Trend Micro™

DEEP SECURITY 9

Comprehensive security platform for physical, virtual, and cloud servers

Virtualization and cloud computing have changed the face of today's data center. Yet as organizations move from physical environments to a mix of physical and virtual, and private and public clouds, many continue to address the prevailing threat landscape with legacy security. In virtual environments, this can increase operational complexity and decrease host performance and VM density. In cloud environments, legacy security leaves gaps in protection undermining the confidence to move mission-critical workloads to agile, low-cost cloud environments. Ultimately, this hinders the ability to fully invest in virtualization and cloud computing and maximize the return on investment in these technologies.

Trend Micro™ Deep Security software provides compliance by providing a comprehensive server security platform designed to protect your data center and cloud workloads from data breaches and business disruptions, and achieve cost-effective compliance across these environments. Tightly integrated modules including anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, and log inspection easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud environments. It is the industry's first agentless security solution on VMware but is also available as a single multi-function agent across all platforms. Either way, Deep Security simplifies security operations while accelerating the ROI of virtualization and cloud projects.

Deep Security also integrates with cloud platforms including those from Amazon and VMware enabling organizations to extend data center security policies to cloud-based workloads. And it is based on a multi-tenant architecture, allowing enterprises with software-defined data centers or service providers to use Deep Security 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 agentless 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
Achieve and prove compliance to a number of regulatory requirements including PCI DSS 2.0, HIPAA, FISMA/NIST, NERC. SAS 70 and more.

COMPREHENSIVE SERVER SECURITY

Virtualization Security

Virtualization security protects virtual desktops and servers against zero-day malware while minimizing operational impact from resource inefficiencies and emergency patching.

Cloud Security

Extend your data center security policies to your public and hybrid cloud workloads and manage both data center and cloud workloads with consistent and context-aware policies. Enable service providers or software-defined data centers to offer a secure multi-tenant cloud environment.

Integrated Server Security

Consolidate all server security point products into one comprehensive, integrated and flexible platform that optimizes protection across physical, virtual, and cloud servers.

KEY ADVANTAGES

Accelerate Virtualization & Cloud ROI

- Provides the industry's first agentless security platform built for VMware environments that yields more efficient resource utilization, higher VM densities and easier manageability over traditional anti-malware solutions
- Also available as a single easy-to-manage multi-function security agent, for added flexibility and defense in depth
- Delivers unparalleled performance via hypervisor-level scanning deduplication
- Integrates with cloud platform APIs such as Amazon AWS and VMware vCloud Director enabling organizations to manage their physical, virtual, and cloud servers with consistent and context-aware security policies
- Multi-tenant architecture enables service providers to offer customers a secure public cloud, isolated from other tenants
- Provides auto-scaling, utility computing and self-service to support agile organizations running a software defined datacenter

Prevent Data Breaches and Business Disruptions

- Detects and removes malware from virtual servers in real time with minimal performance impact
- Blocks malware that attempts to evade detection by uninstalling or otherwise disrupting the security program
- Shields known and unknown vulnerabilities in web and enterprise applications and operating systems
- Detects and alerts suspicious or malicious activity to trigger proactive, preventative actions
- Leverages the web reputation capabilities of one of the largest domain-reputation databases in the world to track credibility of websites and protect users from accessing infected sites
- Identifies and blocks botnet and targeted attack Command and Control (C&C) communications using global and local threat intelligence

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 to management consoles from Trend Micro, VMware, and enterprise directories
- Provides vulnerability protection to prioritize secure coding and cost-effective implementation of unscheduled patching
- 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

Achieve Cost-effective Compliance

- Addresses major compliance requirements for PCI DSS 2.0, as well as HIPAA, NIST, and SAS 70 with one integrated and cost-effective solution
- Provides detailed, auditable reports that document prevented attacks and policy compliance 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 4+

