Virtualization and cloud computing have transformed the data center. Yet many organizations continue to use legacy security as they move from traditional physical environments to the modern data center where virtualization and cloud are the norm. Legacy security can increase operational complexity in virtual environments while decreasing host performance and VM density. It leaves gaps in protection that can undermine the confidence to move mission-critical workloads to agile, low-cost cloud environments. Ultimately, using legacy security in the modern data center hinders the return on investment (ROI) of virtualization and cloud computing.

Protection from data breaches and business disruption. Trend Micro™ Deep Security—available as software 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 virtual and cloud environments.

Multi-function security managed from a single dashboard. Deep Security features integrated modules including anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, 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.

Seamless integration extends policies across cloud environments. Deep Security seamlessly integrates with cloud platforms including Amazon Web Services (AWS), Microsoft Azure, and VMware vCloud Hybrid Service 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.

ACCELERATE THE ROI OF CLOUD AND VIRTUALIZATION WITH SECURITY FOR THE MODERN DATA CENTER

Virtualization Security
Deep Security protects virtual desktops and servers against zero-day malware and network-based attacks while minimizing operational impact from resource inefficiencies and emergency patching.

Cloud Security
Deep Security enables service providers and modern data centers 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.

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.

Data Privacy and Compliance
Demonstrate compliance with a number of regulatory requirements including PCI DSS 3.0, HIPAA, HITECH, FISMA/ NIST, NERC, SAS 70 and more.


**KEY ADVANTAGES**

**Accelerate Virtualization and Cloud ROI**
- Yields more efficient resource utilization and management with higher VM densities than traditional anti-malware solutions that are not agentless.
- Adds flexibility and defense-in-depth capabilities as a single easy-to-manage multi-function security agent.
- Delivers unparalleled performance via hypervisor-level scanning and deduplication.
- Integrates with cloud platforms including AWS, Microsoft Azure, and VMware vCloud Hybrid 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.

**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 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.

**Achieve Cost-effective Compliance**
- Addresses major compliance requirements for PCI DSS 3.0, as well as HIPAA, HITECH, NIST, and SAS 70 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 4+. 

**CONTROL SECURITY ACROSS PHYSICAL, VIRTUAL, AND CLOUD**

- **Deep Security Agent**
- **Deep Security Agentless**
- **Virtual Appliance**
- **Deep Security Manager**

![Diagram of security controls across physical, virtual, and cloud environments]

- **Cloud**
- **Modern Data Center**
- **Alerts**
- **IT Infrastructure Integration**
- **Reports**
- **Administrator**

![Diagram showing the integration of security controls across physical, virtual, and cloud environments]
DEEP SECURITY PLATFORM MODULES

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
- Integrates with the Trend Micro™ Smart Protection Network™ global threat intelligence for web reputation capabilities that strengthen protection for servers and virtual desktops

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 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

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 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

DEPLOYMENT AND INTEGRATION

Rapid Deployment: Leverage 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 Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks, and Symantec Deployment Solution.

CERTIFICATION FOR CSPS
- Trend Ready for Cloud Service Providers is a global testing program designed for Cloud Service Providers (CSPs) to prove interoperability with industry-leading cloud security solutions from Trend Micro.

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
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. Enforces the data center’s security policy (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 Trend Micro 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.

Key Certifications and Alliances

- Amazon Advanced Technology Partner
- Certified Red Hat Ready
- Cisco UCS validated
- Common Criteria EAL 4+
- 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)
- VCE Vblock validated
- Virtualization by VMware

Microsoft® Windows®

- Windows XP, Vista, 7, 8, 8.1 (32-bit/64-bit)
- Windows Server 2003 (32-bit/64-bit)
- XP Embedded

Linux

- Red Hat® Enterprise 5, 6 (32-bit/64-bit)
- SUSE® Enterprise 10, 11 (32-bit/64-bit)
- CentOS 5, 6 (32-bit/64-bit)
- Amazon Linux
- Ubuntu 10, 12 (64-bit)
- Oracle Linux 5, 6 (32-bit/64-bit)
- CloudLinux 5, 6 (32-bit/64-bit)

Oracle Solaris™

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

UNIX

- AIX 5.3, 6.1, 7.1 on IBM Power Systems
- HP-UX 11i v3 (11.31)

VIRTUAL

- VMware®: 5.0/5.1/vCloud Networking and Security 5.1, View 4.5/5.0/5.1, ESX 5.5
- Citrix®: XenServer
- Microsoft®, HyperV

1 Anti-malware support for on-demand scan only
2 Anti-malware not available
3 Anti-malware not available, Firewall and Intrusion Prevention on AIX only
4 Protection via Deep Security Agent only

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo 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.

Page 4 of 4 • DATASHEET • DEEP SECURITY 9