PCI DSS 3.0 Compliance

How Trend Micro Cloud and Data Center Security Solutions Can Help
INTRODUCTION

Merchants and service providers that process credit card payments must comply with the Payment Card Industry Data Security Standard (PCI DSS), now at Version 3.0. Whether the transaction occurs in a store or online, and regardless of the environment, from physical Point of Sale devices, to virtualized servers, or web servers in a public cloud, PCI DSS 3.0 mandates that these organizations are responsible for the security of their customers’ cardholder data.

WHAT’S NEW IN PCI DSS 3.0?

The Payment Card Industry Data Security Standard 3.0 was published in November 2013, and became effective January 1, 2014. The majority of changes that were introduced are clarifications to 2.0 guidance, focused on evolving the way that organizations protect sensitive cardholder data. At a summary level, the new guidance can be grouped into 3 main categories:

1. Increased Education and Awareness: As with all forms of security, even the best technology for protecting cardholder data may not be effective if improperly implemented and maintained. The new guidance adds overall clarity with recommendations on best practices for implementing security, as well as specific changes in Requirement 8.4 on password education and Requirement 9.9 on POS security training and education.

2. Greater Flexibility: There is recognition of the fact that there is more than one way to implement security, which enables organizations to comply with the regulations while fitting the security approach into their particular business situation. Examples include Requirement 8.2.3, which enables organizations to set appropriate password strength for their application, and Requirement 10.6 which introduces flexibility into the log review process based on an organization’s risk management strategy.

3. Security as a Shared Responsibility: Building on the February 2013 release of a supplement focused on the use of the cloud for applications using and storing cardholder data1, PCI DSS 3.0 guidance clearly recognizes the impact and pervasiveness of the use of the cloud and third parties for implanting and hosting applications. The concept of a shared responsibility for security is clearly outlined and guidelines are provided to show where security responsibilities lie in a distributed infrastructure ownership model.

As a part of the guidance, Requirement 12.9 specifically spells out PCI DSS responsibilities for service providers, including hosting providers like a cloud service provider (CSP), such as Amazon Web Services or Microsoft Azure. Regardless of size or locations, CSPs will need to review the list of changes (there are many small changes and clarifications) and plan for the potential business impacts before the deadline of June, 2015. Key highlights relevant to cloud service providers include:

- Increased education and awareness for employees who manage the infrastructure and applications that may involve cardholder data
- Clarity around the use of encryption and cryptographic keys for data protection
- Account access procedures that limit CSP access to any card payment infrastructure
- More detailed and flexible guidance about password strength and use
- Improved descriptions of the boundaries for privileged and standard user access controls
- Remote access guidelines for CSPs that may also have remote access to their customer’s payment card data environments
- New requirements around onsite personnel and physical access
- Increased reporting and visibility into new account creation and privilege escalation by individuals with root and/or administrative authority

---

1 Information Supplement: PCI DSS Cloud Computing Guidelines, February 2013
An example provided by the PCI Council specifically around cloud deployments shows that there are distributed responsibilities for securing cardholder data. Deploying organizations that leverage a CSP need to embrace and understand the shared responsibility for security concept and work with their CSP to understand their role in securing cardholder data.

More information on what's new in the 3.0 guidance can be found online at https://www.pcisecuritystandards.org/.
TREND MICRO CLOUD AND DATA CENTER SECURITY SOLUTIONS

As a part of a broad Trend Micro Cloud and Data Center Security Solution, Trend Micro has three security offerings that provide proven security across the modern data center (including physical and virtual environments) and the cloud. These offerings complement the security provided by service providers, including cloud service providers (CSPs) such as Amazon Web Services (AWS) and Microsoft Azure, and can help organizations achieve PCI DSS 3.0 compliance.

**Trend Micro Deep Security** is a comprehensive server security platform that protects physical, virtual and cloud-based servers from data breaches and business disruptions while enabling compliance. This offering simplifies security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated security modules provide flexible deployment options and enable organizations to ensure server, application, and data security across the modern data center as well as the cloud, including virtual desktops and embedded devices.

With Deep Security, customers can employ any combination of the comprehensive set of capabilities, including anti-malware, web reputation, host-based firewall, intrusion prevention, integrity monitoring, and log inspection. Built on a technology foundation that is proven across thousands of customers and millions of servers, deployment options include automated agent deployment in the data center or cloud, as well as agentless protection in a VMware virtualized environment. The result is an adaptive and efficient security platform that protects mission-critical enterprise applications and data from business disruptions and breaches.

