Trend Micro Solutions for PCI DSS Compliance

A Trend Micro White Paper

Addressing PCI DSS Requirements with Trend Micro Enterprise Security

July 2010

I. PCI DSS AND TREND MICRO ENTERPRISE SECURITY

Targeted threats, distributed environments, and evolving technology make it especially challenging to achieve and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). Yet compliance alone is not enough to minimize the true risk to your enterprise. Trend Micro goes beyond addressing fundamental PCI requirements and offers practical solutions to truly safeguard your business infrastructure against the compromise of cardholder data.

Trend Micro Enterprise Security is a tightly integrated offering of content security products, services and solutions powered by the Trend Micro Smart Protection Network™. Together they deliver immediate protection from emerging threats while greatly reducing the cost and complexity of security management.

Trend Micro Enterprise Security Solutions offer direct mappings or compensating controls in the following PCI requirement areas:

PCI Requirement Area		Trend Micro Enterprise Solutions			
		Endpoint Security	Web Security	Messaging Security	Vulnerability and Threat Management
Build & Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data	●	●		●
	2. Do not use vendor supplied defaults…(shared hosting providers)	●	●	●	
Protect Cardholder Data	3. Protect stored cardholder data	●		●	
	4. Encrypt transmission of cardholder data across open, public networks	●		●	
Maintain a Vulnerability Protection Program	5. Use and regularly update antivirus software or programs	●	●	●	●
	6. Develop and maintain secure systems and applications	●	●		●
Implement Strong Access Measures	7. Restrict access to data 8. Assign unique IDs 9. Restrict physical data access				
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	●	●		
	11. Regularly test security systems and processes	●	●		●
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors	●	●	●	●

PCI Requirements: Direct Mappings or Compensating Controls

II. TODAY'S TOP PCI CONCERNS

Achieving and maintaining PCI compliance and true security requires constant evaluation of the potential impact of evolving threats, employee behavior, and new business and technology initiatives. Trend Micro offers you unique and cost-effective solutions to address today's top PCI challenges.

Business or Technology Driver	PCI Challenge	Trend Micro Solution
Virtualization	Virtualization allows for cost efficient and flexible datacenters and paves a path toward integrated cloud computing. But the complexity and fluidity of virtual environments pose special challenges, rendering traditional network security implementations for IPS, firewalls, and antivirus ineffective in preventing attacks on virtual servers or desktops that process or host cardholder data.	Trend Micro™ Deep Security provides advanced software-based security that protects physical, virtual and cloud-based servers with integrated IPS, firewall, configuration validation and more. Trend Micro™ Core Protection for Virtual Machines is designed specifically to meet the unique needs of the virtual environment with automated protection against malware. Trend Micro OfficeScan provides virtual desktop protection designed to maximize performance and capacity.
Effective Data Protection	Traditional data loss prevention and data encryption solutions are complex and cumbersome to manage and use.	Trend Micro Data Protection solutions protect and encrypt PAN data wherever it resides and enable secure collaboration without end-user actions or usability limitations.
Worker Mobility	Mobile laptops and PDAs are at risk for inbound attacks and cardholder data loss, but network security solutions are ineffective in these cases.	Trend Micro OfficeScan endpoint protection and web reputation technology keep your employee devices protected from malware both on and off the corporate network.
IT Risk Management	Reliably automating the discovery and rapid mitigation of vulnerabilities and evasive threats is critical to compliance and your risk posture. Even the best vulnerability and security defenses can be penetrated by zero-day and targeted threats.	Trend Micro Vulnerability and Threat Management solutions give you total risk visibility and remediation control over active evasive threats, software and systems vulnerabilities, web content, and IT policy compliance. Trend Micro Deep Security and OfficeScan deliver protection from zero-day threats and enable virtual patching to establish immediate protection for 'un-patched' or 'un-patchable' systems.
Controlling Cost and Complexity	According to Information Week, management complexity is the number one issue in security. With distributed environments, multiple point products and constant security signature updates, the cost and complexity of PCI compliance and secure operations is skyrocketing.	Trend Micro Enterprise Security and Smart Protection Network™ change the game by greatly simplifying security management and reducing resource requirements. We offer the breadth of solutions—including Software As A Service (SaaS) and virtualized appliances—that will allow you to reduce vendors, consolidate security and systems management, and cost effectively secure corporate and branch/POS (Point of Sale) environments.
Setting Your Budget Priorities	Achieving full PCI compliance is difficult and costly. The PCI Council has issued a 6-step "prioritized approach" whitepaper which offers guidance on a risk-based prioritized compliance roadmap.	Trend Micro OfficeScan, Deep Security, and Messaging Security products each address many of the top-tier priorities cited by the PCI Council.

