Trend Micro™

DEEP SECURITY™

Complete security for physical, virtual, cloud, and hybrid environments

Virtualization has already transformed the data center and now, organizations are moving some or all of their workloads to private and public clouds. If you're interested in taking advantage of the benefits of hybrid cloud computing, you need to ensure you have security built to protect all of your servers, whether physical, virtual, or cloud.

In addition, your security should not hinder host performance and virtual machine (VM) density or the return on investment (ROI) of virtualization and cloud computing. Trend Micro™ Deep Security™ provides comprehensive security in one solution that is purpose-built for virtualized and cloud environments so there are no security gaps or performance impacts.

BE POWERFUL

Protect against vulnerabilities, malware and unauthorized change with the broadest range of security capabilities

GET STREAMLINED

Consistent protection and visibility, optimized for every part of your hybrid cloud

GO AUTOMATED

Connected security that can be integrated into Dev and Ops processes to ensure adoption

BUILD SECURE

Smart security controls that ensure you meet security and compliance requirements from the first build

SHIP FAST

Security that is connected through automation and integration in your CI/CD pipeline

RUN ANYWHERE

Security that is optimized for the place that best suits your application

Key Business Issues

Virtual Desktop Security
Preserve performance and consolidation ratios with comprehensive security built specifically to maximize protection for VDI environments

Virtual patching
Shield vulnerabilities before they can be exploited, eliminating the operational pains of emergency patching, frequent patch cycles, and costly system downtime

Compliance
Demonstrate compliance with a number of regulatory requirements including PCI DSS, HIPAA, NIST, SSAE 16, and more

Security for the CI/CD pipeline
API-first, developer-friendly tools to help you ensure that security is baked into DevOps processes

TRUSTED HYBRID CLOUD SECURITY

Virtualization security

Deep Security protects virtual desktops and servers against zero-day malware, including ransomware, and network-based attacks while minimizing operational impact from resource inefficiencies and emergency patching.

Cloud security

Deep Security enables service providers and modern data center managers to offer a secure multi-tenant cloud environment with security policies that can be extended to cloud workloads and managed centrally with consistent, context-aware policies.

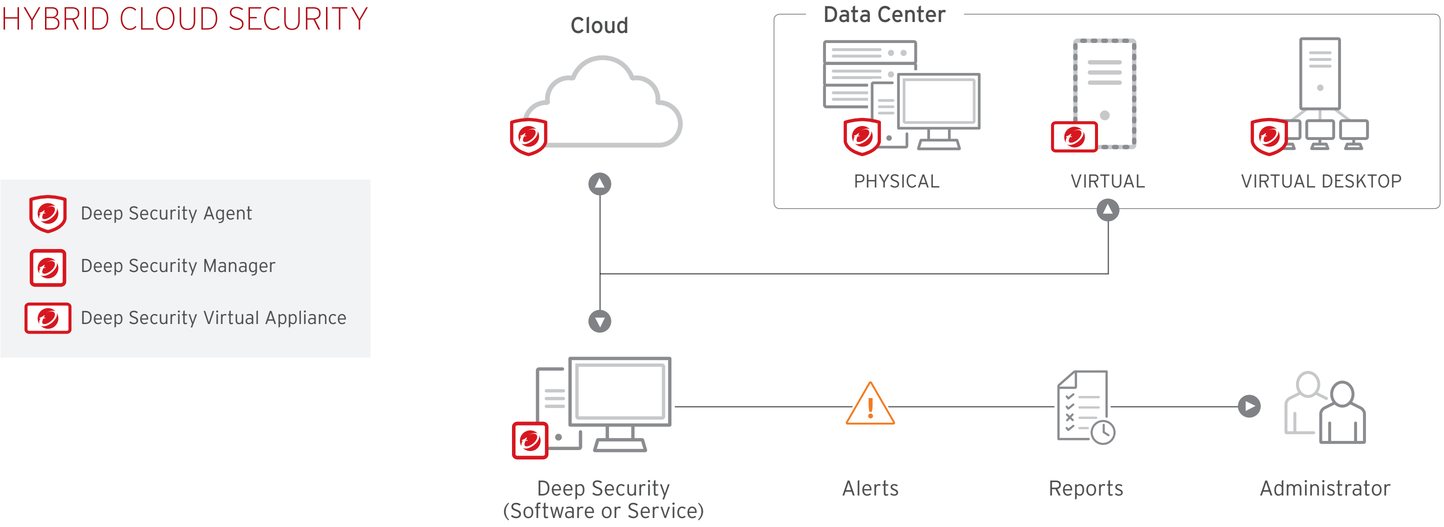
Integrated server security

Deep Security consolidates all server security functions into one comprehensive, integrated, and flexible platform that optimizes protection across physical, virtual, cloud, and container environments.

Container security

Deep Security works seamlessly in the cloud to protect not only your workloads but your containers as well. Designed with API-first integrations, IT Security can protect cloud environments with automated processes for critical security controls to protect containers and the Docker host. Bake security into the CI/CD pipeline for frictionless automation.

