

# Symantec™ Endpoint Protection 11.0

## Migrating to the Next-Generation of Symantec AntiVirus™

### Introduction

Symantec Endpoint Protection 11.0 adds firewall, intrusion prevention, and device control to proven Symantec AntiVirus™ and antispysware protection, for a major advance in IT security and a great value for your customers. This guide will help you introduce your customers to:

- **New features and benefits** they will find in Symantec Endpoint Protection 11.0
- **New deployment tools** to help them put these powerful technologies to use quickly

### At a glance

Symantec Endpoint Protection 11.0 improves protection against more threats, and simplifies administration of security assets. And it comes ready to enable Symantec™ Network Access Control, for even stronger network defenses, managed under the same console.

### Who gets what?

Help your customers protect critical endpoints today. The Symantec Upgrade Assurance Program grants customers the right to upgrade any product listed here to any new version released during the term of its valid maintenance agreement.

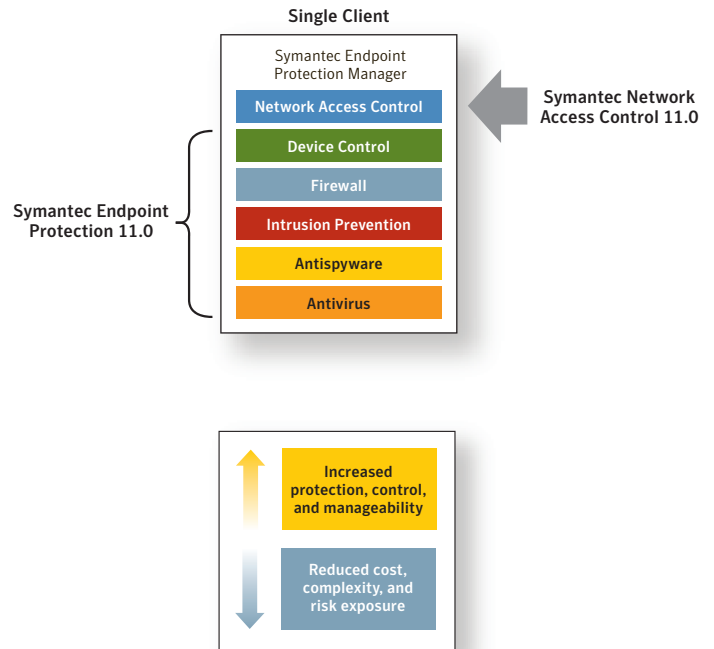


Figure 1. Symantec Endpoint Protection 11.0 consolidates advanced protection from essential security technologies under a single management console—and comes ready to add powerful network access controls.

Product under current maintenance:	Entitled to receive:
Symantec AntiVirus™ Corporate Edition Symantec™ Client Security Symantec Sygate™ Enterprise Protection*	Symantec Endpoint Protection 11.0
Symantec AntiVirus™ Enterprise Edition	Symantec™ Multi-tier Protection 11.0 <i>(includes Symantec Endpoint Protection 11.0, Symantec Mail Security, and Symantec AntiVirus for Linux and Macintosh)</i>

\*Configurations with self-enforcement and other network access control options will receive equivalent technology from Symantec Network Access Control 11.0.



## What's new

Here's a quick overview of the most important new features and benefits your customers will receive with Symantec Endpoint Protection 11.0:

### Proactive threat protection

Malware is getting more sophisticated—your customers' protection should, too. Symantec Endpoint Protection 11.0 combines advanced threat protection to anticipate attacks and prevent damage:

- **Proactive Threat Scan**

Non-signature-based malware detection and blocking delivers real-time protection, even against zero-day attacks that have never been seen before.

- Out-of-the-box detection, with no manual tuning or configuration required
- Highly accurate, with exceptionally low rates of time-wasting false positives
- Field-tested and proven in Symantec consumer products

- **Generic Exploit Blocking (GEB)**

Proactive technology uses a generic signature to block new exploits of known vulnerabilities—even before the software vendor issues a patch. And since GEB scans network traffic at each endpoint, it blocks threats at the network layer, before they infect systems.