III. ADDRESSING PCI COMPLIANCE WITH TREND MICRO ENTERPRISE SECURITY

Trend Micro Enterprise Security is a tightly integrated offering of content security products, services and solutions powered by the Trend Micro Smart Protection Network. Trend Micro enables you to go beyond addressing fundamental PCI requirements with practical solutions that truly safeguard your business infrastructure against the compromise of cardholder data.

These products protect distributed physical/, virtual, and cloud-based environments; support a wide array of platforms and operating systems; and offer a full range of deployment options including hosted, software, and virtual appliance.

PCI Challenge

PCI compliance is not a guarantee of security. How can I best insure that our customer data is secure from outside attack?

Trend Micro Solution

Malware is now an essential component of nearly all large-scale data breach scenarios. Trend Micro offers you a layered content security approach that: Protects your employees from importing threats; protects your resources from zero-day threats and sophisticated direct attacks; and directly protects your cardholder data from compromise

PCI Compliance

for Small & Medium Businesses

Trend Micro all-in-one Worry-Free™ Business Suite Vulnerability Management Services offer an endpoint, web and messaging security solution that helps small and medium business comply with many of the PCI requirements.

Trend Micro Enterprise Security

Endpoint Security
- PC, Server, Mobile Device Security
- Data Loss Prevention & Encryption
- Unified Security & Systems Management

Web Security
- Web Gateway Security
- Website Security

Messaging Security
- Email Gateway Security
- Mail & Collaboration Server Security
- Encryption & Archiving

Operating Environments
- Physical/Virtual/Cloud Computing Broad Platform/OS Support
- Flexible Deployment Options

Security Management
- Centralized Security Management
- Unified Endpoint Security & Systems Management

Solutions & Services
- Data Protection
- Dynamic Data Center
- Regulatory Compliance
- Threat Management Services
- Premium Support Service & more

Protecting Enterprise Data and Resources

IV. PCI COMPLIANCE WITH TREND MICRO SMART PROTECTION NETWORK

Trend Micro Enterprise Security products and services are powered by Trend Micro Smart Protection Network—a next-generation cloud-client infrastructure that combines sophisticated reputation-based technology, feedback loops, and the expertise of Trend Labs researchers to deliver real-time protection from emerging threats.

The Smart Protection Network threat intelligence serves as a compensating control to address the following PCI DSS Requirements:

- **Req. 2.2** (…address all known security vulnerabilities… as related to system configurations), with current and comprehensive vulnerability and threat research

- **Req. 5.2** (Ensure that all antivirus mechanisms are current), with current and accurate intelligence on malware including viruses, spyware, and data-stealing malware
- **Req. 6.2** (Establish a process to identify newly discovered security vulnerabilities…), with automated tools to identify new vulnerabilities and free, public alerts on emerging threats via TrendWatch Threat Resource Center
- **Req. 6.6** (For public-facing web applications, address new threats and vulnerabilities…), with web reputation services, and research to uncover new web threats

PCI Challenge

A new malware threat is created every 2 seconds. Signature-based security leaves a window of new threat vulnerability that can vary from hours to days depending on when systems are updated.

Trend Micro Solution

The Smart Protection Network delivers real-time protection without signature file dependence, minimizing your vulnerability to new threats to your PAN data.

The Smart Protection Network continuously evaluates and correlates threat and reputation intelligence for websites, email sources, and files. This enables Trend Micro Enterprise Security solutions to block threats at the source, before they reach your network and can damage your business. You get the best in real-time threat protection without the delays, higher risks, and management complexity of conventional signature-based security products. Threat intelligence from the Smart Protection Network drives key Trend Micro Enterprise Security Solutions including: Endpoint Security, Web Security, Messaging Security, and Threat Management Services.

V. PCI COMPLIANCE WITH TREND MICRO ENDPOINT SECURITY SOLUTIONS

Trend Micro Endpoint Security solutions safeguard corporate and mobile endpoints with anti-malware, intrusion defense and data protection solutions coupled with real-time reputation services delivered through the Smart Protection Network. Endpoint Security also includes solutions for advanced protection for physical and virtual servers, virtual desktops and unified security and systems management.

