

Trend Micro™

Deep Security 7

Server and Application Protection for Dynamic Datacenters

Enterprises are increasingly online and data-centric, and no matter what the purpose—connecting partners, personnel, suppliers, or customers—applications face a growing danger of cyber attacks. These targeted threats are greater and more sophisticated than ever before, and data security compliance becomes 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 delivers streamlined, integrated products, services, and solutions that cost-effectively protect sensitive data and minimize risk. Deep Security is comprehensive server and application protection software that enables physical, virtual, and cloud computing environments to become self-defending. Whether implemented as software, virtual appliance, or in a hybrid approach, this solution minimizes overhead, streamlines management, and strengthens transparent security for virtual machines. Deep Security also addresses a wide range of compliance requirements, including six major PCI compliance requirements with web application-layer firewall, IDS/IPS, file integrity monitoring, and network segmentation.

ARCHITECTURE

- **Deep Security Virtual Appliance.** Transparently enforces security policies on VMware vSphere virtual machines for 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.

DEPLOYMENT AND INTEGRATION

Rapid Deployment Leverages Existing IT and Security Investments

- VMware integration with VMware vCenter and ESX Server enables organizational and operational information to be imported into Deep Security Manager, and detailed security to be applied to an enterprise's VMware infrastructure
- Integration with VMsafe™ APIs 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
- Configurable management communication minimizes or eliminates firewall changes typically needed for centrally managed systems by enabling either the Manager or the Agent to initiate communication
- 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 six 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 consolidating server resources
- Streamlines administration by automating management of security events
- 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

Deep Packet Inspection

- Examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations
- Operates in detection or prevention mode to protect operating systems and enterprise application vulnerabilities
- Defends against application-layer attacks, SQL injection, and cross-site scripting
- Provides valuable information, including who attacked, when they attacked, and what they attempted to exploit
- Automatically notifies administrators when an incident has occurred

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
- Smart rules provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code

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 realtime detection, checks file properties (PCI 10.5.5), and monitors specific directories
- Delivers flexible and practical monitoring through includes/excludes and auditable reports

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
- Centrally manages server firewall policy, including templates for common server types
- Features fine-grained filtering (IP and MAC addresses, ports), design policies per network interface, and location awareness
- Prevents denial of service attacks and detects reconnaissance scans
- Covers all IP-based protocols (TCP, UDP, ICMP, etc.) and all frame types (IP, ARP, etc.)

Log Inspection

- Collects and analyzes operating system and application logs for security events
- 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
- Detects suspicious behavior, collects security events and administrative actions across your datacenter, and creates advanced rules using OSSEC syntax

PLATFORMS PROTECTED

Microsoft® Windows®

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

Solaris™

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

Linux

- Red Hat® Enterprise 3.0 (32-bit), 4.0, 5.0 (32-bit/64-bit)
- SUSE® Enterprise 9, 10 (32-bit/64-bit)

UNIX®*

- AIX 5.3
- HP-UX® 10, 11i v2, 11i v3

* Integrity Monitoring and Log Inspection available only

VIRTUALIZATION

- **VMware®:** VMware ESX Server (guest OS)
- **Citrix®:** XenServer Guest VM
- **Microsoft®:** HyperV Guest VM
- **Sun:** Solaris 10 OS partitions

KEY CERTIFICATIONS AND ALLIANCES

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

DEEP SECURITY MODULES						
Datacenter Requirement	Deep Packet Inspection			Firewall	Integrity Monitoring	Log Inspection
	IDS/IPS	Web Application Protection	Application Control			
Server Protection	●			●	●	○
Web Application Security	●	●			○	●
Virtualization Security	●	○		●	●	○
Suspicious-Behavior Detection	○		●	●	●	●
Cloud Computing Security	●	○		●	●	●
Compliance Reporting	○	●	○	○	●	●

● Essential ○ Advantageous



©2009 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. [DS02DeepSecurity7_091125US]

www.trendmicro.com