

Trend Micro™

Deep Security 8.0

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, virtual, and cloud, many have addressed the prevailing threat landscape with yesterday's mix of legacy security solutions. The results can actually threaten desired performance gains—causing undue operational complexity, leaving unintentional security gaps, and ultimately hindering the organization's ability to fully invest in virtualization and cloud.

Trend Micro Deep Security provides a comprehensive server security platform designed to simplify security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops. So you can custom tailor your security with any combination of agentless and agent-based protection, including anti-malware, firewall, IDS/IPS, web application protection, integrity monitoring, and log inspection. The result is a comprehensive, adaptive and efficient server security platform that protects mission-critical enterprise applications and data from breaches and business disruptions without expensive emergency patching.

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+

KEY FEATURES

Accelerate Virtualization, VDI, and Cloud ROI

- Provides a lighter, more manageable way to secure VMs with the industry's first and only agentless security platform—anti-malware, intrusion prevention, and integrity monitoring—built for VMware environments
- **NEW!** Offers agentless integrity monitoring for greater virtual server security without added footprint
- Delivers 11X more efficient resource utilization and supports 3X the VM densities of traditional anti-malware solutions
- Improves the manageability of security in VMware environments by reducing the need to continually configure, update, and patch agents
- Secures VMware View virtual desktops while in local mode with an optional agent
- Coordinates protection with virtual appliance and agents to allow continuous and optimized protection of virtual servers as they move between data center and public cloud

Maximize Operational Cost Reductions

- Optimizes the savings of virtualization or cloud computing by allowing greater virtual machine consolidation
- 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
- Eliminates the cost of deploying multiple software clients with a centrally managed, multi-purpose software agent or virtual appliance
- Reduces management costs by automating repetitive and resource intensive security tasks, reducing false-positive security alerts, and enabling workflow of security incident response
- **NEW!** Significantly reduces the complexity of managing file integrity monitoring with cloud-based event whitelisting and trusted events

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
- **NEW!** 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
- **NEW!** Provides hypervisor integrity monitoring for VMware vSphere utilizing Intel TPM/TXT technology

DEEP SECURITY PLATFORM MODULES

Anti-Malware Protection for VMware Environments

- Integrates new VMware vShield Endpoint APIs to protect VMware virtual machines against viruses, spyware, trojans and other malware with zero in-guest footprint
- **NEW!** Delivers an anti-malware agent to extend protection to physical servers as well as to virtual desktops while in local mode
- **NEW!** Integrates with the Trend Micro™ Smart Protection Network™ for web reputation capabilities that strengthen protection for servers and virtual desktops
- 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
- **NEW!** Provides agentless integrity monitoring on the same virtual appliance as agentless anti-malware and intrusion prevention for greater virtual server security without added footprint
- **NEW!** Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire data center
- **NEW!** Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro Certified Safe Software Service
- **NEW!** Protects the hypervisor from exploits by providing hypervisor integrity monitoring utilizing Intel TPM/TXT technology

Intrusion Detection and Prevention

- Protects against known and zero-day attacks by shielding known vulnerabilities from unlimited exploits
- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Automatically shields newly discovered vulnerabilities within hours, pushing protection to thousands of servers in minutes without a system reboot
- Integrates with agentless anti-malware and integrity monitoring in the same virtual appliance for increased protection
- Includes out-of-the-box vulnerability protection for all major operating systems and 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
- Provides automatic notification that outlines who attacked, when they attacked, and what they attempted to exploit.