PCI Challenge

Increasing employee use of remote laptops, mobile devices and poorly secured Web 2.0 applications open your network to employee transmitted exploits that can steal cardholder data.

Trend Micro Solution

OfficeScan protects off-network PCs as well as smart phones and PDAs. Your employees are protected wherever they are.

TREND MICRO OFFICESCAN™

Trend Micro OfficeScan provides superior defense against threats—both on and off the corporate network—combining world-class malware protection with innovative in-the-cloud security from the Smart Protection Network. OfficeScan offers a single solution to protect desktops, virtual desktops, laptops, servers, storage appliances, and smart phones. A flexible plug-in architecture and extended platform support ensure better security, lower management costs, and ultimate flexibility.

Trend Micro Core Protection for Virtual Machines provides automated malware protection designed specifically to meet the unique needs of the virtual environment. Features include active and dormant VM protection, WMware vCenter management integration, and a performance-optimized architecture.

With proper deployment and configuration, both of these solutions directly meet the following PCI requirements:

- **Req. 1.4** (install personal firewall software) with inbound connection control
- **Req. 5.1** (deploy antivirus software) and **Req. 5.2** (ensure all antivirus mechanisms are current) with auto updates for endpoint antivirus engines and signature files

They also serve as a compensating control for the following requirements:

- **Req. 1.2** (build a firewall that restricts connections from un-trusted networks) by protecting the endpoint from unauthorized inbound connections
- **Req. 5.1** (deploy antivirus software) and **Req. 5.2** (ensure current antivirus signatures)
  - File Reputation technology moves the burden of signature management into the cloud and buys time for enterprises trying to keep virus signature files up to date with real-time query of the safety of a new file
- **Req. 12.6** (Implement a formal security awareness program) with virus scan notification to end users

PCI Challenge

Server virtualization saves money, but introduces difficult challenges to PCI compliance and your overall security posture.

Trend Micro Solution

Deep Security and Core Protection for Virtual Machines are designed to fully support the complex and fluid configurations of virtualized environments, allowing you to isolate and secure payment processing applications wherever they physically reside.

TREND MICRO ENDPOINT SECURITY PLATFORM

Trend Micro™ Endpoint Security Platform provides a unified platform for security and systems management. A single server, management console and lightweight client enable you to distribute software, manage assets, maintain availability, and secure data across all clients and servers regardless of location or network connectivity. Key components under management include:

- Core Endpoint Security and Web Protection
- Data Loss Prevention
- Patch Management
- Power Management

Centralized reporting on endpoint protection policies and status helps prepare for an actual PCI audit and also helps efficiently demonstrate endpoint security PCI compliance to auditors. In addition to simplifying compliance reporting for endpoint security, this solution helps meet the following PCI requirement with direct mappings:

- **Req. 6.1** (Ensure latest vendor-supplied security patches installed)
  - Patch Management module efficiently applies patches to systems by prioritizing vulnerable systems and grouping multiple patches

The solution also serves as direct mapping or in the following area:

- **Req. 5.1** (deploy antivirus software) and **Req. 5.2** (ensure current antivirus signatures)

The Web Protection module serves as a compensating control in the following area:

- **Req. 5.1** (deploy antivirus software) and **Req. 5.2** (ensure current antivirus signatures)

TREND MICRO DEEP SECURITY

Trend Micro Deep Security provides comprehensive software-based security for critical business servers operating in standalone, virtual, and cloud-based environments. Key features include deep packet inspection (enabling IDS/IPS, application control and web application protection), firewall, integrity monitoring, log inspection, and patch management.

PCI Challenge

Applying server security in the context of virtualized systems, ensuring safeguards both on physical and virtual system.

Trend Micro Solution

Deep Security technology is aware of both the physical (IP address, hardware) and virtual environment, allowing policy-based control over different virtual machines on the same physical system.

