Symantec™ Protection Center Sizing and Scalability Guide

Symantec™ Protection Center Sizing and Scalability Guide

Documentation version: 2.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Introduction to Symantec Protection Center sizing and scalability

This document includes the following topics:

About this guide

This guide is intended to help you correctly size and deploy Symantec Protection Center for optimum protection and serviceability in your environment.

This guide provides the following information:

- Overview of Protection Center functionality and its major components
  See "Introduction to Symantec Protection Center" on page 4.
- Hardware recommendations for virtual and physical Protection Center implementations

See "Hardware recommendations" on page 7.

- Scaling recommendations for the number of endpoints and combination of integrated security products in your environment
  See "Determining the appropriate combination of integrated products for your environment" on page 9.
- Backup plan recommendations
  See "Protection Center backup recommendations" on page 10.

The architectures, designs, and recommendations that are provided in this guide are based on metrics from internal testing of Protection Center. These tests are performed in an isolated environment. Implementations in production environments might result in performance metrics that vary from the testing scenarios. These variations can alter the recommended sizing and architecture.

Note: This guide references possible modifications to Protection Center capability, functions, metrics, and features. These modifications are subject to change and should not be considered as firm commitments by Symantec.

Introduction to Symantec Protection Center

Symantec Protection Center is a centralized security management application. It enables organizations to identify emerging threats, prioritize tasks, and accelerate time to protection based on relevant actionable intelligence. Protection Center uses a combination of process automation and security intelligence to enable users to remediate incidents and proactively protect key systems and information assets.

See "About Protection Center components" on page 5.

Protection Center collects information from security products in your environment as well as from the Symantec Global Intelligence Network. Protection Center normalizes the data and creates context for each of the individual product events. The information and tasks appear in the Protection Center dashboard, where users can generate cross-product reports and start remediation workflows across integrated products. Protection Center provides single sign-on access to the integrated Symantec and third-party products.

Protection Center performs the following major functions:

- Collects the data that security products provide and collects data from the Global Intelligence Network
- Correlates local product data with global intelligence data

- Provides a centralized view across endpoint, messaging, and third-party security products through single sign-on, data collection, and process automation
- Delivers notifications of events based on event severity
- Generates cross-product reports
- Facilitates workflow processes
- Provides single sign-on access to security products in your organization

About Protection Center components

Symantec Protection Center contains a number of architectural components that work together to protect your company from security threats.

See "Introduction to Symantec Protection Center" on page 4.

Table 1-1 Protection Center components

Component	Description
Symantec Protection Center Server (Protection Center)	The management server that is used to gather data from integrated security products. The management server uses this data to build online cross-product reports and generate notifications. Protection Center is deployed as a virtual or a physical appliance, depending on the needs of your organization. The virtual appliance is created using a VMware ESX virtual machine. The physical appliance is created using a physical server. The appliance monitors itself to ensure that it is secure, available, and performing at specified levels. If Protection Center detects an issue, it automatically takes actions to resolve the issue. If the issue cannot be resolved without user intervention, a notification is generated to inform the administrator of the issue. For example, if a hard drive is near capacity, a notification is generated to notify the administrator.
SQL Data Store (database)	The database that stores all configurations, updates, the data that is collected from endpoints, and report information.
Pluggable Application Component (PAC)	A file that contains the set of software components that each supported security product requires to integrate with Protection Center. The PAC allows Protection Center to collect threat summary data and system data from the integrated product and reflect that data in cross-product reports. The PAC also allows a Protection Center user to use single sign-on (SSO) to access the user interface of each integrated product.

Table 1-1 Protection Center components *(continued)*

Component	Description
Symantec Protection Center interface	A Web-based user interface that lets you configure Protection Center and manage Protection Center resources such as users, supported products, and workflows of remediation actions. The Protection Center interface also lets users access cross-product reports and alerts, and use SSO for direct access to integrated product servers. You can also interact with Protection Center through the Protection Center control panel. The control panel provides access to a limited number of features, such as changing the predefined administrator account (SPC_Admin) password.
LiveUpdate	The service that Protection Center uses to update the Protection Center software and PAC files. Keeping Protection Center current helps to ensure that you have the latest features, software fixes, and security enhancements.
Symantec Backup Exec System Recovery (BESR)	The service that Protection Center uses to perform scheduled backups of itself and the data it receives. If anything happens to Protection Center or its data, you can easily restore them to the way they were before the issue.
Integrated products	Protection Center lets you bring multiple security products together to centralize security management. The following are some of the ways in which an integrated product can work with Protection Center: ■ Sending notifications for display in the dashboard and reports ■ Making data available for cross-product reports ■ Embedding all or a portion of the product's user interface into Protection Center so that the product can be accessed and managed through Protection Center ■ Making product functionality, such as an endpoint scan, available through report actions ■ Adding custom reports For a current list of Symantec and third-party products that can integrate with Protection Center, see the Protection Center page on the Symantec Web site. The Protection Center page is located at the following URL: http://go.symantec.com/protection-center

Planning your Protection Center installation

Consolidating security data from multiple security products requires a robust and a responsive infrastructure that is designed to support your environment. Before you deploy Protection Center, you should determine the best way to configure the appliance to suit the scale of your particular environment.

See "Introduction to Symantec Protection Center" on page 4.

The crucial factors to providing a high performance Protection Center installation are:

- Deploying Protection Center on the appropriate hardware to support the number of endpoints in your environment.
  See "Hardware recommendations" on page 7.
- Configuring the Protection Center database to support the expected data load in your environment.
  The expected data load can be determined from the number of endpoints and the number of integrated products that Protection Center supports.
  See "Determining the appropriate combination of integrated products for your environment" on page 9.

