Trend Micro™

DEEP SECURITY™

Comprehensive 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.

Protection from data breaches and business disruptions

Deep Security—available as software, Amazon Web Services (AWS) or Microsoft® Azure™ offerings, or as-a-service—is designed to protect your data center and cloud workloads from data breaches and business disruptions. Deep Security helps you achieve compliance by closing gaps in protection efficiently and economically across hybrid cloud environments.

Multiple security controls managed from a single dashboard

Deep Security features integrated modules including anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, application control, and log inspection to ensure server, application, and data security across physical, virtual, and cloud environments. Deep Security can be deployed as a single, multifunction agent across all environments and simplifies security operations with a single management dashboard for all capabilities. You can use Trend Micro Control Manager as your dashboard, or a third-party system such as VMware vRealize Operations, Splunk, HP ArcSight, or IBM QRadar.

Seamless integration extends policies across cloud environments.

Deep Security seamlessly integrates with cloud platforms including AWS, Azure, and VMware® workloads enabling you to extend data center security policies to cloud-based workloads. With a wide range of capabilities optimized across environments, Deep Security empowers enterprises and service providers to offer a differentiated and secure multi-tenant cloud environment to their users.

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

> "Deep Security also allowed us to eliminate another antivirus solution on our servers... It had consumed a large amount of memory, and generated a lot of CPU churning due to the scans. We haven't had any of those problems with Deep Security."
>
> **Blaine Isbelle**
> Systems Administrator
> Information Services Technology
> University of California at Berkeley

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.

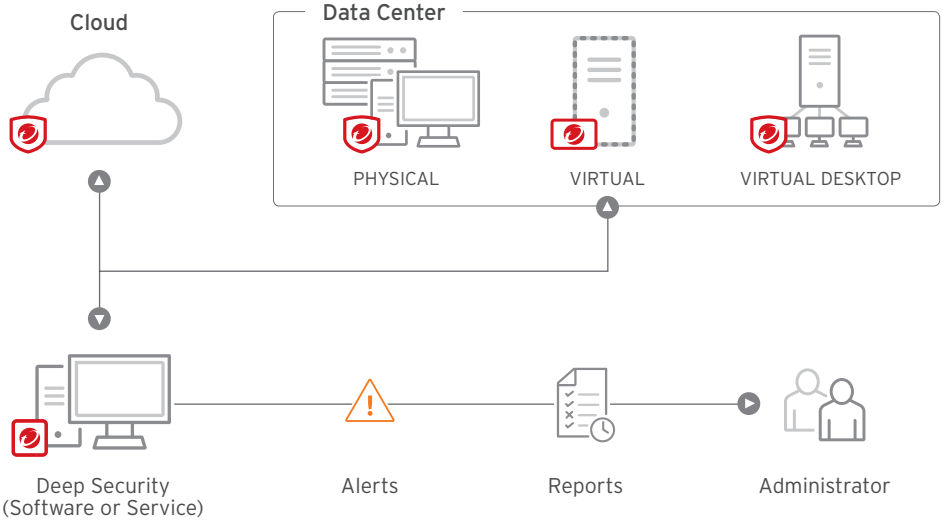
Cloud security

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, and cloud servers.

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 vCloud Air, 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 VMware vSphere 6 and NSX™. 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 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 containers on a host across all of their environments by applying pre-defined policies to the host in order to secure them
- Provides vulnerability shielding to allow secure coding and cost-effective implementation of unscheduled patches
- 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 attacks prevented 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
- Leverages proven technology certified to Common Criteria EAL

DEEP SECURITY CAPABILITIES

Anti-malware with web reputation

- Integrates VMware vShield Endpoint APIs to protect VMware virtual machines against viruses, spyware, Trojans, and other malware with zero in-guest footprint
- Delivers an anti-malware agent to extend protection to physical, virtual, and cloud servers, including AWS, Microsoft, and VMware environments
- Includes improved performance through VMware ESX-level caching and deduplication
- Optimizes security operations to avoid antivirus storms commonly seen in full system scans and pattern updates from traditional security capabilities
- Protects from sophisticated attacks in virtual environments by isolating malware from critical operating system and security components
- Identifies and analyzes suspicious objects through sandbox analysis
- Integrates with the Trend Micro™ Smart Protection Network™ global threat intelligence for web reputation capabilities that strengthen protection for servers and virtual desktops

Log inspection

- Collects and analyzes operating system and application logs in over 100 log file formats, identifying suspicious behavior, security events, and administrative events across your data center
- Assists with compliance (PCI DSS section 10.6) to optimize the identification of important security events buried in multiple log entries
- Forwards events to SIEM system or centralized logging server for correlation, reporting, and archiving