The solution offers a direct mapping to the following PCI requirements:

- **Req. 1.2 and 1.3** (build a firewall that restricts connections from un-trusted networks… restricts inbound and outbound traffic… prohibit direct public access between the Internet and cardholder environment) with a sophisticated, centrally managed, software-based stateful firewall to protect servers and endpoints from unauthorized inbound and outbound connections
- **Req. 1.4** (Install personal firewall software) with a sophisticated, centrally managed, stateful firewall for multiple platforms including Microsoft Windows and Linux
- **Req. 2.2.1** (one primary function per server, including configuration standards for all systems components addressing known vulnerabilities), with security profiles that can be used to specify configurations for unique server functions and restrict or prevent access to services and protocols; current and comprehensive vulnerability and threat research used to issue vulnerability shield updates for affect applications and operating systems
- **Req. 2.2.2** (Disable all unnecessary and insecure services and protocols) by restricting specific services and protocols from running on the server
- **Req. 10.5** (secure audit trails.. use file integrity monitoring on logs) by using a complete file integrity monitoring capability with hashes of confidential files containing cardholder data and monitoring/ alerting on security events related to these files
- **Req. 11.4** (use IDS, and/or intrusion prevention system (IPS)), by blocking inbound attacks with up-to-date vulnerability shielding, including vulnerability updates based on the CVE standard
- **Req. 11.5** (Deploy file integrity monitoring software on logs) with an Integrity Monitoring module which goes even further to monitor 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.

The solution also serves as compensating controls for several areas:

- **Req. 2.4, A.1:** (Hosting providers must protect each entity's environment) allows enterprises to enforce security of their business systems, even if the hosting provider's environment is compromised
- **Req. 5.1, 5.2** (anti-virus software) by limiting the risk of malware, including viruses, with software-based IPS, which can block processes from accessing certain services or resources on the host
- **Req. 6.1** (latest vendor supplied security patches) with virtual patching that monitors for system compromise and blocks malicious activity on un-patched systems, helping organizations buy time while patches are being tested and rolled out to systems
- **Req. 6.2 (**Establish a process to identify newly discovered security vulnerabilities) with ongoing vulnerability research and security update services (leveraging the Smart Protection network) including a "recommendation engine" to assist in maintaining appropriate vulnerability coverage in line with patch management strategies
- **Req. 6.5** (develop all web applications based on secure coding guidelines) by providing strong detection and prevention capabilities that address attacks as identified by OWASP

- **Req. 6.6** (for public facing applications, address new threats and vulnerabilities) by providing web-application–layer protection and detection/prevention of attacks, including encrypted ones, to compensate for applications that may not have been built with cardholder security in mind in addition to virtual patching of underlying web server applications and operating systems
- **Req. 10.2 and 10.3** (Track and monitor all access to network resources and cardholder data, audit trails) with default rules and custom log inspection capabilities for the most common enterprise operating systems and applications to enable sophisticated collection and forwarding of PCI compliance related security events
- **Req. 10.6** (Review logs for all system components) by monitoring critical OS and application logs in real time for relevant security events, and forwarding these events to a SIEM or centralized logging server for further analysis, correlation, alerting, and archival—automating the process of log reviews
- **Req. 12.9** (Implement an incident response plan…Include alerts from intrusion detection, intrusion prevention and file integrity monitoring systems) with near real-time and scheduled alerts via email, console, or SIEM integration plus delegated administration and management to assist in workflow of security incident response.

TREND MICRO DATA LOSS PREVENTION

Trend Micro DLP provides extremely accurate and effective detection and protection of sensitive data on the endpoint. Sophisticated tagging, analytics, and small footprint ensure minimal performance impact, and PCI templates and reports simplify tracking and protecting cardholder data.

PCI Challenge

Endpoint data loss prevention products typically have a strong negative impact on system performance.

Trend Micro Solution

Trend Micro DLP provides extremely accurate and effective detection and protection with an exceptionally small footprint. Sophisticated tagging and analytics ensure minimal performance impact.

This solution directly addresses the following PCI requirement:

- **Req. 4.2** (never send unencrypted PANs via email) by detecting cardholder data on the endpoint and blocking it from being sent by email or webmail.

The solution also serves as a compensating control in the following areas:

- **Req. 3.1** (Keep cardholder data storage to a minimum), **Req. 3.2** (Don't store authentication info), **Req. 3.4** (Render PAN, at minimum, unreadable anywhere it is stored) by easily detecting cardholder data on the endpoint through discovery, using predefined templates for PCI, and allowing administrators to configure how the violation is handled. Trend Micro DLP can:
  - Automatically detect and block copy of cardholder data to external media
  - Enforce use of built-in data encryption module to copy data onto USB devices (optional)
- **Req. 9.7** (Control distribution of media containing cardholder data) and **Req. 9.9** (Control storage and accessibility of media containing cardholder data) by blocking the copy or movement of cardholder data to external media or enforcing encryption so that even if it fell into the wrong hands, no cardholder data could be readable
- **Req. 12.6** (Implement a formal security awareness program) with end-user alerts that explain the policy violation while the action is being attempted and dialog boxes which require the user to justify their action before proceeding

VI. PCI COMPLIANCE WITH TREND MICRO MESSAGING SECURITY

Trend Micro Messaging Security products offer a comprehensive layered approach to communications security, combining gateway email security, mail server protection, email encryption, and extended protection for instant messaging and collaboration systems. Powered by the Smart Protection Network, these products:

- Protect your business from external threats such as spam, data stealing spyware, malware, and phishing. Stopping the threat at the network edge before it can infect your network.
- Ensure that your business communications systems do not become host to infection
- Protect sensitive data exposure via content filtering and identity-based encryption

TREND MICRO EMAIL ENCRYPTION

Trend Micro Email Encryption offers advanced identity-based encryption that allows universal reach without pre-registration. Unlike conventional PKI encryption, Trend Micro email encryption uses cloud-based key management to generate keys on demand without the need for certificates and per pair pre-registration. End-user encryption as well as policy-based automated gateway encryption ensures that all sensitive correspondence is protected. By simply accessing the Zero Download Reader web page, users can view the encrypted emails, allowing for secure file sharing with anyone, anywhere, and at any time.

PCI Challenge

Ensuring unencrypted PAN data is not present in electronic communications.

Trend Micro Solution

Trend Micro Messaging Security identifies PAN data based on keywords, lexicons, attachment characteristics and customizable policies. The email can be automatically encrypted or be blocked and the sender notified.

This solution offers direct mappings for the following PCI requirements:

- **Req. 2.4, A.1** (Hosting providers must protect each entity's environment), with key management for encryption performed in the cloud, each entity's keys are stored securely to avoid any compromise to emails which may contain cardholder data
- **Req. 4.1** (Use strong cryptography and security protocols such SSL/TLS or IPSEC), with IPSEC based encryption of emails using end-user identity to generate the private key
- **Req. 4.2** (Never send unencrypted PANs by end-user messaging technologies…) by automatically encrypting email based on policy, using content filtering from Trend Micro Messaging Security
  - The solution also solves the problem of complicated key management, user pre-registration, and automation with identity-based encryption which uses cloud-based key management to generate keys on demand without the need for certificates and per pair pre-registration, nor does it requires end users to decide which emails should be encrypted
  - Businesses have the option of encrypting emails from gateway to gateway, to prevent compromise over public networks or they can further ensure privacy by enforcing end to end encryption, to prevent compromise on the enterprise network

TREND MICRO EMAIL AND COLLABORATION SECURITY

Trend Micro Email and Collaboration Security Solutions (InterScan Messaging Security, ScanMail Suite, and Communication and Collaboration Solution) provide outbound content filtering and inbound malware protection for enterprise email systems, enterprise IM (Microsoft OCS), collaboration software (Microsoft SharePoint) and Microsoft Exchange.

The solutions offer direct mappings for the following PCI requirements:

- **Req. 2.4, A.1** (Hosting providers must protect each entity's environment), InterScan Messaging Hosted Security ensures data storage security for any entity using this shared service for antispam and antivirus protection
- **Req. 4.2** (Never send unencrypted PANs by end-user messaging technologies) by identifying and blocking, based on policy, PAN data based on keywords, lexicons, attachment characteristics, and customized data rules.
- **Req. 5.1** (Deploy antivirus software on all systems commonly affected by malicious software…) and **Req. 5.2** (Ensure that all antivirus mechanisms are current…), the solutions also provide protection for inbound emails and instant messages by blocking malicious attachments and web links to malicious websites.
  - Spam emails in particular are notorious for tricking users into visiting malicious websites, but with Trend Micro's ability to stop up to 99% of spam at its source, before reaching employee desktops and your network, enterprises also benefit from increased user productivity and fewer IT costs due to mail server storage or archive of junk email
- **Req. 12.6** (Implement a formal security awareness program…) by providing user training at the moment of the violation through automated email notifications of the policy violation. This approach makes a subsequent violation less likely

The solution offers compensating controls in the following areas:

- **Req. 1** (Install and maintain a firewall configuration to protect cardholder data) since firewalls cannot block inbound SMTP/email traffic without disrupting business, email security must inspect inbound connections and exert control if the sender is malicious (e.g. anti-spam) or the content is malicious (e.g. antivirus)
- **Req. 2.2.1** (one primary function per server) and **Req. 6.1** (system with security patches) with a hardened and tuned operating system running email security (virtual appliance version)

VII. PCI COMPLIANCE WITH TREND MICRO WEB SECURITY

Trend Micro Web Security solutions provide website protection and PCI Compliance Scanning for corporate websites as well as employee web access security at the gateway via Smart Protection Network reputation services, content scanning, and URL filtering policies.