Application Control

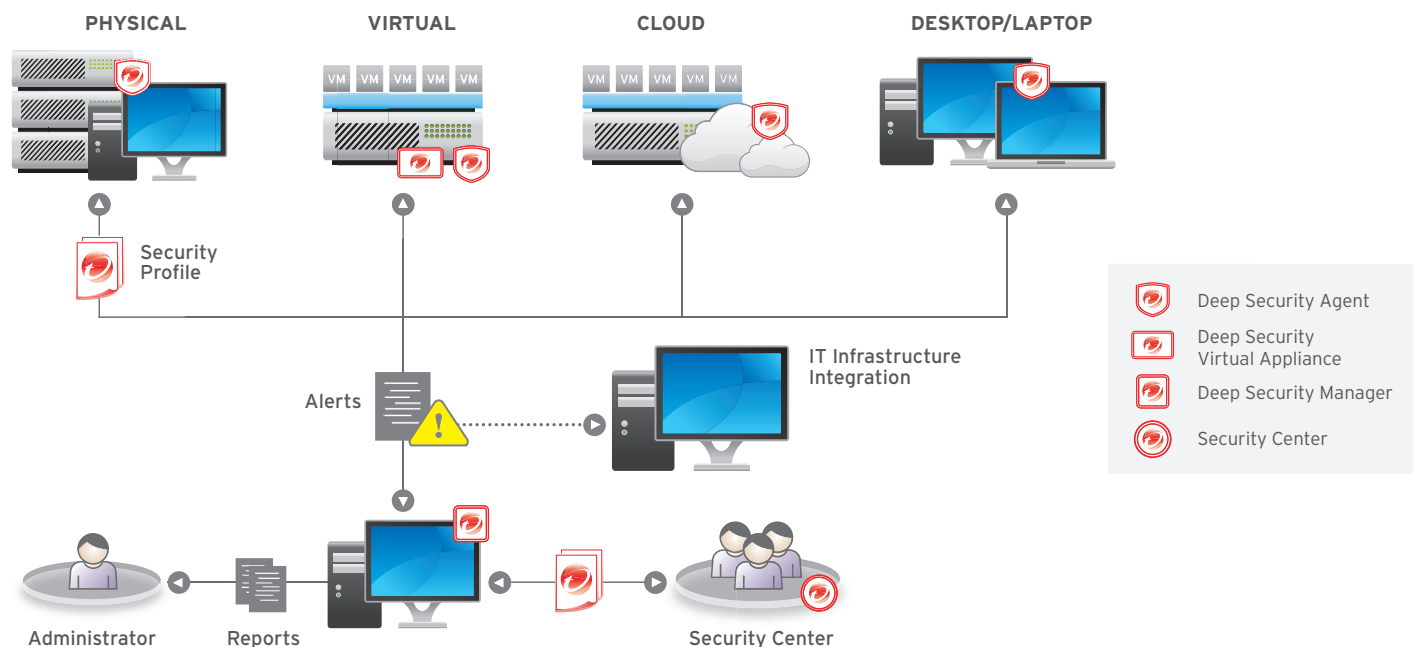
- Provides increased visibility into, or control over applications accessing the network
- Uses application control rules to identify malicious software accessing the network
- Reduces vulnerability exposure of servers

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

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



BUILT FOR VMWARE VIRTUAL AND CLOUD ENVIRONMENTS

Deep Security is specifically designed for virtual environments. Its agentless architecture addresses AV storms, minimizes operational complexity of security and allows organizations to increase VM densities and accelerate virtualization and cloud adoption. Developed in close collaboration with VMware, Deep Security is the first product in its category to offer support for VMware vSphere 5.0 and VMware vShield Endpoint 2.0. Deep Security also provides full backward compatibility with vSphere 4.1 environments. The Deep Security 8.0 Manager also supports mixed mode VMware environments supporting both vSphere 5.0 and vSphere 4.1 protected by the Deep Security 8.0 or 7.5 virtual appliances.

PLATFORM ARCHITECTURE

Deep Security Virtual Appliance. Transparently enforces security policies on VMware vSphere virtual machines for agentless anti-malware, IDS/IPS, integrity monitoring, web application protection, application control, 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, 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. 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.

Deep Security Helps You Resolve Key Business Issues

Virtual Patching

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

Virtual Desktop and Server Security

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

Compliance

Achieve and prove compliance to a number of regulatory requirements including PCI DSS 2.0, HIPAA, FISMA/NIST, NERC. SAS 70, and more.

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.

Data Protection

Protect and manage access to critical data in—and as it moves between—your data center and private cloud environments. Deep Security combines advanced technologies such as intrusion prevention and integrity monitoring with policy-based key management technology, available through its integration with SecureCloud.

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 Certifications and Alliances

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

PLATFORM ARCHITECTURE

Microsoft® Windows®

- 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 R2 (64-bit)

Linux

- Red Hat® Enterprise 5, 6 (32-bit/64-bit)¹
- SUSE® Enterprise 10, 11 (32-bit/64-bit)¹

Solaris™

- OS: 8, 9, 10 (64-bit SPARC), 10 (64-bit x86)¹

UNIX

- AIX 5.3, 6.1 on IBM Power Systems²
- HP-UX 11i v3 (11.31)²

VIRTUAL

- VMware®: ESX/ESXi 3.x³, vSphere 4.0⁴, vSphere 4.1/5.0⁵, View 4.5/5.0⁵
- Citrix®: XenServer³
- Microsoft®: HyperV³

¹ Anti-malware not available

² Only Integrity Monitoring and Log Inspection available on this platform

³ Protection via Deep Security Agent only

⁴ Protection via Deep Security Agent and Virtual Appliance for Firewall, IDS/IPS and Web application protection, via Agent only for other modules

⁵ Protection via Deep Security Agent only for Log Inspection, via Agent and Virtual Appliance for all other modules, separate license to vShield Endpoint required



©2011 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. [DS01_DeepSecurity8_110816US]

www.trendmicro.com