Security built for virtual and cloud environments

- First and only agentless security platform for the VMware hypervisor
- Proven to improve security, manageability, and VM density in the real world over thousands of agentless customer deployments
- First and only security to integrate with cloud platforms including Amazon EC2 and VMware vCloud
- First and only security architecture designed for service providers and enterprises with software defined datacenters, with support for multi-tenancy, auto-scaling, utility computing and self-service

DEEP SECURITY PLATFORM MODULES

Anti-Malware

- 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 servers as well as Citrix, HyperV and public cloud servers
- Includes improved performance through ESX level caching and deduplication
- Optimizes security operations to avoid antivirus storms commonly seen in full system scans and pattern updates
- Tamper-proofs security from sophisticated attacks in virtual environments by isolating malware from anti-malware

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
- Utilizes Intel TPM/TXT technology to perform hypervisor integrity monitoring. Monitors for any unauthorized changes to the hypervisor, thereby extending security and compliance of virtualized systems to the hypervisor
- 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

Web Reputation

- Integrates with the Trend Micro™ Smart Protection Network™ for web reputation capabilities that strengthen protection for servers and virtual desktops
- Provides agentless web reputation on the same virtual appliance as agentless anti-malware and intrusion prevention for greater virtual server security with small footprint

Intrusion Prevention

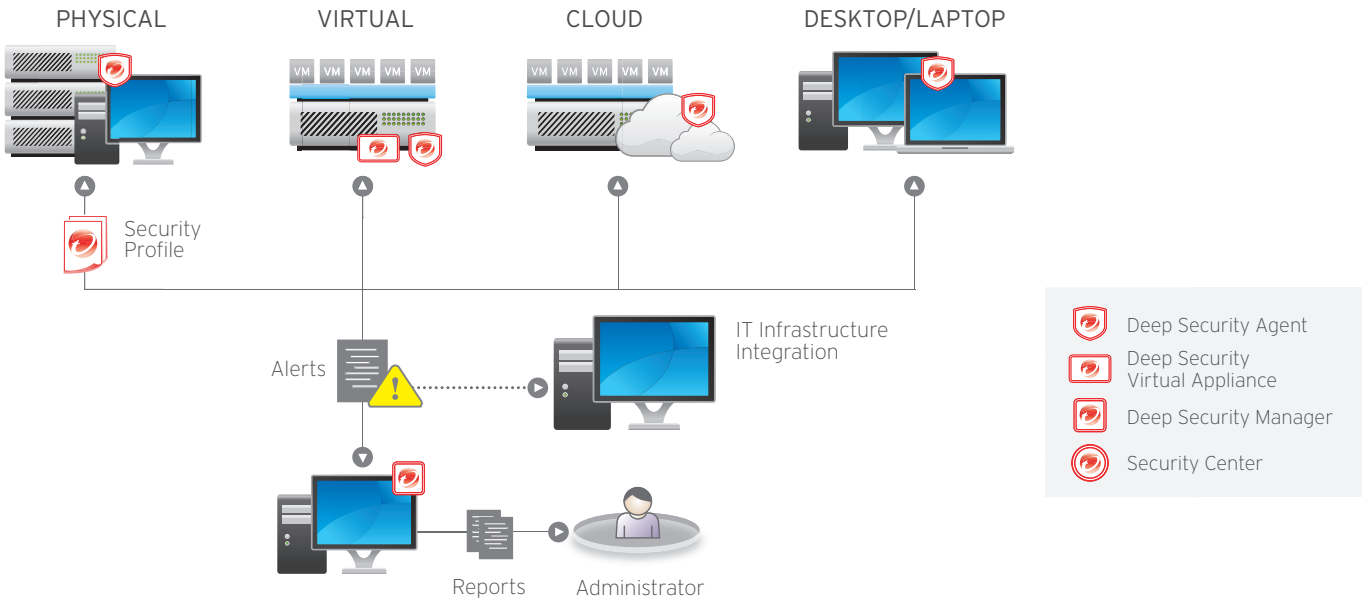
- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Protects against known but unpatched vulnerabilities by virtually patching (shielding) them from an unlimited number of exploits
- Automatically shields newly discovered vulnerabilities within hours, pushing protection to thousands of servers in minutes without a system reboot
- Assists compliance (PCI DSS 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 into, or control over applications accessing the network