TREND MICRO VULNERABILITY MANAGENT SERVICES

Trend Micro Vulnerability Management Services is a SaaS offering which helps you to continuously secure your websites and remain compliant by identifying vulnerabilities and associated risk across a wide range of web applications, databases, networks, operating systems, commercial applications, and other software products.

PCI Challenge

Our websites are constantly being updated. How can we ensure that vulnerabilities aren't introduced?

Trend Micro Solution

Vulnerability Management and PCI Scanning Service provides automated and manual scanning of your websites for both web threats and vulnerabilities, making use of the most current to ensure your compliance and security.

This solution offers direct mappings in the following areas:

- **Req. 11.2** (Run internal and external network vulnerability scans at least quarterly and after any significant change in the network … Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV))Trend Micro fulfills this requirement as an ASV through scanning services
- **Req. 6.6** (For public-facing web applications, address new threats and vulnerabilities on an ongoing basis …manual or automated application vulnerability assessment…) with continuous monitoring of your websites for vulnerabilities,
  including SQL injection attacks, commonly used to access internal databases where credit card data may be stored

The solution also offers compensating controls in the following areas:

- **Req. 6.3** (secure software development) by scanning these applications during testing phases, can uncover these vulnerabilities and fix the vulnerabilities before production deployment. Compensates for rapid application development common in today's Web 2.0 world, where security considerations are not necessarily in the forefront.
- **Req. 6.5** (Develop internal and external web applications based on secure coding guidelines) by scanning for and detecting vulnerabilities on external web applications, providing vulnerability reports for developers to review and develop patches
- **Req. 11.2** (Run internal and external network vulnerability scans at least quarterly and after any significant change in the network…)
  - Beyond quarterly scans, the solution can provide continuous scanning on both internal and external networks, further mitigating the risk of compromise to cardholder data security.
  - Vulnerability reports and recommended remediation actions enable administrators to mitigate risks efficiently.

TREND MICRO INTERSCAN™ WEB SECURITY

Trend Micro InterScan™ Web Security provides immediate protection against web threats by integrating multiple layers of protection at the Internet gateway and also provides real-time monitoring and reporting of Internet activity to facilitate better risk management. Powered by the Smart Protection Network, it combines award-winning antivirus and antispyware with cloud-based web reputation security and URL filtering to detect and block threatening website access based on reputation and company policy. It also filters HTTP, HTTPS, and FTP traffic of malicious content and triggers agent-less cleanup.

The solution serves as a compensating control for the following PCI requirements:

- **Req. 5.1** (deploy antivirus software) and **Req. 5.2** (ensure all antivirus mechanisms are current) with award-winning antivirus and antispyware
  - Goes further to provide cloud-based web reputation security and URL filtering to detect and block threatening website access based on reputation and company policy
  - In Reverse Proxy deployment mode, it prevents the posting of malicious web content to website hosts, limiting the liability of the enterprise as a possible tool in propagating more web-based malware attacks

TREND MICRO DEEP SECURITY™

Trend Micro Deep Security provides comprehensive software-based security for critical web servers operating in standalone, virtual, and cloud-based environments. Key features include deep packet inspection (enabling IDS/IPS, application control and web application protection), firewall, integrity monitoring, log inspection and patch management. See section on Endpoint and Server security for additional solution capabilities.

This solution offers direct mappings in the following areas:

- **Req. 1.1, 1.2, 1.2.1, 1.3, 1.4** (various requires for firewalling between systems storing cardholder data and un-trusted networks) by serving as a full-featured, software-based firewall with the ability to monitor and block inbound web traffic
- **Req. 2.2, 2.2.1, 2.2.2** (configuration standards, one function per server, disable unnecessary services) with controls to limit a web server only to protocols and services necessary for a secure and available web service
- **Req. 6.6** (For public-facing Web applications, address new threats and vulnerabilities …protect using vulnerability assessment, web application firewall) with built-in protection rules for SQL injection and cross-site scripting attacks as well as various web application vulnerabilities. Monitoring and detection of web activity also provides early indication of web-based attacks.
- **Req. 11.5** (Deploy file integrity monitoring software on logs) with an Integrity Monitoring module which can monitor attempts to hide Web-based attacks by tampering with web application logs. Described further in the Endpoint and Server security section.