**Deep Security Key Benefits:**

- Single technology platform with broadest set of recommended security capabilities for physical, virtual and cloud deployments.
- Eases operational impacts with a centralized management console that enables streamlined policy and resource management.
- Optimized for virtualized environments, including VMware, with automated, agentless security that increases performance and reduces management overhead.
- Optimized for cloud deployments, including AWS, with support for leading cloud deployment tools (Chef, Puppet, OpWorks), and the ability to automatically provision and de-provision security across instances, removing the need for manual intervention and ensuring compliance with built-in reporting on all security events.

**Trend Micro SecureCloud** provides data protection for cloud deployments using encryption and leveraging policy-based key management to ensure effective protection of sensitive corporate information. This protection applies to securing both boot and data volumes on servers deployed on leading cloud service providers, including AWS. This allows businesses to control their own keys, ensuring they aren’t tied to one provider’s encryption system. SecureCloud provides a patent-pending key management system that enables organizations to set policies that determine where and when encrypted data can be accessed. In addition, server validation applies identity and integrity rules when servers request access to secure storage volumes. SecureCloud's simple approach safely delivers encryption keys to valid devices without the need to deploy an entire file system and management infrastructure.

With SecureCloud, organizations can ensure that data is not only protected while stored in the cloud, but can also help with data destruction needs, with the ability to destroy the keys used to encrypt data and effectively make it not accessible any more. This protection helps support internal governance and ensures compliance with regulations such as HIPAA, HITECH, Sarbanes-Oxley, GLB and PCI DSS 3.0. SecureCloud also features FIPS 140-2 certification to support government agencies and companies that mandate high security standards.
SecureCloud Key Benefits:

- Enables data protection in private and public clouds environments across boot and data volumes, including safe storage recycling by rendering any data remnants indecipherable
- Facilitates compliance and supports internal governance through the ability to define when and where information is accessed through policy-based key management
- Enables organizations to secure information independent of a CSP, avoiding vendor lock-in and ensuring separation of controls

Trend Micro Deep Security for Web Apps is a comprehensive application security solution that delivers continuous vulnerability detection with automated scanning, expert business logic testing and comprehensive reporting. It also protects applications with unlimited globally-trusted SSL certificates and speeds mitigation of discovered vulnerabilities through native web application firewall rule integration and intrusion prevention capability. Whether an application is hosted in the data center or in a public cloud like AWS, Deep Security for Web Apps can ensure that applications are scanned for vulnerabilities continuously, helping with compliance with PCI DSS 3.0 requirements.

Deep Security for Web Apps Key Benefits:

- Continuously scans web applications for vulnerabilities and removes distracting false positives. Includes being able to operate automatically in AWS as one of a select group of Pre-Approved Vulnerability Scanning vendors
- Finds application logic flaws with hands on expert testing
- Identifies security vulnerabilities at the platform layer and provides advice on remediation along with automated virtual patching
- Integrates with leading WAF vendors and provides customized rules to protect applications without patching or updates.

CLOUD AND DATA CENTER SECURITY & PCI DSS 3.0 REQUIREMENTS

**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.

Trend Micro Deep Security host-based firewall is a stateful firewall product designed to be fully configurable. Default firewall policies may be used or customized to each protected machine within a deployment.

Firewall Rules can be applied based on a combination of protocol, port use, traffic direction, interfaces in use, and host identification triggers. As it is a stateful firewall, rules can also be implemented to protect against various reconnaissance scans and denial of service attacks.

Firewall protection can be implemented on physical and cloud-based machines by installing Deep Security Agents. Agentless protection of Virtual Machines in a VMware environment can be enabled by installing a Deep Security Virtual Appliance on the VMware ESX/ESXi™ hypervisor hosting the VMs. The Virtual Appliance provides firewall protection to the VMs without having to install a Deep Security agent on each guest VM.

Increased protection is possible by also installing a Deep Security agent on the guest VM for a Coordinated Approach. In this scenario, the Agent provides primary protection and the Virtual Appliance acts as a backup. Trend Micro Deep Security firewall facilitates network segmentation through stateful firewall implementation.
Trend Micro Deep Security firewall provides capabilities for managing network firewall configuration standards for process, procedure and testing approvals, as well as network management roles and responsibilities and requirements for periodic review of standards and configurations.