HYBRID CLOUD SECURITY



KEY ADVANTAGES

Effective and efficient

- Yields more efficient resource utilization and management with higher VM densities than traditional anti-malware solutions
- Adds flexibility and defense-in-depth capabilities as a single, easy-to-manage multi-function security agent
- Delivers unparalleled performance via hypervisor-level scanning deduplication
- Integrates with cloud platforms including AWS, Microsoft Azure, and VMware Cloud, enabling organizations to manage their physical, virtual, and cloud servers with consistent and context-aware security policies
- Enables service providers to offer customers a secure public cloud, isolated from other tenants via multi-tenant architecture
- Provides auto-scaling, utility computing, and self-service to support agile organizations running a software-defined data center
- Leverages Deep Security's tight integration with VMware to automatically detect new VMs and apply context-based policies for consistent security across the data center and cloud
- Integrates with the latest VMware vSphere and NSX™ versions. Deep Security extends the benefits of micro-segmentation in the software-defined data center with security policies and capabilities that automatically follow VMs no matter where they go

Prevent data breaches and business disruptions

- Prevents unknown applications from running on your most critical servers
- Detects and removes malware from virtual servers in real time with minimal performance impact
- Detects and blocks unauthorized software with multi-platform application control
- Shields known and unknown vulnerabilities in web and enterprise applications and operating systems
- Delivers advanced threat detection and remediation of suspicious objects through sandbox analysis
- Sends alerts and triggers proactive prevention upon detection of suspicious or malicious activity
- Tracks website credibility and protects users from infected sites with web reputation threat intelligence from Trend Micro's global domain-reputation database
- Identifies and blocks botnet and targeted attack command and control (C&C) communications using unified threat intelligence from Trend Micro's global domain-reputation database

Maximize operational cost reductions

- Eliminates the cost of deploying multiple software clients with a centrally managed, multi-purpose software agent or virtual appliance
- Reduces complexity with tight integrations with management consoles from Trend Micro, VMware, and enterprise directories such as VMware vRealize Operations, Splunk, HP ArcSight, and IBM QRadar
- Protects Docker host and containers with Anti-Malware scans and Intrusion Protection
- Reduces management costs by automating repetitive and resource-intensive security tasks, reducing false-positive security alerts, and enabling workflow of security incident response
- Significantly reduces the complexity of managing file-integrity monitoring with cloud-based event whitelisting and trusted events
- Detects vulnerabilities and software via Recommendation Scanning to detect changes and provide protection from vulnerabilities
- Ensures improved operational efficiency with a lighter, more dynamic smart agent that eases deployment to maximize resource allocation across the data center and cloud
- Matches security to your policy needs so fewer resources need to be dedicated to specific security controls
- Simplifies administration with centralized management across Trend Micro security products. Centralized reporting of multiple security controls reduces the challenge of creating reports for individual products

Achieve cost-effective compliance

- Addresses major compliance requirements for PCI DSS, as well as HIPAA, SSAE 16, and more with one integrated and cost-effective solution
- Provides audit reports that document prevented attacks and compliance policy status
- Reduces the preparation time and effort required to support audits
- Supports internal compliance initiatives to increase visibility of internal network activity
- Enhanced file integrity monitoring to help consolidate tools for meeting compliance requirements
- Leverages proven technology certified to Common Criteria EAL

DEEP SECURITY CAPABILITIES

Network Security tools stop network attacks and shield vulnerable applications and servers

- Host-Based Intrusion Prevention: Blocks network-based exploits of known vulnerabilities in popular applications and operating systems using intrusion prevention (IPS) rules
- Web Reputation: Blocks known-bad URLs and websites
- Firewall: Host-based firewall protects endpoints on the network using stateful inspection
- Vulnerability Scanning: Performs a scan for known network-based vulnerabilities in the operating system and applications

System Security tools lock down systems and detect suspicious activity

- Application Control: Blocks any executables (and scripts) that aren't identified as known-good applications or DLLs from installing/executing
- File Integrity Monitoring: Monitor files, libraries and services, etc. for changes. To monitor a secure configuration, a baseline is created that represents the secure configuration. When changes from this desired state are detected, details are logged and alerts can be issued to stakeholders
- Log Inspection: Identify and alert on unplanned changes, intrusions, or advanced malware attacks; including ransomware as they are happening on your systems

Malware Prevention stops malware and targeted attacks

- Anti-Malware:
  i. File Reputation: Blocks known-bad files using our antimalware signatures
  ii. Variant Protection: Looks for obfuscated, polymorphic or variants of malware by using fragments of previously seen malware and detection algorithms
- Behavioral Analysis: Examines an unknown item as it loads and looks for suspicious behavior in the operating system, applications, scripts - and how they interact to block them
- Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious
- Sandbox Analysis: Suspicious objects can be sent to the Deep Discovery™ network sandbox for detonation and extensive analysis to determine if it is malicious. Confirmation and a rapid response update is then provided back to Deep Security for the appropriate response

