TREND MICRO DEEP SECURITY
MEETING PCI DSS V 2.0 COMPLIANCE REQUIREMENTS

The Payment Card Industry Data Security Standard (PCI DSS 2.0) specifies requirements to secure cardholder data that is stored, processed or transmitted by merchants and any other organization.

Trend Micro Deep Security provides software-based integrated security and compliance for business systems operating in standalone, virtual, and cloud-based environments. Deep Security helps assure the PCI compliance and overall security of critical business servers and endpoints with a single, centrally managed solution that minimizes your operational costs. Deep Security provides core PCI security controls with a unique approach that economically solves the toughest compliance challenges, including:

Deep Security provides a unique host-based software solution to address 7PCI regulations and over 20 sub-controls including:*

- *Network Segmentation*
- *Host Firewall*
- *Antivirus*
- *Virtual Patching / Shielding*
- *Web Application Protection*
- *Log Review*
- *IDS/IPS*

- **Distributed Locations.** Deep Security provides integrity monitoring, firewall, IPS and other core controls directly to host systems that process PAN data, eliminating the cost and complexity of multiple appliances at each location.
- **Vulnerability and Patch Management.** Deep Security virtual patching keeps you protected and compliant by closing your window of exposure to vulnerabilities, protecting "un-patchable" systems, lengthening standard patch cycles, and eliminating the need for costly ad-hoc and emergency patching.
- **Website Protection and Compliance.** The public exposure and dynamic nature of your website leave it extremely vulnerable to attack. Deep Security comprehensive system and web application protection and shielding keeps your website and company reputation secure.
- **Virtualization and Cloud Compliance.** The complexity and fluidity of desktop and server virtualization pose security, compliance, and performance risks that require the specialized, virtualization-optimized protection and performance of the Deep Security solution. Most features are available as an agent or agent-less VMware appliance.

DEEP SECURITY FEATURES

- **Intrusion Detection and Prevention (IDS/IPS).** Advanced deep packet inspection detects and blocks host attacks by examining all traffic for protocol deviations, exploit indications and policy violations.
- **Virtual Patching.** Discovers host vulnerabilities and recommends rules to shield applications and systems with advanced deep packet inspection technology.
- **Firewall.** An enterprise-grade, bi-directional and stateful firewall enables network segmentation and PCI audit scope reduction. Includes centralized management of server firewall policy, and pre-defined templates for common enterprise server types.
- **Web Application Protection.** Protects web applications against sophisticated attacks such as SQL injection, cross-site scripting, and more.
- **Antivirus Protection.** Provides "agentless" malware protection via a high-performance VMware virtual appliance.
- **Integrity Monitoring.** For critical OS and application files (including data files, directories, log files, registry keys and values). Detects and reports malicious and unexpected changes to both physical servers and virtual machines.
- **Application Control.** Application control rules provide visibility and control over applications accessing the network. Rules can also identify malicious software activity and reduce the vulnerability exposure of servers.
- **Logs and Log Inspection.** Analyzes OS and application logs to identify important security events, generate alerts, and forward to SIEM system.
- **Virtualization Compliance.** VM isolation and hardening protects and isolates payment processing applications from other VMs on the same hardware. Most features are available as an agent or agent-less appliance for VMware.

TREND MICRO™

* Network Segmentation applicable to remote/distributed environments. Virtual Patching may provide a compensating control. Antivirus available for VMware only until 2H 2011

TREND MICRO DEEP SECURITY
MEETING PCI DSS V 2.0 COMPLIANCE REQUIREMENTS

PCI Requirement	How Trend Micro Deep Security Addresses It
1.1 Establish firewall and router configuration standards that include: 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Deep Security includes a sophisticated, centrally managed, stateful firewall. It helps prevent policy violations, logging and reporting any attempted firewall policy violations. The solution's security profiles contain the firewall configuration policy. Role-based access-control capabilities support separation of administrative duties with respect to creating, deploying, and auditing firewall policy and events that violate the policies. Deep Security is used to create and manage sophisticated firewall rules that allow and deny appropriate connections with a minimum number of rules and maximum flexibility. Centralized management makes this easy to administer and deploy to the right systems. Deep Security provides out-of-box reporting capabilities for creating reports that detail the hosts' stateful firewall configuration. Deep Security firewall capabilities can enable network segmentation to isolate systems that store, process, or transmit cardholder data from systems that do not. This enables cardholder data environments to be easily defined, reducing the overall scope of the PCI audit.
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.	The next-generation firewall in Deep Security provides advanced protection against threats to mobile users.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system-hardening standards as defined.	Security profiles can be used to specify configurations for unique server functions (e.g., a DNS, Web, or database server), and restrict or prevent access to services and protocols.
2.2.1 Implement only one primary function per server or per virtual system component.	In virtualized environments, the ability to create virtual machine zones and isolate payment-processing applications from applications that are not part of the cardholder data environment—but do reside on the same physical hardware— is a critical factor during compliance audits. The solution's firewall and IDS/IPS capabilities provide next-generation firewall protection capabilities down to the virtual machine level, ensuring that compliance requirements have been met, independent of the fact that virtualization technology is being utilized.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	Deep Security provides the ability to deploy firewall rules that block all unnecessary ports and protocols not directly needed to perform the server's specified function. In addition, Deep Security supports the ability to audit the system's firewall configuration by running port scans to validate that no unexpected ports are accessible.
2.4 Shared hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."	Shared hosting providers leverage virtualization to make services cost-effective for their clients. In virtualized environments, the ability to create virtual machine zones and isolate payment-processing applications from other applications—ones not part of the cardholder data environment but residing on the same physical hardware—is a critical factor during compliance audits. The solution's host-based firewall and IDS/IPS capabilities provide next-generation firewall protection capabilities down to the virtual machine level, helping ensure that compliance requirements have been met, independent of the fact that virtualization technology is being utilized. Deep Security can also help hosting providers with Appendix A requirements, by enforcing logical access restrictions to the host and through RBAC and delegated administration restrictions on Deep Security Manager.

