



---

## Deep Security Training for Certified Professionals

**Duration: 3 Days**    **Course Code: TMDS**

---

### Overview:

Trend Micro™ Deep Security™ 12 Training for Certified Professionals is a three-day, instructor-led training course. Participants will learn how to use Trend Micro Deep Security for advanced hybrid-cloud security on physical, virtual, and cloud-based servers. This course details the basic architecture of the Deep Security solution, deployment options, protection modules, policy configuration, and administration of the system. As part of the course, participants will deploy Deep Security Agents on a variety of Windows Server platforms, as well as the Deep Security Virtual Appliance. Best practices and troubleshooting details for successful implementation and long-term maintenance of the system are discussed. This course incorporates a variety of hands-on lab exercises, allowing participants to put the lesson content into action. This course is taught by Trend Micro certified trainers. Upon completion of this course, participants may complete the certification examination to obtain designation as a Trend Micro Certified Professional for Deep Security.

---

### Target Audience:

This course is designed for IT professionals who are responsible for protecting users, networks, data centers, and cloud resources from data breaches and targeted attacks.

This includes those responsible for:

- Operations
- Deployment
- Security Response
- Compliance
- Support

---

### Objectives:

- After completing this training course, participants will be able to:
    - Describe available configuration and administration options
  - Describe the purpose, features, functions, and capabilities of Trend Micro Deep Security 12
    - Attempt the Trend Micro Certified Professional for Deep Security
  - Define and install components that make up Deep Security
    - Certification Exam
  - Implement security by enabling protection modules
- 

### 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

Firewalls and packet inspection devices

VMware® ESXi/vCenter/NSX

Amazon AWS/Microsoft® Azure™/VMware vCloud

---

## Virtualization technologies

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.

---

## Content:

Product Overview :	Setting the security level	Event tagging
Introduction to Deep Security	Filtering Traffic Using the Firewall :	Reporting
Deep Security protection modules	Enabling the Deep Security firewall	Protecting Containers :
Deep Security deployment options	Firewall rules	Continuous integration/continuous deployment
Deep Security components	Traffic analysis	Software development using containers
Trend Micro™ Deep Security™ Manager :	Traffic order of analysis	Protecting containers with Deep Security
Server, operating system, and database requirements	Port scan	Automating Deep Security Operations :
Deep Security Manager architecture	Protecting Servers from Vulnerabilities :	Scheduled tasks
Installing and upgrading Deep Security Manager	Virtual patching	Event-based tasks
Deep Security Agents :	Protocol hygiene	Quick start templates
Deep Security Agent architecture	Protocol control	Baking the Deep Security Agent into an
Deploying Deep Security Agents	Web application protection	Amazon® machine image
Viewing computer protection status	Enabling intrusion prevention	Application programming interface
Upgrading Deep Security Agents	Running recommendation scans	Activating and Managing Multiple Tenants :
Organizing computers using groups and	Intrusion prevention rules	Segmentation using multi-tenancy
Smart Folders	Security Sockets Layer (SSL) filtering	Enabling multi-tenancy
Keeping Deep Security Up to Date :	Protecting web applications	Creating and managing tenants
Security updates	Detecting Changes to Protected Servers :	Activating Deep Security Agents on tenants
Software updates	Enabling integrity monitoring	Usage monitoring
Deep Security relays	Running recommendation scans	Detecting Emerging Malware Through :
Trend Micro™ Smart Protection™ :	Detection changes to baseline objects	Connected Threat Defense

Smart Protection services used by	Blocking Unapproved Software :	Connected Threat Defense phases
Deep Security	Enforcement modes	Trend Micro™ Deep Discovery™ Analyzer
Configuring the Smart Protection source	Enabling application control	Trend Micro Apex Central™
Policies :	Detecting software changes	Configuring Deep Security for Connected
Policy inheritance and overrides	Creating an inventory of approved software	Threat Defense
Creating new policies	Pre-approving software changes	Tracking submission
Protecting Servers from Malware :	Inspecting Logs on Protected Servers :	Protecting Virtual Machines Using the Deep Security Virtual Appliance :
Anti-malware scanning techniques	Enabling log inspection	Deep Security Virtual Appliance
Enabling anti-malware protection	Running recommendation scans	Virtual Appliance deployment models
Smart Scan	Events and Alerts :	Virtual appliance deployment and activation
Blocking Malicious Websites :	Event forwarding	
Enabling web reputation	Alerts	

## Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

[training@globalknowledge.com.sa](mailto:training@globalknowledge.com.sa)

[www.globalknowledge.com/en-sa/](http://www.globalknowledge.com/en-sa/)

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia