



Authorized Training Center

Trend Micro APEX ONE™ TRAINING FOR CERTIFIED PROFESSIONALS Course Outline

Course Title	Trend Micro Apex One Training for Certified Professionals
Course Length	Three Days
Level	Professional
Delivery Language	English

Course Description

In this course, you will learn how to use Trend Micro Apex One™ as a Service—detailing basic architecture, Security Agent management, protection functionality, and policy deployment.

Through hands-on labs, participants practice configuring Trend Micro Apex One™ protection features along with the administration options needed for a successful deployment.

Taught by Trend Micro certified trainers, this course incorporates a variety of practical lab exercises, allowing participants to put the lesson content into action.

Target Audience

This course is designed for IT professionals responsible for protecting endpoint computers from data breaches and targeted attacks.

This includes those involved with:

- Operations
- Deployment
- Security Response
- Compliance

Course Prerequisites

There are no prerequisites to attend this course, however, a working knowledge of Trend Micro products and services, as well as an understanding of basic networking concepts and principles will be helpful.

Basic knowledge of the following topics is also beneficial:

- Windows® servers and clients
- Microsoft® Internet Information Server (IIS)
- General understanding of malware

Participants are required to bring a laptop computer with a recommended screen resolution of at least 1980 x 1080 or above, and a display size of 15" or above.

Course Objectives

After completing this course, participants will be able to:

- Describe the purpose, features, functions, and capabilities of Apex One
- Define the components that make up Apex One
- Implement security using Security Agents
- Configure and administer Apex One Servers and Agents
- Deploy Apex One policies using Trend Micro Apex Central
- Troubleshoot common issues
- Attempt the Trend Micro Certified Professional for Apex One Certification Exam

Course Outline

The course topics in this training are divided into the following lessons:

Trend Micro Apex One Overview

- Trend Micro solutions
- Key features of Apex One
- Apex One as a Service components
- Deployment methods
- Threat detection

Managing Apex One as a Service

- Trend Micro Apex Central™ server tasks
- Apex One server tasks
- Logging into the management consoles
- Integrating with Active Directory
- Creating new administrative accounts
- Apex Central management modes

Managing Security Agents

- Security Agent tasks
- Security Agent services and components
- Security Agent requirements
- Installing/uninstalling Agents
- Migrating from other endpoint security software
- Agent-to-server communication
- Endpoint location
- Agent self-protection
- Security Agent tree

Deploying Policies

- Identifying policy targets
- Defining policy settings
- Policy inheritance

Keeping Security Agent Up to Date

- Pattern updates
- Updating managed products
- Updating Security Agents
- Update Agents

Trend Micro™ Smart Protection

- Smart Protection services

Protecting Endpoint Computers from Malware

- Scanning for malware
- Scan settings
- Quarantining malware
- Trend Micro™ Smart Scan™
- Spyware/Grayware protection
- Preventing outbreaks

Protecting Endpoint Computers Through Behavior Monitoring

- Malware behavior blocking
- Ransomware protection
- Anti-exploit protection
- Fileless malware protection
- Newly encountered program detection
- Event monitoring
- Behavior monitoring exceptions

Protecting Endpoint Computers from Unknown Threats

- Common vulnerabilities and exposures exploits
- Predictive machine learning
- Offline predictive machine learning

Blocking Web Threats

- Web reputation
- Detecting suspicious connections
- Protecting against browser exploits

Protecting Endpoint Computers Through Traffic Filtering

- Firewall filtering
- Application filtering
- Certified Safe Software list
- Stateful inspection
- Intrusion detection system
- Firewall policies and profiles

Blocking Unapproved Applications on Endpoint Computers

- Integrated Application Control
- Lockdown mode
- Application Control criteria
- Implementing Application Control
- User-based Application Control
- Best practices

Protecting Endpoint Computers from Vulnerabilities

- Integrated Trend Micro™ Vulnerability Protection™
- Vulnerability Protection pattern
- Selecting a priority mode
- Network engine settings

Preventing Data Loss on Endpoint Computers

- Digital asset control
- Configuring data identifiers, data loss prevention templates, and policies
- Data discovery
- Device control

Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense™

- Connected Threat Defense phases
- Connected Threat Defense requirements
- Cloud sandbox
- Suspicious objects
- Enabling sample submission
- Viewing suspicious objects

Detecting and Investigating Security Incidents on Endpoint Computers

- Integrated Endpoint Sensor
- Endpoint detection and response (EDR)
- Apex One incident response model
- Managed detection and response (MDR)