TREND MICRO DEEP SECURITY
MEETING PCI DSS V 2.0 COMPLIANCE REQUIREMENTS

PCI Requirement	How Trend Micro Deep Security Addresses It
5.1 Deploy anti-virus software on all systems commonly affected by malicious software	Deep Security antivirus module provides advanced malware protection for physical and virtual systems host servers and endpoints (Available for VMware only until 2H 2011)
5.2 Ensure that all anti-virus mechanisms are current	Deep Security antivirus signatures are automatically kept up to date via the Trend Micro Smart Protection Network. Antivirus events are automatically logged to the Deep Security Manager.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Deep Security virtual patching capabilities protect systems and data until patches can be deployed. When approved by your QSA, it can act as a compensating control for systems that cannot be patched within the required time frame. Deep Security can also shield known vulnerabilities for which a vendor patch is not available, or in custom applications where source code changes are required to remediate vulnerabilities.
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	Deep Security systematically monitors and categorizes a wide range of vulnerability research sources to identify and deliver new deep packet inspection (DPI) rules to customers. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention. Deep Security also supports the ability to schedule automatic scans—one time only, daily, weekly, and so forth—of host systems, offering recommendations on the appropriate security rules to protect these hosts.
6.5 Develop applications based on security coding guidelines. Prevent common coding vulnerabilities in software development processes. .	Deep Security complements secure coding initiatives by providing strong detection and prevention capabilities that address attacks as identified by OWASP: ▪ Detection−It is important to detect attacks, even if an application is not susceptible to a specific attack or class of attack, because it identifies the attacker before they can find other potential vulnerabilities. ▪ Protection—Deep Security shields Web application vulnerabilities, preventing security breaches until the underlying flaws can be addressed.
6.6 For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure that these applications are protected against known attacks by either of the following methods: ▪ Reviewing public-facing Web applications via manual or automated application-vulnerability security-assessment tools or methods, at least annually and after any changes ▪ Installing a Web application firewall in front of public-facing Web applications	Web application protection rules defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed. Deep Security also protects against vulnerabilities in the operating system and Web infrastructure. Deep Security Integrity Monitoring and Log Inspection modules provide immediate insight into suspicious activity that might be occurring in your Web environment. Monitoring and detecting suspicious behavior is a key element in identifying data breach attempts.
10.3 Record at least the following audit trail entries for all system components for each event: ▪ User identification ▪ Type of event ▪ Date and time ▪ Success or failure indication ▪ Origination of event ▪ Identity or name of affected data system component or resource	Deep Security provides the ability to collect and forward all operating system and application events to a centralized logging server or SIEM. Alternatively, Deep Security provides the ability to correlate and forward just the operating system and application logging events of relevance to PCI compliance, significantly reducing network bandwidth consumption for centralized logging, in addition to reducing the number of events that need to be analyzed, correlated, and archived. Deep Security provides default log inspection rules for many of the most common enterprise operating systems and applications, as well as enabling the creation of custom log inspection rules. Deep Security firewall, IDS/IPS, antivirus, and integrity monitoring events can also be forwarded to the SIEM or centralized logging server.

TREND MICRO DEEP SECURITY
MEETING PCI DSS V 2.0 COMPLIANCE REQUIREMENTS

PCI Requirement	How Trend Micro Deep Security Addresses It
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	The Deep Security Log Inspection module enables you to forward event information to centralized logging servers or SIEMs via syslog in real time, in addition to sending these events to the Deep Security Manager.
10.5.5 Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts—although new data being added should not cause an alert.	The Deep Security Log Inspection module provides the ability to monitor log files without generating alerts as new data is added to the log.
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions, such as intrusion detection system (IDS) and authentication, authorization, and accounting (AAA) protocol servers—for example, RADIUS. Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.	The Deep Security Log Inspection module monitors critical OS and application logs in real time for relevant security events, and forwards these events to a SIEM or centralized logging server for further analysis, correlation, alerting, and archival—automating the process of log reviews.
11.4 Use IDS, and/or intrusion prevention system (IPS), to monitor all traffic at the perimeter of the CDE as well as at critical points inside the CDE. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	Deep Security includes a host-based IDS/IPS module. This module monitors traffic, prevents intrusions, and alerts personnel to suspected compromises. Security updates that shield newly discovered vulnerabilities are automatically delivered to customers and hosts. Deep Security's "recommendation scan" feature identifies applications running on hosts that might be vulnerable, and recommends which rules should be applied to these hosts, ensuring that the correct protection is continuously in place with minimal effort.
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configure the software to perform critical file comparisons at least weekly.	The Deep Security Integrity Monitoring module meets and exceeds these requirements by monitoring system executables, application executables, configuration and parameter files, and log and audit files. The Windows registry, services, ports, and directory contents can also be monitored.
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	Deep Security provides alerts that are integral to a security incident response plan. And because it can prevent attacks as well, Deep Security reduces the number of incidents requiring a response. The solution's integration with leading SIEM vendors enables you to receive a consolidated view of security incidents.
Appendix B: Compensating Controls for Encryption of Stored Data.	Deep Security delivers comprehensive, modular protection including IDS/IPS, Web application protection, application control, stateful firewall, log inspection, and integrity monitoring. This centrally managed solution offers capabilities that can be used to address gaps identified in a PCI audit assessment.

For more information please call or visit us at.
www.trendmicro.com/go/enterprise
+1-877-21-TREND