

SOPHOS ENDPOINT ARCHITECT

COURSE OVERVIEW

This course provides an in depth study of Sophos Endpoint, designed for experienced technical professionals who will be planning, installing, configuring, and supporting deployments in production environments.

DELIVERY

This course is available online via the Training Portal, or as an instructor-led classroom course. Please contact your Sophos Partner to find out more about the availability of classroom training in your region. Electronic copies of the supporting documents for the course are provided to each trainee via the training portal.

DURATION

This course will take approximately **3 days (24 hours)** to complete.

ASSESSMENT

To complete this course, trainees must take and pass an online assessment. Trainees will have **3 hours** to complete the assessment; the pass mark is **80%** and trainees will have **3 attempts** to pass.

OBJECTIVES

On completion of this course, trainees will be able to:

- Plan and deploy complex installations of Sophos Endpoint
- Explain the core configuration concepts of Sophos Endpoint and demonstrate how to configure and implement them
- Perform manual cleanup of threats
- Proactively investigate suspicious activities
- Perform preliminary troubleshooting and basic support steps

PREREQUISITES

Prior to taking this training, trainees must:

- Have completed and passed the **Sophos Endpoint Certified Engineer** course
- Have completed any subsequent **delta courses** up to **version 6.0**

We also recommend that trainees have the following knowledge and experience:

- Windows networking and the ability to troubleshoot issues
- A good understanding of IT security
- Linux command line from common tasks
- Configuring Active Directory group policies

If you are uncertain whether you meet the necessary requirements, please email us at globaltraining@sophos.com and we will be happy to help.

COURSE AGENDA

Module	Chapter	Duration
1. User Management		
Chapters	<ul style="list-style-type: none"> Role-based User Access Advanced Directory Synchronization in Sophos Central Configuring Federated Authentication in Sophos Central 	20 minutes
Lab Tasks	Lab Preparation <ul style="list-style-type: none"> Register for a Sophos Central Trial User Management <ul style="list-style-type: none"> Install and Configure AD Sync Utility Configure role-based User Access 	35 minutes
2. Sophos Endpoint Agent Deployment		
Chapters	<ul style="list-style-type: none"> Sophos Endpoint Agent Deployment Strategy Automating Sophos Endpoint Agent Deployment on Windows Automating Sophos Endpoint Agent Deployment on macOS Automating Sophos Endpoint Agent Deployment on Linux 	25 minutes
Lab Tasks	Preparation <ul style="list-style-type: none"> Install Sophos Endpoint on a Windows Server Deploy an Update Cache and Message Relay Sophos Endpoint Agent Deployment <ul style="list-style-type: none"> Install Sophos Endpoint on Linux Use AD GPO to deploy multiple Window devices 	80 minutes
3. Updating and Communication		
Chapters	<ul style="list-style-type: none"> Advanced Sophos Endpoint Updating Controlling Sophos Endpoint Updates Considerations when using Sophos Endpoint Update Cache and Message Relays Advanced Update Cache and Message Relays 	20 minutes
4. Virtual Protection		
Chapters	<ul style="list-style-type: none"> Protecting Azure Hosted Virtual Servers Protecting AWS Hosted Virtual Servers 	15 minutes
5. Device Management		
Chapters	<ul style="list-style-type: none"> Managing Server Protection for Linux 	10 minutes
Lab Tasks	<ul style="list-style-type: none"> Create Server Groups Manage Tamper Protection 	15 minutes

6. Policies		
Chapters	<ul style="list-style-type: none"> Advanced Sophos Endpoint Control Policies Advanced Sophos Endpoint Data Loss Prevention Advanced Sophos Endpoint Policies and Exclusions Getting Started with Partner Global Policies Getting Started with Server File Integrity Monitoring 	70 minutes
Lab Tasks	<p>Investigation Preparation</p> <ul style="list-style-type: none"> Preparation for a later lab task <p>Policies</p> <ul style="list-style-type: none"> Configure and Test Threat Protection Policies Configure and Test Web Control Configure and Test Application Control Configure and Test DLP using CCLs Configure and Test Exclusions Test Linux Server Protection 	90 minutes
7. Remediation and Reports		
Chapters	<ul style="list-style-type: none"> Getting Started with SIEM Integration with Sophos Central Linux Server Protection Threat Detection and Remediation Advanced Sophos Endpoint Threat Remediation Getting Started with Sophos Endpoint Forensic Snapshots 	25 minutes
Lab Tasks	<ul style="list-style-type: none"> Configure SIEM with Splunk Release a File from SafeStore Remediate a Linux Server Create a Forensic Snapshot and Interrogate the Database 	95 minutes
8. Detection and Response		
Chapters	<ul style="list-style-type: none"> Sophos APIs 	30 minutes
Lab Tasks	<ul style="list-style-type: none"> Use Data Lake Search to locate unauthorized software Investigate a Detection 	40 minutes
9. Course Review		
Chapters	<ul style="list-style-type: none"> How to Find Help from Sophos Course Review 	10 minutes

FURTHER INFORMATION

If you require any further information on this course, please contact us at globaltraining@sophos.com