularly scheduled or on-demand reports.

Management
• Features a management interface that is easy to use and administer

• Frequently updated virus definitions so there is no lag between new threats and your protection

Overview

Symantec Protection for SharePoint Servers (SPSS) detects and removes viruses, spyware, and other threats in files uploaded to and downloaded from your SharePoint server(s). Using Symantec award-winning antivirus technologies, it quickly scans files for potential threats. The technology integrates with the SharePoint Administration Console, enabling easy and seamless management of your SharePoint server environment.

SPSS leverages the power of the Symantec Global Intelligence Network to alert you quickly if a malicious attack is about to strike your company. It blocks the threat and keeps it from affecting your business by helping to ensure that your Symantec products maintain the latest virus definitions. SPSS receives updated virus definitions automatically and frequently, so there is no lag between the time that Symantec finds a new threat and your organization is protected from it.
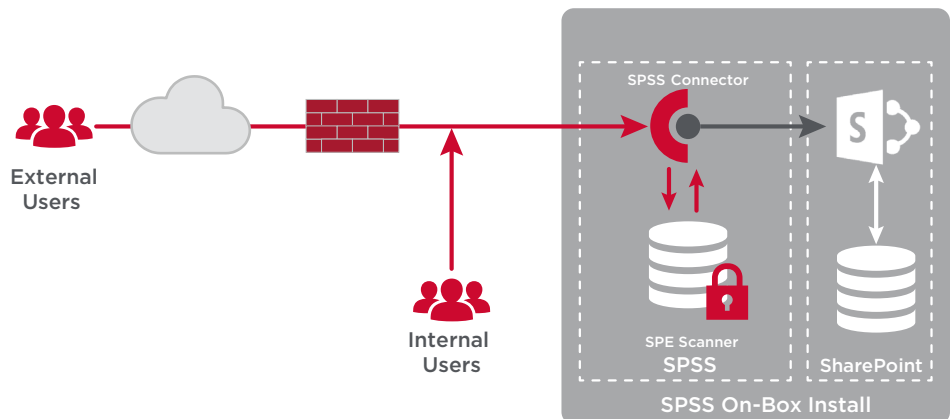
Key Features

Scanning
In addition to the real-time scanning of files, SPSS can perform scheduled or on-demand scans on your SharePoint server(s). Scheduled scans of the SharePoint document library help ensure that all files are protected by new virus definitions as they become available. Scheduled scans take place in the background, so they do not interfere with SharePoint operation. Administrators also can conduct manual, on-demand scanning of the SharePoint library at any time. Performing a manual scan does not affect previously scheduled scans.

SPSS offers the industry's only off-box scanning option. The Symantec Protection Engine component can be installed on the SharePoint server as usual, or on a separate server to increase performance, allow scalability, provide fail-over, and reduce the load on the SharePoint server.

Key Features (cont.)

Reporting

SPSS lets administrators obtain updates on virus activity within the SharePoint environment via regularly scheduled or on-demand reports. Reports can be created in PDF format and automatically forwarded to a list of recipients upon generation.

Management

SPSS features a management interface that is easier to use and administer. It seamlessly integrates with the Microsoft SharePoint Administration Console so that administrators can use a single interface to manage all SharePoint settings, including advanced security settings and scan engine configurations. Settings can be updated remotely from any machine without the need to install a separate agent.

Key Benefits

- Simplifies and speeds up the process of recovering quarantined files by storing both the file and its metadata

- Features a management interface that makes the product even easier to use and administer, saving your organization valuable time and allowing you to focus on key strategic IT initiatives

- Prevents your SharePoint server from becoming a repository of infected files by scanning and cleaning files stored in SharePoint but not accessible to endpoint antivirus solutions

- Allows both manual and scheduled scanning of the SharePoint document library

- Delivers fast response to and remediation of malware threats

- Leverages Symantec STARGate Security engine, a collaborative ecosystem of security technologies that protect Symantec customers from malicious attacks.

- Integrates tightly with the Microsoft SharePoint Administration Console to provide a single management interface for configuring all SharePoint settings, both locally and remotely

Enhancements in SPE for SharePoint Servers

Increased Protection

- Integration with Symantec Protection Engine 8.2.0

- Higher efficacy by leveraging the latest STARGate technology stack

- Block active content: Disarm feature removes active content from the files during a real-time scan

- Large (64-bit) file and container support: Removes the scanning limit based on size of the file and container

- Enhanced file scanning performance on Windows

- New malware detection techniques for better correlation of features and attributes across a file or multiple files in containers

Increased Usability/Productivity

- High Intensity Detection (HID): Provides enhanced prevention by having greater visibility through higher level detections

- Malware Policy Rule: Unrepairable files will be treated as Malware files from SPSS 6.1.0 onwards

- Integrated definition management with STAR components that self-update

Microsoft SharePoint Platform Support

- Microsoft SharePoint Server 2013

- Microsoft SharePoint Server 2016

- Microsoft SharePoint Server 2019

Support for Microsoft SharePoint Server 2010 has been discontinued in this release.

See the latest Platform Support Matrix and documentation.

Learn more about Symantec Protection Engine for SharePoint Servers.