

Symantec Endpoint Protection 11.x

COURSE DESCRIPTION

The *Symantec Endpoint Protection 11.x* course is designed for the network, IT security, and systems administration professional tasked with architecting, implementing, and monitoring antivirus and antispyware, and client firewall solutions. This class covers how to design, deploy, install, configure, and monitor Symantec Endpoint Protection (SEP).

Students also learn how to create and implement client firewall, intrusion prevention, and behavioral protection policies that guard the enterprise from viruses, hackers, and spam. In addition, students learn how to troubleshoot SEP managers and clients.

Delivery Method

Instructor-led

Duration

Five days

Course Objectives

By the end of this course, you should be able to:

- Describe the security threats facing today's enterprise customers and the solutions that Symantec offers to mitigate those risks.
- Describe SEP products, components, product dependencies and the system hierarchy.
- Install and configure SEP management and client components.
- Deploy SEP clients.
- Manage Antivirus and Antispyware policies.
- Configure Proactive Threat Protection.
- Design an Endpoint Protection deployment.
- Monitor and maintain the SEP environment.
- Configure Firewall and Intrusion Prevention policies.
- Customize Network Threat Protection.
- Manage the client UI.

Who Should Attend

This course is for network managers, resellers, systems administrators, client security administrators, systems professionals, and consultants who are charged with the installation, configuration, and day-to-day management of Symantec Endpoint Protection in a variety of network environments, and who are responsible for troubleshooting and tuning the performance of this product in the enterprise environment.

Prerequisites

You should have working knowledge of advanced computer terminology, including TCP/IP networking terms and Internet terms, and an administrator-level knowledge of Microsoft Windows 2000/XP/2003 operating systems.

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Introduction:

- Course Overview
- The Classroom Lab Environment

Lesson 1: Today's Security Landscape

- Security Risks
- Security Risk Management
- Managing and Protecting Systems
- Corporate Security Policies and Security Assessments

Lesson 2: The Symantec Endpoint Protection Product Solution

- Why Symantec Endpoint Protection?
- Symantec Endpoint Protection Technologies
- Symantec Endpoint Protection Components
- Symantec Endpoint Protection Policies and Concepts

Lesson 3: Installing Symantec Endpoint Protection

- Identifying Software Requirements
- Preparing Computers
- Installing the Symantec Endpoint Protection Manager
- Navigating the Symantec Endpoint Protection Manager

Lesson 4: Deploying Clients

- Preparing for Client Deployment
- Choosing the Client Installation Method
- Installing Clients
- Scanning Clients
- Managing the User Environment

Lesson 5: Installing Additional Management Components

- Configuring LiveUpdate Settings
- Configuring LiveUpdate Policies
- Installing LiveUpdate Servers
- Installing and Configuring the Central Quarantine
- Expanding the Management Environment

Lesson 6: Configuring Antivirus and Antispyware Policies

- Overview
- Configuring Administrator-Defined Scans
- Configuring Auto-Protect Scans
- Quarantining Files
- Configuring Miscellaneous Settings

Lesson 7: Configuring Additional Protection

- Configuring Proactive Threat Protection
- Configuring Tamper Protection
- Configuring Centralized Exceptions

Lesson 8: Monitoring Antivirus and Antispyware

- Viewing Summary Data
- Viewing and Managing Logs
- Viewing and Managing Notifications
- Creating and Viewing Reports

Lesson 9: Performing Server and Database Management

- Managing Symantec Endpoint Protection Manager Servers
- Managing Server Security
- Communicating with Other Servers
- Managing Administrators
- Managing the Database

Lesson 10: Designing an Endpoint Security Deployment

- Deployment Overview
- Assessing the Environment
- Determining the Architecture
- Testing the Deployment
- Completing the Deployment
- Example Deployments

Lesson 11: Introduction to Network Threat Protection and Application and Device Control

- Network Threat Protection Basics
- The Firewall
- Intrusion Prevention
- Application and Device Control

Lesson 12: Configuring Firewall Policies

- Firewall Policy Overview
- Defining Rule Components
- Modifying Firewall Rules
- Configuring Smart Traffic Filtering
- Configuring Traffic and Stealth Settings

Lesson 13: Managing Intrusion Prevention System (IPS) Policies

- Configuring Intrusion Prevention
- Managing Custom Signatures

Lesson 14: Configuring Application and Device Control

- Creating Application and Device Control Policies
- Defining Application Control
- Modifying Policy Rules
- Defining Device Control

Lesson 15: Customizing Network Threat Protection and Application and Device Control

- Managing Locations
- Managing Policy Components
- Configuring Learned Applications
- Configuring System Lockdown

Lesson 16: Monitoring Network Threat Protection and Application and Device Control

- Viewing Summary Data
- Viewing and Managing Logs
- Creating and Viewing Reports