Intrusion prevention

- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Automatically protects against known but unpatched vulnerabilities by virtually patching (shielding) them from an unlimited number of exploits, pushing protection to thousands of servers in minutes without a system reboot
- Assists with compliance (PCI DSS section 6.6) to protect web applications and the data they process
- Defends against SQL injection, cross-site scripting, and other web application vulnerabilities
- Includes out-of-the-box vulnerability protection for all major operating systems and over 100 applications, including database, web, email, and FTP servers
- Provides increased visibility and control over applications accessing the network

Bidirectional host-based firewall

- Decreases the attack surface of physical, cloud, and virtual servers with fine-grained filtering, policies per network, and location awareness for all IP-based protocols and frame types
- Centrally manages server firewall policy, including templates for common server types
- Prevents denial-of-service attacks and detects reconnaissance scans
- Provides logging of firewall events at the host, enabling compliance and audit reporting that is especially critical for public cloud deployments

Integrity monitoring

- Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time
- Uses Intel TPM/TXT technology to perform hypervisor integrity monitoring for any unauthorized changes to the hypervisor, thereby extending security and compliance to the hypervisor layer
- Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire data center
- Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro™ Certified Safe Software Service

Application control

- Detects and blocks unauthorized software automatically
- Scans a machine and determines which applications are currently on it
- Locks down the system once the inventory is created, preventing new applications from running without being whitelisted
- Integrates into a DevOps environment to support continuous changes to application stacks, while maintaining application control protection using APIs
- Helps to catch threats that yet to have a signature, including some zero-day threats

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. For non-NSX environments, 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 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 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.

DEPLOYMENT AND INTEGRATION

Rapid Deployment: Leverage Existing IT and Security Investments

- Agent software can be deployed easily through standard software distribution mechanisms such as Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks, and Symantec Deployment Solution
- Detailed, server-level security events are provided to a SIEM system, including HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic, and other systems through multiple integration options.
- Directory integration with enterprise directories, including Microsoft Active Directory

SYSTEM REQUIREMENTS
Microsoft® Windows®
• Windows XP, Vista, 7, 8, 8.1, 10 (32-bit/64-bit) • Windows Server 2003 (32-bit/64-bit) • Windows Server 2008 (32-bit/64-bit), 2008 R2, 2012, 2012 R2, 2012 Server Core (64-bit), 2016 (64-bit), 2016 Server Core (64-bit) • XP Embedded (32-bit/64-bit)[1]
Linux[2]
• Red Hat® Enterprise 5, 6, 7 (32-bit/64-bit)[3] • SUSE® Enterprise 10, 11, 12 (32-bit/64-bit)[3] • CentOS 5, 6, 7 (32-bit/64-bit)[5] • Ubuntu 12, 14, 16 (64-bit, LTS only)[4, 5] • Oracle Linux 5, 6, 7 (32-bit/64-bit)[4, 5] • CloudLinux 5, 6, 7 (32-bit/64-bit)[2,4] • Amazon Linux (32-bit/64-bit)[4, 5] • Debian 6, 7 (64-bit)[2,4]
Oracle Solaris™ [6, 7]
• OS: 10, 11 (64-bit SPARC), 10, 11 (64-bit x86)[7, 8] • Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud and SPARC Super Cluster via the supported Solaris operating systems
UNIX[6]
• AIX 5.3, 6.1, 7.1 on IBM Power Systems[7, 8] • HP-UX 11i v3 (11.31)[7, 9]
VIRTUAL
• VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3 • Citrix®: XenServer[11] • Microsoft®: HyperV[11]

[1] Due to the customization possible with Windows XP Embedded, we request that customers validate correct operation in their own environments to ensure the services and ports necessary to run the Deep Security Agent have been enabled.
[2] See documentation for supported kernels
[3] Support for SAP protection only in Red Hat 6 (64-bit) and SUSE 11 (64-bit) agent side only. To have SAP protection function correctly, the anti-malware module must be enabled in the agent side.
[4] Anti-malware support for on-demand scan only
[5] See latest release notes for supported versions
[6] Anti-malware and web reputation monitoring not available
[7] Supported via 9.0 agents
[8] Anti-malware not available
[9] Log inspection and integrity monitoring only
[10] vCloud Networking and Security allows for agentless anti-malware and integrity monitoring
[11] Protection via Deep Security Agent only

POWERED BY XGEN™ SECURITY

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

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

Securing Your Journey to the Cloud