

Trend Micro™

Deep Security 7.5

Server and Application Protection for Dynamic Datacenters

Enterprises are increasingly online and data-centric, connecting partners, personnel, suppliers, or customers with applications that face a growing danger of cyber attacks. These targeted threats are greater and more sophisticated than ever before, and data security compliance requirements become more stringent every day. Your company needs uncompromising security that enables you to modernize your datacenter with virtualization and cloud computing without reducing performance.

Trend Micro Deep Security Trend Micro Deep Security provides advanced security for physical, virtual, and cloud servers and virtual desktops. Whether implemented as software, virtual appliance, or in a hybrid approach, this solution minimizes overhead, streamlines management, and provides strong agentless security for virtual machines. Deep Security also addresses a wide range of compliance requirements, including seven major PCI compliance requirements with multiple protection modules in one consolidated solution.

ARCHITECTURE

NEW! Deep Security Virtual Appliance. Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, IDS/IPS, web application protection, application control, and firewall protection—coordinating with Deep Security Agent, if desired, for integrity monitoring and log inspection.

Deep Security Agent. This small software component deployed on the server or virtual machine being protected enforces the datacenter's security policy (IDS/IPS, web application protection, application control, firewall, integrity monitoring, and log inspection).

Deep Security Manager. Powerful, centralized management enables administrators to create security profiles and apply them to servers, monitor alerts and preventive actions taken in response to threats, distribute security updates to servers, and generate reports. New Event Tagging functionality streamlines the management of high-volume events.

Security Center. Our dedicated team of security experts helps you stay ahead of the latest threats by rapidly developing and delivering security updates that address newly discovered vulnerabilities. A customer portal gives you access to security updates that are delivered to Deep Security Manager for deployment.

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-scale directories, including Microsoft Active Directory
- Agent software can be deployed easily through standard software distribution mechanisms such as Microsoft® SMS, Novel Zenworks, and Altiris

KEY BENEFITS

Prevents Data Breaches and Business Disruptions

- Provides a line of defense at the server, whether physical, virtual, or in the cloud
- Shields known and unknown vulnerabilities in applications and operating systems
- Protects web applications from SQL injection and cross-site scripting attacks
- Blocks attacks to enterprise systems
- Identifies suspicious activity and behavior, enabling proactive and preventive measures

Helps Comply with PCI and Other Regulations and Standards

- Addresses seven major PCI data security standards, and a wide range of other, compliance requirements
- Provides detailed, auditable reports that document prevented attacks and policy compliance status
- Reduces the preparation time and effort required to support audits

Achieves Operational Cost Reductions

- Optimizes the savings of virtualization or cloud computing by allowing greater virtual machine consolidation
- Simplifies management for virtual server and desktop environments by providing anti-malware and other security mechanisms in an agentless configuration
- Streamlines administration by automating management of security events across all servers
- Provides vulnerability protection to prioritize secure coding and cost-effective implementation of unscheduled patching
- Eliminates the cost of deploying multiple software clients with a centrally managed, multi-purpose software agent or virtual appliance

DEEP SECURITY MODULES

NEW! Agentless Malware Protection for VMware Environments

- Integrates new VMware vShield Endpoint APIs for protection of VMware virtual machines against viruses, spyware, trojans and other malware with zero in-guest footprint
- Optimizes security operations to avoid security brown-outs commonly seen in full system scans and pattern updates
- Tamper-proofs security from sophisticated attacks by isolating malware from anti-malware

Deep Packet Inspection

- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Operates in detection or prevention mode to protect operating systems and enterprise application vulnerabilities
- Provides automatic notification that outlines who attacked, when they attacked, and what they attempted to exploit

Intrusion Detection and Prevention

- Protects against known and zero-day attacks by shielding known vulnerabilities from unlimited exploits
- Automatically shields newly discovered vulnerabilities within hours, pushing protection to thousands of servers in minutes without a system reboot
- Includes out-of-the-box vulnerability protection for over 100 applications, including database, web, email, and FTP servers

Web Application Protection

- 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
- Shields against vulnerabilities until code fixes can be completed

Application Control

- Provides increased visibility into, or control over applications accessing the network
- Uses application control rules to identify malicious software accessing the network
- Reduces vulnerability exposure of servers

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

Integrity Monitoring

- Monitors critical operating system and application files, such as directories, registry keys, and values, to detect malicious and unexpected changes
- Detects modifications to existing file systems and new file creations and reports them in real time
- Enables on-demand, scheduled, or real-time detection; checks file properties (PCI 10.5.5); and monitors specific directories

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

PLATFORMS PROTECTED

Microsoft® Windows®

- 2000 (32-bit)
- XP (32-bit/64-bit)
- XP Embedded
- Windows 7 (32-bit/64-bit)
- Windows Vista (32-bit/64-bit)
- Windows Server 2003 (32-bit/64-bit)
- Windows Server 2008 (32-bit/64-bit)
- Windows Server 2008 R2 (64-bit)

Solaris™

- OS: 8, 9, 10 (64-bit SPARC), 10 (64-bit x86)

Linux

- Red Hat® Enterprise 4.0, 5.0 (32-bit/64-bit)
- SUSE® Enterprise 10, 11 (32-bit/64-bit)

UNIX® *

- AIX 5.3, 6.1
- HP-UX® 10, 11i v2/v3

* Integrity Monitoring and Log Inspection available only

VIRTUALIZATION

- **Virtual Appliance:** VMware vSphere 4.1
- **VMware®:** VMware ESX 4.1 Server (guest OS)
- **Citrix®:** XenServer
- **Microsoft®:** HyperV
- **Sun:** Solaris 10 containers

KEY CERTIFICATIONS AND ALLIANCES

- Common Criteria EAL 3+ (EAL 4 in progress)
- PCI Suitability Testing for HIPS (NSS Labs)
- Virtualization by VMware
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Novell
- Oracle Partnership
- HP Business Partnership
- Certified Red Hat Ready

Datacenter Requirement	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection	NEW! Anti-Malware
	IDS/IPS	Web Application Protection	Application Control				
Server Protection	●			●	●	○	●
Web Application Security	●	●			○	●	
Virtualization Security	●	○		●	●	○	●
Suspicious-Behavior Detection	○		●	●	●	●	
Cloud Computing Security	●	○		●	●	●	●
Compliance Reporting	○	●	○	○	●	●	
Agent-based	●	●	●	●	●	●	
Virtual Appliance	●	●	●	●			●

● Essential ○ Advantageous



©2010 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, OfficeScan, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS03DeepSecurity7.5_100721US]

www.trendmicro.com