Trend Micro Deep Security firewall provides capabilities for defining standards related to confidential or sensitive information of what can or cannot be disclosed to authorized or unauthorized third parties, such as private IP address or routing information. The offering also includes the ability to log and report on traffic at the host-level, which is important for compliance and audit when deployed in public cloud environments, such as AWS, where access to the built-in logs for the Cloud Service Provider (CSP) are not available.

Trend Micro Deep Security firewall provides capabilities to validate only necessary services are enabled and functionality for administrators to review any enabled insecure services.

Requirement 2:
Do not use vendor-supplied defaults for system passwords and other security parameters.

Trend Micro Deep Security has configurable security profiles that can be defined and customized for each type of machine role, helping to ensure that each server instance meets the one function-per-server requirement and that only the necessary services are accessible.

Security profiles can include a variety of proactive rules to lock down each machine’s role, ranging from firewall rules to block access to service ports, to configuration and integrity monitoring of application and service configuration files and registry, to auditing of service and administrative log events for unauthorized changes. Security policies enable consistent configurations to be applied to common groups of machines, simplifying the audit process and ensuring that changes made to the group policy are automatically inherited and applied to all machines assigned that policy.

Deep Security also supports local overrides so that additional policy assignments and configurations can be made to further secure particular machines/servers and account for different configuration requirements.

Deep Security’s Recommendation Scan feature profiles each machine instance being protected and ensures that each machine is running the necessary security policy rules (Intrusion Prevention, Integrity Monitoring, and Log Inspection) throughout the machine lifecycle. The Recommendation Scan feature can be considered the equivalent of ‘auto-tuning’ the security policies of the machine instance to ensure optimum protection.

Deep Security for Web Apps vulnerability scanning engine automatically checks application and platform components for known vulnerabilities and misconfigurations, including the use of vendor-supplied base passwords. When detected, the offering reports on the vulnerability with specific recommendations for remediation. This can be used in conjunction with Deep Security’s comprehensive range of security capabilities to detect vulnerabilities and protect from them.
**Requirement 3:**
Protect stored cardholder data.

Trend Micro SecureCloud provides AES-256 full disk encryption for private and public cloud machines and supports both EBS boot volume and data volume encryption. In addition, SecureCloud encryption is performed independent of the infrastructure (for example, a cloud service provider), ensuring that customers have full control over encryption keys and the encryption key release policies and can more easily achieve compliance and reporting.

SecureCloud encryption policies enable customers to control the conditions under which encryption keys are released to requesting SecureCloud Agents (i.e. location of the server instance, IP address, OS type, Deep Security status, custom AWS metadata, etc.) This enables organizations to not only protect data in current use, but also effectively destroy access to the data by deleting the encryption keys for a given set of data. SecureCloud implements a FIPS 140-2 Level 1 certified cryptographic library to perform the volume encryption.

**Requirement 4:**
Encrypt transmission of cardholder data across open, public networks.

Trend Micro Deep Security for Web Apps includes unlimited, globally trusted SSL certificates that can be used to protect cardholder data in transit. This is achieved by creating a uniquely encrypted channel for communication, using the SSL certificate as the foundation for the securing of the data. The offering includes an enterprise-class management console and certificate health checks to reduce configuration issues and expiry risk.

The transmission of data can additionally be protected with Deep Security’s host-based firewall, which can be configured to block HTTP traffic (port 80), ensuring that all traffic occurs over HTTPS ports (443).

**Requirement 5:**
Protect all systems against malware and regularly update anti-virus software or programs.

Trend Micro Deep Security provides anti-malware protection for physical, virtual and cloud environments. Deep Security anti-malware capabilities include:

- Highly customizable anti-malware configurations applicable to Security Profiles and virtual machines
- Real-time, manual and scheduled scans of protected servers
- Use of the Trend Micro Smart Protection Network™ global threat intelligence for the most up to date threat protection
- Quarantined file management, including download and delete from Deep Security Manager
- Agentless anti-malware protection using VMware vCloud Networking and Security Endpoint
- Protection of active virtual machines running on vSphere
- Protection of cloud instances in public cloud deployments, including AWS, with automated provisioning and protection
- Support for a broad range of enterprise operating systems, including Microsoft Windows and many variants of Linux including RedHat, Suse, Amazon, Ubuntu, and others.
Trend Micro Deep Security's anti-malware capabilities provide the ability to fully document security policy and procedure requirements for maintaining anti-virus software and definitions on systems commonly affected by malware.