In addition to considering these crucial factors, consider the following variables when planning your Protection Center installation:

- Number of endpoints in your environment
- Retention of event data in the archive
- Number of registered security products
- Symantec Protection Center technologies that are to be integrated
- Number of Protection Center users that need to access the data concurrently

Hardware recommendations

The recommended hardware for your Protection Center installation depends on whether you have a virtual or a physical appliance. The recommended hardware also depends on the number of endpoints that Protection Center needs to support.

See "Planning your Protection Center installation" on page 6.

See "Protection Center backup recommendations" on page 10.

Table 1-2 Protection Center hardware requirements

Item	1 - 5000 endpoints (virtual or physical)	5000 - 50000 endpoints (virtual) 5000 - 150000 endpoints (physical)
Processor cores	Two physical cores	Four physical cores
Memory	8 GB	16 GB

Table 1-2 Protection Center hardware requirements *(continued)*

Item	1 - 5000 endpoints (virtual or physical)	5000 - 50000 endpoints (virtual) 5000 - 150000 endpoints (physical)
Hard disk	100 GB SAS 10K rpm	500 GB NAS (virtual only) or SAS 15K rpm in high-performance disk array
Storage device	Hardware RAID levels 1, 5, 6, 10, and 50 are supported. Software raids are not supported. In non-NAS and non-RAID environments, only a single hard disk is supported. External storage devices that are not on the same subnet as Protection Center must be able to resolve appropriate drive mappings.	
Processor speed	Minimum: 1.8 GHz Recommended: 2.53 GHz	
Network	Required: Static IPv4 IP address, subnet mask, default gateway, and DNS Optional: Static IPv6 IP address, prefix length, default gateway, and DNS	
Network card	A single 1 Gigabit Ethernet network card that supports Microsoft Windows Server Core 2008 R2 Web edition.	
General hardware	Required: Dedicated resources that no other application uses Required (virtual appliance): 64-bit hardware that supports VMware ESX 4.0 or 4.1 and Microsoft Windows Server Core 2008 R2 Web edition Required (physical appliance): 64-bit hardware that supports Microsoft Windows Server Core 2008 R2 Web edition	

Note: The disk capacity recommendations assume that you want to retain raw event data in the Protection Center archive for at least 90 days.

RAID 1 should be used only on relatively small installations, as disk saturation may occur in installations with larger numbers of endpoints.

Advanced RAID configurations should be considered for larger configurations. With performance and fault tolerance in mind, Symantec recommends the following RAID configurations. The configurations are listed in order of best performance to worst performance: RAID 10, 50, 5, 6, 1.

Improved hard disk, RAM, and CPU configurations all provide significant performance and scalability benefits. If it is not practical to improve specifications in all of these areas, it is recommended that you first optimize disk configuration. You should then increase RAM, and then add CPU cores.

Determining the appropriate combination of integrated products for your environment

Each integrated security product produces a data load on Protection Center. This data load varies according to the number of endpoints that report to the product server. The data load also varies according to the number of threats in the environment and the type of data that the product generates. The information in this section can help you determine the number of security products that can be integrated into your environment without degrading Protection Center performance.

See "Planning your Protection Center installation" on page 6.

Note: You should use this information only to determine the optimal mix of integrated products for the total number of endpoints in your environment. You should choose the specific hardware configuration that you use for Protection Center based on the total number of endpoints that you need to support.

See "Hardware recommendations" on page 7.

Each Symantec security product is given a weighted variable that represents the effect of the product on Protection Center performance. You can use these variables to determine the most appropriate combination of security products for your Protection Center hardware configuration.

Only the security products that support data integration with Protection Center are relevant to calculating the system load score. Products that support console integration only have a negligible effect on Protection Center performance. The system load calculation formula includes only the products that currently support data integration with Protection Center: Symantec Endpoint Protection (SEP), Symantec Messaging Gateway (SMG), Symantec Encryption Family (PGP), Symantec Mail Security for Microsoft Exchange (SMSMSE). When additional products support data integration with Protection Center, the formula may be modified accordingly.

The system load score is calculated as follows:

((3.78 x # of SEP servers + 7.17 x # of SMG servers + 0.8 x # of PGP servers + 7.0 x # of SMSMSE servers)/100) x (# of endpoints/1000)

The following table shows the system load scores that are appropriate to environments with various numbers of supported endpoints. For optimal Protection Center performance, you should select your mix of integrated security products accordingly.

Table 1-3 Protection Center system load score

System Load Score	Number of endpoints supported
1 - 5	Maximum of 5000 endpoints
5 - 25	Maximum of 50,000 endpoints (virtual appliance only)
25 - 75	Maximum of 150,000 endpoints (physical appliance only)

Protection Center backup recommendations

Database backups create a copy of the Protection Center database. In the event of data corruption or hardware failure, the Protection Center administrator can retrieve lost data by restoring the most recent backup. By default, the database is backed up with the rest of the Protection Center appliance when a full backup is performed.

You should create backups regularly and store them on a separate disk drive, preferably at a secure off-site facility. The recommended backup plan assumes that Protection Center uses the embedded database that is supplied with Protection Center. Use the Protection Center interface to schedule regular backups. Protection Center backups are performed using Symantec Backup Exec System Recovery, which is automatically installed as an appliance component.

At initial installation, Protection Center requires approximately 45 GB of storage per backup. By default, Protection Center maintains three backup copies so the storage location for the appliance backups requires a minimum of approximately 150 GB. These requirements increase as Protection Center adds and processes more information. When Protection Center purges older information from the database, the amount of space that is required for individual backups is reduced. However, if you want to maintain a large history of report information, you should consider providing more storage capacity.

See "Hardware recommendations" on page 7.

Index