BUILT FOR SECURITY IN THE CLOUD

Trend Micro Deep Security as a Service is optimized for leading cloud providers' infrastructures, including support of the most common operating systems:

Linux Windows SUSE redhat CentOS ubuntu

And compatibility with configuration and event management tools:

CHEF puppet labs OpsWorks SALTSTACK splunk> sumologic ANSIBLE

ARCHITECTURE

Deep Security Virtual Appliance. Transparently enforces security policies on VMware vSphere virtual machines. For VMware NSX environments, this provides agentless anti-malware, web reputation, intrusion prevention, integrity monitoring, and firewall protection. Combined mode can be used where the virtual appliance is used for agentless anti-malware and integrity monitoring and an agent for intrusion prevention, application control, firewall, web reputation, and log inspection.

Deep Security Agent. Enforces the data center's security policy (application control, anti-malware, intrusion prevention, firewall, integrity monitoring, and log inspection) via a small software component deployed on the server or virtual machine being protected (can be automatically deployed with leading operational management tools like Chef, Puppet, and AWS OpsWorks).

Deep Security Manager. Powerful, centralized management console: role-based administration and multi-level policy inheritance allows for granular control. Task-automating features such as Recommendation Scan and Event Tagging and event-based tasks simplify ongoing security administration. Multi-tenant architecture enables isolation of individual tenant policies and delegation of security management to tenant admins.

Global Threat Intelligence. Deep Security integrates with the Smart Protection Network to deliver real-time protection from emerging threats by continuously evaluating and correlating global threat and reputation intelligence for websites, email sources, and files.

The Deep Security Scanner is a module that integrates with and protects SAP systems by integrating with the NetWeaver Virus Scan interface systems.

SAP Partner

Certification for CSPs

Trend Ready for Cloud Service Providers is a global validation testing program designed for Cloud Service Providers (CSPs) to prove interoperability with industry-leading cloud security solutions from Trend Micro.

SYSTEM REQUIREMENTS (SAAS, MANAGER, VIRTUAL APPLIANCE, AND AGENTS)

- Deep Security is available as a service (SaaS) and all management components are hosted and maintained by Trend Micro
- Deep Security is also available as a software or a virtual appliance to run in your data center or cloud. System requirements are available at the following URL: https://help.deepsecurity.trendmicro.com/11_0/on-premise/Get-Started/Install/system-requirements.html

SUPPORTED PLATFORMS (FOR AGENT)

- As Trend Micro is constantly supporting new operating systems and versions, please refer to the following URL for the complete list including Microsoft® Windows®, Linux®, Solaris, AIX, and Docker containers: https://help.deepsecurity.trendmicro.com/11_0/on-premise/Manage-Components/Software-Updates/compatibility.html

DEEP SECURITY AS A SERVICE (SAAS)

Deep Security as a Service gives you the proven protection of Deep Security without all the work. As a service deployment, we do the heavy lifting for you. We manage regular product and kernel updates, set up and maintain the security database, and administer the Deep Security manager. Our cloud-based security offering enables quick setup, and automates and simplifies security operations for cloud instances.

Key Benefits

- **Fast**: Start securing workloads in minutes
- **Cost-effective**: Usage-based pricing starting at $0.01 / hour
- **Simple**: Multiple security controls in a single product
- **Saves Time**: We manage and update the product so you can focus on your business
- **Proven**: Protects thousands of customers and millions of servers globally
- **Flexible**: Purchase and procure through AWS and Azure Marketplaces to protect multicloud environments

Flexible pricing to meet cloud needs

Deep Security as a Service usage-based pricing:

AWS EC2 INSTANCE SIZE	MICROSOFT AZURE VIRTUAL MACHINE	HOURLY PRICE (USD)
Micro, small, medium	1 Core: A0, A1, D1	$0.01
Large	2 cores: A2, D2, D11, G1	$0.03
XLarge and above	4+ cores: A3-A11, D3-D4, D12-D14, G2-G5, D3, D4, D12-D14, G2-G5	$0.06

POWERED BY XGEN™ SECURITY

Deep Security is part of the Trend Micro Hybrid Cloud Security solution, powered by XGen™.

POWERED BY XGen™ SECURITY

Key certifications and alliances

- Amazon Advanced Technology Partner
- Certified Red Hat Ready
- Cisco UCS validated
- Common Criteria EAL 2+
- EMC VSPEX validated
- HP Business Partnership
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- NetApp FlexPod validated
- Oracle Partnership
- PCI Suitability Testing for HIPS (NSS Labs)
- SAP Certified (NW-VSI 2.0 and HANA)
- VCE Vblock validated
- Virtualization by VMware
- FIPS 140-2 validated
- VMware Cloud on AWS

aws marketplace

Azure

vmware®

TREND MICRO TREND READY

TREND MICRO™

Securing Your Connected World