Deep Security is capable of detecting, blocking or removing all known types of malicious software. It automatically updates policies and malware information from a known, trusted source and cannot be disabled or removed from protected systems.

Deep Security for Web Apps includes the ability to scan applications for malware and threats, providing an additional important layer of detection that can help protect applications. This real-time malware detection is enabled through an ability to crawl an entire web application and check all links and content for potential malware that would not be detectable on the server itself.

**Requirement 6:**
Develop and maintain secure systems and applications.

Trend Micro Deep Security intrusion prevention provides virtual patching to protect unpatched network and platform vulnerabilities, and can serve as an effective compensating control and risk management strategy for the patching requirements of Section 6.1 of PCI DSS 3.0 until the appropriate patches can be applied.

Deep Security intrusion prevention capabilities can also provide web application protection by intercepting web requests based on the OWASP top 10 vulnerabilities including Injection, Cross Site Scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery (CSRF), Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection and Unvalidated Redirects and Forwards. Deep Security blocks malicious requests from reaching the web server preventing these vulnerabilities from being exploited.

Deep Security has extensive integration with leading operational tools like Chef, Puppet, RightScale, and AWS OpsWorks, which can help organizations maintain and automate consistent configurations and security policies for their deployments that are involved with cardholder data.

Trend Micro Deep Security for Web Apps provides continuous, automated vulnerability scanning of applications and platforms to help you meet Section 6.6 requirements. It also protects your applications with custom generated rules for major WAF providers (Citrix, iMPERVA, ModSecurity, ALERTLOGIC) so discovered vulnerabilities can immediately be blocked from potential exploitation.

**Requirement 7:**
Implement strong access control measures.

Deep Security maintains a full audit trail of all system and administrative operations/events, which can be forwarded to a centralized SIEM or Syslog server for further correlation and archival.

SecureCloud can be used to encrypt all sensitive data and require appropriate authentication and role validation before allowing access.
Deep Security supports role-based access control ensuring that administrative privileges can be restricted on a per administrator basis.

This is further supplemented by Deep Security’s multi-tenant capability where different departments or business units can be created as separate tenants ensuring complete isolation from a security management perspective.

The Trend Micro Cloud and Data Center solution does not address this requirement. This requirement could be addressed by a CSP like Amazon Web Services as a part of their underlying commitment to security in the shared responsibility model.

Trend Micro Deep Security’s host-based firewall can log and audit access at the host (physical, virtual machine, or cloud instance), enabling tracking of access to any and all sensitive data.

Deep Security’s integrity monitoring capabilities provide active monitoring of critical files, folders, ports, applications and registry settings for unauthorized changes.

Deep Security’s log inspection capabilities provide log correlation and inspection for protected systems. System logs are analyzed for configured events. Alerts from these events are raised in the Deep Security Manager providing administrators with near real time events for analysis. Supported across over 100 log formats, this log inspection capability provides a robust approach to monitoring access to network resources and cardholder data.

Deep Security’s intrusion prevention provides the ability to monitor 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.

Deep Security’s integrity monitoring provides integrity monitoring of critical OS, application and configuration files and registry to meet Sections 11.4 and 11.5.

Trend Micro Deep Security for Web Apps provides continuous, automated scanning of both application and platform deployments. Vulnerabilities that affect PCI compliance are flagged in the results with specific explanations of the vulnerability along with remediation recommendations. Expert hands-on business logic testing is also available to catch vulnerabilities that would not be discovered with automated scanning. Deep Security for Web Apps is one of a select group of security partners that have been certified as a Pre-Authorized Scanner for deployments on AWS, streamlining the ability to continuously scan instances in the cloud for potential vulnerabilities at the platform and application layers, as well as checking for malware and potentially malicious links. Malicious link checking is powered by the Trend Micro Smart Protection Network and information gathered from over 150 million endpoints around the world.
**Requirement 12:**

Maintain a policy that addresses information security for all personnel.

Trend Micro 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. Deep Security’s integration with leading SIEM vendors enables a consolidated view of security incidents.

**CONCLUSION**

Merchants and service providers that are involved in processing credit card payments must comply with the Payment Card Industry Data Security Standard (PCI DSS), now at Version 3.0. The Trend Micro Cloud and Data Center Security Solution provide valuable capabilities to assist with achieving compliance and fit with the modern environment of leveraging service providers for achieving business agility and efficiency. For more information on Trend Micro’s Cloud and Data Center Security solutions, visit [www.trendmicro.com/cloud](http://www.trendmicro.com/cloud).

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).