Bidirectional Stateful Firewall

- Decreases the attack surface of physical, cloud, and virtual servers with fine-grained filtering, design 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

Log Inspection

- Collects and analyzes operating system and application logs for suspicious behavior, security events, and administrative events across your datacenter
- Assists compliance (PCI DSS 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



PLATFORM ARCHITECTURE

Deep Security Virtual Appliance. Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, web reputation, intrusion prevention, integrity monitoring, and firewall protection—coordinating with Deep Security Agent, if desired, for log inspection and defense in depth.

Deep Security Agent. This small software component deployed on the server or virtual machine being protected enforces the datacenter's security policy (anti-malware, web reputation, intrusion prevention, firewall, integrity monitoring, and log inspection).

Deep Security Manager. Powerful, centralized management console with role-based administration and multi-level policy inheritance allows for very 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.

Smart Protection Network. Deep Security integrates with this next-generation cloud-client infrastructure to deliver real-time protection from emerging threats by continuously evaluating and correlating threat and reputation intelligence for websites, email sources, and files.

Deployment and Integration

Rapid Deployment Leverages Existing IT and Security Investments

- Integration with vShield Endpoint and VMsafe™ APIs as well as VMware vCenter enables rapid deployment on ESX servers as a virtual appliance to immediately and transparently protect vSphere virtual machines
- Detailed, server-level security events are provided to a SIEM system, including ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic, and other systems through multiple integration options
- Directory integration with enterprise directories, including Microsoft Active Directory
- Agent software can be deployed easily through standard software distribution mechanisms such as Microsoft® SMS, Novel Zenworks, and Altiris

PLATFORM ARCHITECTURE

Microsoft® Windows®

- Windows XP, Vista, 7, 8 (32-bit/64-bit)
- Windows Server 2003 (32-bit/64-bit)
- Windows Server 2008 R2, 2012 (64-bit)
- XP Embedded

Linux

- Red Hat® Enterprise 4, 5, 6 (32-bit/64-bit)[1]
- SUSE® Enterprise 10, 11 (32-bit/64-bit)[1]
- CentOS 5, 6 (32-bit/64-bit)[1]
- Amazon Linux[1]

Oracle Solaris™

- OS: 9, 10 (64-bit SPARC), 10, 11 (64-bit x86)[2]
- Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud and SPARC Super Cluster via the supported Solaris operating systems

UNIX

- AIX 5.3, 6.1 on IBM Power Systems[3]
- HP-UX 11i v3 (11.31)[3]

VIRTUAL

- VMware®: ESX/ESXi 3.x4, ESX/ESXi 4.05, ESX/ESXi/vShield Endpoint 4.1, ESXi 5.0/5.1/vCloud Networking and Security 5.1, View 4.5/5.0/5.1
- Citrix®: XenServer[4]
- Microsoft®: HyperV[4]

[1] Anti-malware support for on-demand scan only
[2] Anti-malware not available
[3] Only Integrity Monitoring and Log Inspection available on this platform
[4] Protection via Deep Security Agent only
[5] Agentless Protection for Firewall and Intrusion Prevention only

Key Certifications and Alliances

- Common Criteria EAL 4+
- PCI Suitability Testing for HIPS (NSS Labs)
- Virtualization by VMware
- Amazon Advanced Technology Partner
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Oracle Partnership
- HP Business Partnership
- Certified Red Hat Ready
- VCE Vblock validated
- Cisco UCS validated
- EMC VSPEX validated
- NetApp FlexPod validated

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

TREND MICRO™

Securing Your Journey to the Cloud