Symantec Endpoint Protection 14.x: Configure and Protect

Category: Networking & Security | **Vendor:** Symantec

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Prerequisites & Entry Requirements

General Prerequisites:

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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

By the completion of this course, you will be able to:

- Secure endpoints against network and filebased threats
- Control endpoint integrity and compliance
- Enforce adaptive security posture

Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14

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

Detailed Course Outline

Introduction

- Course environment
- Lab environment

Securing Endpoints against Network-Based Attacks

Introducing Network Threats

- Describing how Symantec Endpoint Protection protects each layer of the network stack
- Discovering the tools and methods used by attackers

- Describing the stages of an attack
- Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
- Preventing network attacks
- Examining Firewall Policy elements
- Evaluating built-in rules
- Creating custom firewall rules
- Enforcing corporate security policy with firewall rules
- Blocking network attacks using protection and stealth settings
- Configuring advanced firewall feature
- Blocking Threats with Intrusion Prevention
- Introducing Intrusion Prevention technologies
- Configuring the Intrusion Prevention policy
- Managing custom signatures
- Monitoring Intrusion Prevention events

Securing Endpoints against File-Based Threats

Introducing File-Based Threats

- Describing threat types
- Discovering how attackers disguise their malicious applications
- Describing threat vectors
- Describing Advanced Persistent Threats and a typical attack scenario
- Following security best practices to reduce risks Preventing Attacks with SEP Layered Security
- Virus and Spyware protection needs and solutions
- Describing how Symantec Endpoint Protection protects each layer of the network stack
- Examining file reputation scoring
- Describing how SEP protects against zero-day threats and threats downloaded through files and email
- Describing how endpoints are protected with the Intelligent Threat Cloud Service
- Describing how the emulator executes a file in a sandbox and the machine learning engine’s role and function

Securing Windows Clients

- Platform and Virus and Spyware Protection policy overview
- Tailoring scans to meet an environment’s needs
- Ensuring real-time protection for clients
- Detecting and remediating risks in downloaded files
- Identifying zero-day and unknown threats
- Preventing email from downloading malware
- Configuring advanced options
- Monitoring virus and spyware activity

Securing Mac Clients

- Touring the SEP for Mac client
- Securing Mac clients
- Monitoring Mac clients

Securing Linux Clients

- Navigating the Linux client
- Tailoring Virus and Spyware settings for Linux clients
- Monitoring Linux clients

Controlling endpoint integrity and compliance

Providing Granular Control with Host Integrity

- Ensuring client compliance with Host Integrity

- Configuring Host Integrity

- Troubleshooting Host Integrity

- Monitoring Host Integrity

Controlling Application and File Access

- Describing Application Control and concepts

- Creating application rulesets to restrict how applications run

- Monitoring Application Control events

Restricting Device Access for Windows and Mac Clients

- Describing Device Control features and concepts for Windows and Mac clients

- Enforcing access to hardware using Device Control

- Discovering hardware access policy violations with reports, logs, and notifications

Hardening Clients with System Lockdown

- What is System Lockdown?

- Determining to use System Lockdown in Whitelist or Blacklist mode

- Creating whitelists for blacklists

- Protecting clients by testing and Implementing System Lockdown.

- Enforcing Adaptive Security Posture

- Customizing Policies based on Location

- Creating locations to ensure the appropriate level of security when logging on remotely

- Determining the criteria and order of assessment before assigning policies

- Assigning policies to locations

Managing Security Exceptions

- Creating file and folder exceptions for different scan types
- Describing the automatic exclusion created during installation
- Managing Windows and Mac exclusions
- Monitoring security exceptions

Skills You Will Learn:

By the completion of this course, you will be able to:

- Secure endpoints against network and filebased threats
- Control endpoint integrity and compliance
- Enforce adaptive security posture
Network, IT security, and systems administration professionals in a Security Operations position who are tasked with configuring optimum security settings for endpoints protected by Symantec Endpoint Protection 14

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

Frequently Asked Questions

Q: What delivery options are available for Symantec Endpoint Protection 14.x: Configure and Protect?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Symantec Endpoint Protection 14.x: Configure and Protect course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Symantec Endpoint Protection 14.x: Configure and Protect training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Symantec Endpoint Protection 14.x: Configure and Protect?

Yes, we provide corporate training, dedicated training, and closed classes for Symantec Endpoint Protection 14.x: Configure and Protect. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Symantec Endpoint Protection 14.x: Configure and Protect, Endpoint Security, SEPCP

Q: Why choose Nexus Human for Symantec Endpoint Protection 14.x: Configure and Protect?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Symantec Endpoint Protection 14.x: Configure and Protect training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.