The solution serves as a compensating control for the following PCI requirements:

- **Req. 5.1, 5.2** (anti-virus software) by limiting the risk of malware infecting the web application server with intrusion prevention capabilities
- **Req. 6.1** (latest vendor supplied security patches) and **Req. 6.2** (Establish a process to identify newly discovered security vulnerabilities) with virtual patching and vulnerability research and updates as described in the Endpoint and Server Security section.
- **Req. 6.5** (Develop all web applications based on secure coding guidelines) by protecting poorly written software with web vulnerability detection and protection as described for Req. 6.6, above.
- **Req. 11.2** (Run internal and external network vulnerability scans) and **Req. 11.3.2** (penetration testing including ones mentioned in Req. 6.5, related to secure web application development)
  - By implementing Deep Security after vulnerability and penetration testing, its benefit can clearly be shown, with protection and automated remediation of system and application vulnerabilities
  - Repeating vulnerability and penetration tests after Deep Security leave administrators with a manageable list of remediation tasks which are out-of-scope of automated methods

VIII. PCI COMPLIANCE WITH TREND MICRO VULNERABILITY MANAGEMENT SERVICES

Trend Micro Vulnerability Management Services automate the process of vulnerability management and policy compliance across the enterprise, providing network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Policy compliance features allow security managers to audit, enforce and document compliance with internal security policies and external regulations. And it's easy to implement. As an on demand Software-as-a-Service (SaaS) solution, there is no infrastructure to deploy or manage.

This solution offers direct mappings in the following areas:

- **Req. 2.2** (Develop configuration standards for all system components...) Create host configuration policies and hardening standards based on standards such as ISO 7799/27001, Cobit, CIS or NIST. Automate the necessary workflow of assessing assets, identifying non-compliant ones, creating remediation tickets, and reporting on status and progress.
- **Req. 6.2** (Establish a process to identify newly discovered security vulnerabilities...) Automated vulnerability scanning services identifies vulnerabilities, identifies appropriate patches and verifies patch deployment.
- **Req. 6.6** (For public-facing web applications, address new threats and vulnerabilities...) Vulnerability Management Services PCI's WAS Module automates regular scans of all web applications and the associated remediation effort in case security risks are found.
- **Req. 11.2** (Run internal and external network vulnerability scans at least quarterly...) Automated vulnerability scanning identifies internal/external vulnerabilities, identifies appropriate patches, and verifies patch deployment

This solution may serve as a compensating control in the following areas:

- **Req. 6.3** (secure software development) and **Req. 6.5** (Develop internal and external web applications based on secure coding guidelines) by scanning applications for vulnerabilities the solution finds vulnerabilities that have been introduced through insecure coding practices

IX. PCI COMPLIANCE WITH TREND MICRO THREAT MANAGEMENT SERVICES

Trend Micro Threat Management Services deliver best-in-class threat discovery and remediation services for zero-day and targeted attacks based on non-intrusive network appliances, Smart Protection Network threat analysis, and dedicated threat researchers. The solution complements traditional protective security measures such as antivirus, email security, web security, and vulnerability scanning with an additional layer that detects and remediates malware that has infiltrated your defenses.

Both continuous and comprehensive monitoring of all inbound and outbound traffic for malicious activity immediately identifies data-stealing malware targeting cardholder data and, if desired, can automatically remove that malware to eliminate any risk of a data breach. This solution therefore serves as a compensating control for the following PCI DSS requirements:

PCI Challenge

Certain threats can evade the security of a PCI-compliant company.

Trend Micro Solution

PCI DSS requirements focus primarily on threat prevention and do not address the likelihood that zero-day and targeted exploits may evade security measures and penetrate core systems. Trend Micro Threat Management Services detect and remediate these active resident threats before they can steal PAN data.

