

# Trend Micro Apex One SaaS Training for Certified Professionals

In diesem Kurs lernen Sie die Verwendung von Trend Micro Apex One™ as a Service kennen - mit Details zur grundlegenden Architektur, zur Verwaltung von Sicherheitsagenten, zur Schutzfunktionalität und zur Bereitstellung von Richtlinien. In praktischen Übungen lernen die Teilnehmer, die Sicherheitsfunktionen von Trend Micro Apex One™ zu konfigurieren und die Verwaltungsoptionen zu nutzen, die für eine erfolgreiche Bereitstellung erforderlich sind. Dieser Kurs beinhaltet eine Vielzahl praktischer Laborübungen, die es den Teilnehmern ermöglichen, die Lerninhalte in die Praxis umzusetzen.

## Kursinhalt

- Trend Micro Apex One Overview
- Managing Apex One as a Service
- Managing Security Agents
- Deploying Policies
- Keeping Security Agent Up to Date
- Trend Micro™ Smart Protection
- Protecting Endpoint Computers from Malware
- Protecting Endpoint Computers Through Behavior Monitoring
- Protecting Endpoint Computers from Unknown Threats
- Protecting Endpoint Computers Through Traffic Filtering
- Blocking Unapproved Applications on Endpoint Computers
- Protecting Endpoint Computers from Vulnerabilities
- Vulnerability Protection™
- Preventing Data Loss on Endpoint Computers
- Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense™
- Detecting and Investigating Security Incidents on Endpoint Computers

**E-Book** Sie erhalten ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

## Zielgruppe

Dieser Kurs richtet sich an IT-Experten, die für den Schutz von Endpoint-Computern vor Datenmissbrauch und gezielten Angriffen verantwortlich sind.

Dies betrifft u. a. die folgenden Bereiche:

- Operations
- Deployment
- Security Response
- Compliance

## Voraussetzungen

Es gibt keine Voraussetzungen für die Teilnahme an diesem Kurs, jedoch sind Grundkenntnisse der Produkte und Dienstleistungen von Trend Micro sowie ein Verständnis der grundlegenden Netzwerkkonzepte und -prinzipien hilfreich.

Grundkenntnisse in den folgenden Themen sind ebenfalls von Vorteil:

- Windows® and Mac clients
- Malware
- Cloud technologies

## Kursziel

Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional Apex One ablegen. Die Prüfung ist im Kurspreis inkludiert.

Für die Registrierung zum Examen wird ein Account im Trend Micro Education Portal benötigt.

## Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/TMAS](http://www.experteach.at/go/TMAS)

## Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

## Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

## Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
<b>Termine in Österreich</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
<b>Online Training</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
Termine auf Anfrage		

Stand 24.01.2025



# Inhaltsverzeichnis

## Trend Micro Apex One SaaS Training for Certified Professionals

### 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
- 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)