- **Enhanced spyware/rootkit detection and removal**

Enhanced rootkit detection and removal integrates advanced Raw Disk Scan technology, getting under the OS to prevent even self-cloaking rootkits from compromising systems and critical data.

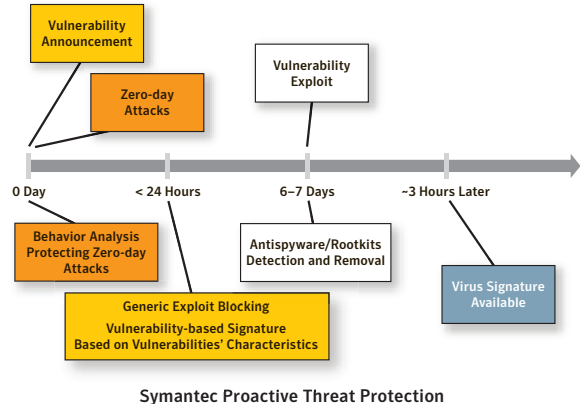


Figure 2. Proactive Threat Protection deploys three technologies—Proactive Threat Scan, Generic Exploit Blocking and rootkit detection and removal—for advanced protection against sophisticated threats.

### Simplified administration

- **Single console**

A single console manages all Symantec Endpoint Protection functions, as well as Symantec Network Access Control (licensed separately). Central management simplifies administration and adds operational efficiencies such as single software and policy updates, unified central reporting, and unified licensing and maintenance.

- **Single agent**

A single agent supports all five Symantec Endpoint Protection technologies, to simplify management and reduce system loads. It supports Symantec Network Access Control, too—so there's no need to install a new agent when you extend protection.

### Higher performance, better security

- **Light footprint**

The new, resource-friendly Symantec Endpoint Protection agent uses up to 84 percent less base memory\*, compared to previous versions of Symantec Client Security and Symantec AntiVirus, and adjusts its use of client resources to minimize performance impact.

\*Preliminary results from beta tests.

- **Client firewall**

Location-aware policies grant or deny laptops network access, based on their physical or network location, according to policies defined by the administrator. The firewall monitors both inbound and outbound traffic, and prevents malware from communicating confidential information outside your customers' networks.

- **Device and application control**

Application control provides process, file-registry, module and DLL access controls. Advanced device control manages peripherals and controls how they are used—to prevent data leakage through USB ports, MP3 players, and other external devices.

### **Flexible deployment**

Symantec Endpoint Protection 11.0 includes essential technologies that can be enabled or disabled to match customers' exact requirements:

- **Standard implementation**

Customers can establish basic protection quickly by implementing technologies selectively, or gradually as their needs and capabilities expand. Antivirus, antispysware, and intrusion prevention including rootkit detection and removal, behavior threat protection, and Generic Exploit Blocking are all available in standard implementations that speed configuration and setup.

- **Advanced implementation**

When they're ready for increased security and control over threats from internal users, customers can deploy complete endpoint protection with client firewall, application control, and device control, as well as OS protection.

- **Full implementation**

For comprehensive Endpoint Security deployment, customers can simply add and license Symantec Network Access Control, which uses the same management console and agent as Symantec Endpoint Protection.

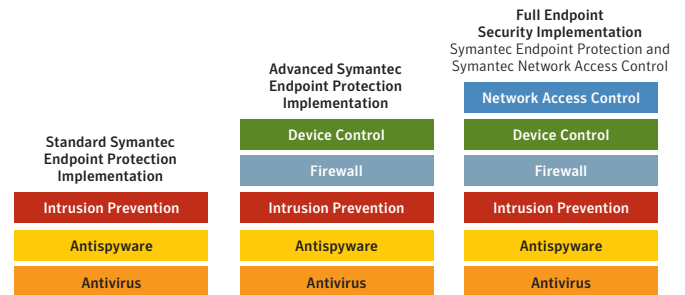


Figure 3. Symantec Endpoint Protection 11.0 can be configured to match individual customers' threat environment and business requirements.