- **Req. 5.1** (Deploy antivirus software on all systems commonly affected by malicious software…) and **Req. 5.2** (Ensure that all antivirus mechanisms are current…) for cases where zero-day attacks are in progress or unmanaged systems without antivirus are infected. Through monitoring and remediation services, the solution can protect endpoints from data-stealing malware.
- **Req. 6.2** (Establish a process to identify newly discovered security vulnerabilities…), with automated threat discovery
- **Req. 6.3** (secure software development) and **Req. 6.5** (Develop internal and external web applications based on secure coding guidelines) by monitoring traffic from business applications which handle cardholder data. If these applications are vulnerable and then later exploited, the solution would catch these exploits and the organization could be told to request or develop a patch for the vulnerable (and compromised) application.
- **Req. 11.2** (Run internal and external network vulnerability scans) and **Req. 11.3** (external and internal penetration testing). Even though the service neither scans for vulnerabilities nor does it launch actual exploits on end user systems, the desired effect of all these safeguards is to ultimately rid business systems of malware.

X. SUMMARY

Trend Micro offers proven solutions that address most PCI DSS requirements and enable you to truly safeguard your business infrastructure against the compromise of cardholder data. The following table summarizes the products that address each requirement for large and mid-size enterprises. For small business, Trend Micro also offers all-in-one Worry-Free ™ Business Security Suites.

PCI Requirement	Direct Mapping	Compensating Control
1.1: Establish firewall and router configuration standards	• Deep Security	
1.2: Firewall connections between untrusted networks and any system containing cardholder data	• Deep Security	• OfficeScan • Worry-Free Business Security • Trend Micro Messaging Security Solutions
1.3: Prohibit direct public access between the Internet and any system component in the cardholder data environment.	• Deep Security	
1.4: Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet	• OfficeScan • Worry-Free Business Security • Deep Security	
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.	• Vulnerability Management Services • Deep Security (Req. 2.2.1, 2.2.2)	• Trend Micro Messaging Security Solutions
2.4, A.1: Hosting providers must protect each entity's environment	• Worry-Free Business Security • InterScan Hosted Email Security • Email Encryption	• Deep Security
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	• Email Encryption	• Data Loss Prevention
3.2: Don't store authentication info	• Email Encryption	• Data Loss Prevention
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media,…)	• Endpoint Encryption	• Data Loss Prevention • Email Encryption Client
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse…	• Endpoint Encryption • Email Encryption	
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for the encryption of cardholder data…	• Endpoint Encryption • Email Encryption	

PCI Requirement	Direct Mapping	Compensating Control
4.1 Use strong cryptography and security protocols such SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	• Email Encryption	• Endpoint Encryption
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	• Data Loss Prevention • Email Encryption • IM Security for Microsoft Office Communications Server • ScanMail Suite for Microsoft Exchange	• Endpoint Encryption
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	• OfficeScan • Deep Security • Worry-Free Business Security • Web Protection Module (Endpoint Security Platform component) • InterScan Messaging Security • PortalProtect for Microsoft SharePoint • ScanMail Suite for Microsoft Exchange • IM Security for Microsoft Office Communications Server • Threat Management Services	• InterScan Web Security
5.2 Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.	• OfficeScan • Worry-Free Business Security • Threat Management Services (compensating control) • PortalProtect for Microsoft SharePoint • ScanMail Suite for Microsoft Exchange • IM Security for Microsoft Office Communications Server	• Deep Security • InterScan Web Gateway Security
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed.	• Vulnerability Management Services • Patch Management Module (Endpoint Security Platform component) • Deep Security • OfficeScan Intrusion Defense firewall (compensating control)	

PCI Requirement	Direct Mapping	Compensating Control
6.2 Establish a process to identify newly discovered security vulnerabilities	• Vulnerability Management Services	• Threat Management Services
6.3 Develop software applications in accordance with PCI DSS…		• Vulnerability Management Services • Deep Security • Threat Management Services
6.5 Develop internal and external web applications based on secure coding guidelines		• Vulnerability Management Services • Deep Security • Threat Management Services
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:	• Vulnerability Management Services • Deep Security	
9.7: Control distribution of media containing cardholder data		• Data Loss Prevention
9.9: Control storage and accessibility of media containing cardholder data		• Data Loss Prevention
10.5 Secure audit trails so they cannot be altered.	• Deep Security	
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network …	• Vulnerability Management Services	• Deep Security
11.4 Use intrusion detection systems	• Deep Security	
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files;	• Deep Security	
12.6 Implement a formal security awareness program	• Trend Micro Messaging Solutions	• OfficeScan • Worry-Free Business Security • Data Loss Prevention • Deep Security
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach	• Deep Security • Threat Management Services	

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