

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD MEETING STRINGENT REQUIREMENTS

The prescriptive, multifaceted PCI Data Security Standard (PCI DSS) includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The PCI DSS is intended to help you proactively protect your payment transaction systems to prevent identity theft and fraud using customer account data.

These standard requirements apply to all payment card network members, merchants, and service providers that store, process, or transmit cardholder data, and they affect all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. The latest version of the standard PCI DSS v1.2 was made available in October 2008 and—as noted on the Web site www.pcisecuritystandards.org—it “was a culmination of two years of feedback and suggestions from its industry stakeholders, and is designed to clarify and ease implementation of the foremost standard for cardholder account security.”

Trend Micro is dedicated to empowering your organization to meet these high standards for PCI data security, using the Deep Security solution—server and application protection software that enables systems to become self-defending.

HOW TREND MICRO DEEP SECURITY HELPS COMPANIES ACHIEVE PCI COMPLIANCE

Trend Micro Deep Security provides integral, comprehensive server security for datacenter modernization initiatives, including virtualization and cloud computing. This end-to-end protection helps you prevent data breaches and business disruptions, enables regulatory compliance, and reduces operational costs.

Deep Security can accelerate and simplify your PCI audit, and help achieve compliance, by:

- Monitoring the integrity of critical system and application files such as executables, configuration and parameter files, and log and audit files—it includes support for alerting, dashboards, and reporting on events raised
- Detecting and preventing attacks that target cardholder data, alerting your personnel the moment an attack has been attempted, and providing detailed logging of the event for audit purposes
- Virtual patching, as a compensating control for systems that cannot have vendor security patches applied to them within one month of release
- Enabling firewall network segmentation, to reduce the scope of the PCI audit
- Web application protection to complement secure coding initiatives and to protect against attacks such as SQL injection, cross-site scripting [XSS], and many more
- Log collection of important security events from operating system and application log files, including the ability to forward all events—or only events relevant to a centralized logging server
- Creating virtual machine zones and isolating payment processing applications from virtual machines on the same physical hardware that are separate from the cardholder data environment



PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD MEETING STRINGENT REQUIREMENTS

PCI Requirement	How Trend Micro Deep Security Addresses It
<p>1.1 Establish firewall and router configuration standards that include:</p> <p>1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.</p> <p>1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.</p> <p>1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p>	<p>Deep Security includes a sophisticated, centrally managed, stateful firewall. It helps prevent policy violations, logging and reporting any attempted firewall policy violations.</p> <p>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.</p> <p>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.</p> <p>Deep Security provides out-of-box reporting capabilities for creating reports that detail the hosts' stateful firewall configuration.</p> <p>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.</p>
<p>1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.</p>	<p>The next-generation firewall in Deep Security provides advanced protection against threats to mobile users.</p>
<p>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.</p>	<p>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.</p>
<p>2.2.1 Implement only one primary function per server.</p>	<p>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.</p>
<p>2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).</p>	<p>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</p>
<p>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."</p>	<p>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.</p>



PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD MEETING STRINGENT REQUIREMENTS

PCI Requirement	How Trend Micro Deep Security Addresses It
<p>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.</p>	<p>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.</p>
<p>6.2 Establish a process to identify newly discovered security vulnerabilities—for example, subscribe to alert services freely available on the Internet. Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.</p>	<p>Deep Security systematically monitors 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.</p>
<p>6.5 Develop all Web applications—internal and external, and including Web administrative access to application—based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes.</p> <p>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</p>	<p>Deep Security complements secure coding initiatives by providing strong detection and prevention capabilities that address attacks as identified by OWASP:</p> <ul style="list-style-type: none"> ▪ 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.
<p>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:</p> <ul style="list-style-type: none"> ▪ 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 	<p>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.</p>
<p>10 Track and monitor all access to network resources and cardholder data.</p> <p>10.3 Record at least the following audit trail entries for all system components for each event:</p> <ul style="list-style-type: none"> ▪ 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 	<p>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, and integrity monitoring events can also be forwarded to the SIEM or centralized logging server.</p>



PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD MEETING STRINGENT 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 in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines 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

© 2009 Trend Micro, Incorporated. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. WP01TBDS_ProtDynDC_090218