### **Migration tools**

To help your customers secure full value from this new release, Symantec has developed tools and services that make it easy to deploy:

- **Management console installation wizard**

This step-by-step program speeds installation of the Symantec Endpoint Security Manager for centralized control and management of Symantec Endpoint Protection 11.0, and Symantec Network Access Control 11.0, if licensed.

- **Management console shares a server**

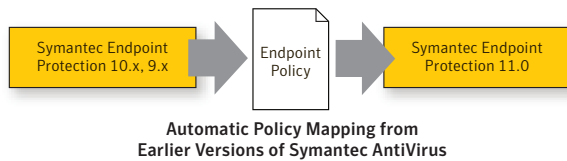
The new Symantec Endpoint Protection Manager can be installed on the same server as the Symantec System Center, or on a separate server if desired.

- **Automatic policy mapping**

To reduce IT overhead during migration from Symantec AntiVirus (versions 9.x and 10.x), the management console automatically maps their policies. An additional conversion tool helps move Group and Policy information

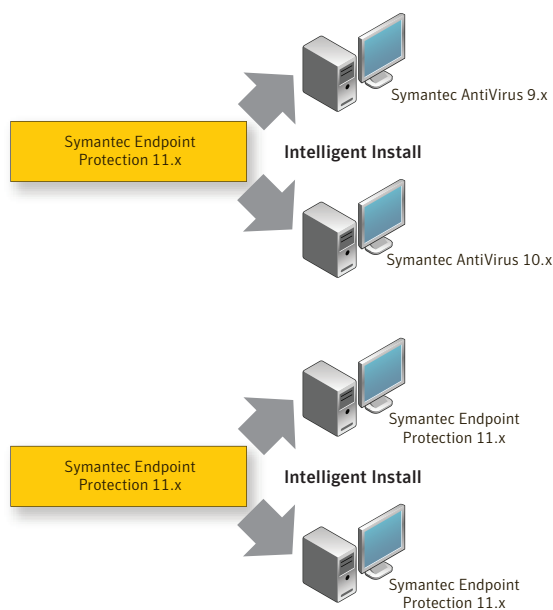
## Symantec Migration Guide Symantec Endpoint Protection 11.0

from Symantec System Center to Symantec Endpoint Security Manager.



### • Intelligent agent install

For speed and efficiency, the new client agent installs directly on top of the existing agent, with no need to remove the previous agent, and in most new installations, no need to reboot. The new agent connects automatically to the new management console.



### • Collects legacy data

The Symantec Endpoint Protection Manager can receive events and logs forwarded by legacy management servers, to maintain consistent monitoring of trends and gap-free reports.

### Documentation and resources

To these time-saving tools, Symantec adds online guides and tutorials to help you and your customer take advantage of these new, powerful security features and management tools:

[www.symantec.com/enterprise/support/index.jsp](http://www.symantec.com/enterprise/support/index.jsp)

For further assistance in making a smooth transition, Symantec Global Services offers a broad spectrum of services to assist with deployments so customers can focus on other business-critical projects:

[www.symantec.com/enterprise/products/category.jsp?pcid=1015](http://www.symantec.com/enterprise/products/category.jsp?pcid=1015)

### Endorsements

Here are even more reasons to implement Symantec Endpoint Protection 11.0:

- More than 30 consecutive VB 100 Certifications for Symantec AntiVirus



- Award-winning Symantec technology

Information Security/  
SearchSecurity.com

Redmond  
Magazine

Windows IT  
Pro 2006

Microsoft  
TechEd 2006



Symantec AntiVirus  
Corporate Edition

Symantec AntiVirus  
Corporate Edition

Symantec AntiVirus  
Corporate Edition

Symantec Client  
Security

- eWeek.com Channel Product of the year; Security Client Software (Symantec Client Security)



- CRN 2007 Channel Champions; Client Security Software (Symantec)

