WHITE PAPER

USING TREND MICRO'S HYBRID CLOUD SECURITY SOLUTION TO MEET PCI DSS 3.2 COMPLIANCE

IMPLEMENTING TREND MICRO'S DEEP SECURITY IN A PAYMENT CARD ENVIRONMENT

AUGUST 2017

COALFIRE℠

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper examines the applicability of Trend Micro's Hybrid Cloud Security Solution[1], specifically Trend Micro Deep Security, to secure Payment Card Industry (PCI) data in accordance with the PCI Data Security Standard (PCI DSS)[2] 3.2 when used in physical, virtual, cloud, or container environments. Deep Security delivers a broad range of security controls optimized for modern data centers, cloud environments, as well as container deployments. This offering complements the security provided by platform and service providers, including cloud service providers (CSP) such as Amazon Web Services (AWS) and Microsoft Azure, and can help an organization achieve compliance with specific PCI DSS 3.2 requirements.

As datacenters virtualize across private, public, and hybrid cloud, datacenter security is increasingly challenging as threat environments gain sophistication. Not only is customer data protection critical to compliance with regulations like PCI DSS v3.2, but datacenter security must reduce risk and maintain cost effectiveness while enabling a superior user experience.

Sean Pike
IDC Program VP
Security Products

Coalfire's evaluation and analysis of Deep Security shows that it is capable of helping to support eight of the twelve PCI DSS v3.2 compliance requirements as documented in this paper, when implemented within the context of PCI compliant security architecture and appropriately configured. In addition, there are no known inhibitors within the solution that would prevent an organization from running in-scope PCI applications in a compliant manner and there are functions that facilitate controls necessary to meet certain PCI requirements. While it is not included in the scope of this product review, Trend Micro also operates Deep Security as a managed security service, and has assessed this offering as a Level 1 Service Provider to further streamline client PCI compliance.

Although this paper specifically addresses PCI compliance, the same basic security principles can be applied when implementing systems that comply with other similar regulations, such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the EU Global Data Protection Regulations (GDPR), and regulations put forth by the North American Electric Reliability Corporation (NERC) or the Federal Energy Regulatory Commission (FERC).

Coalfire conducted the product applicability assessment through interviews with the Trend Micro Hybrid Cloud Security product experts, observing product demonstrations, and analyzing documentation and website content provided by Trend Micro. An independent test of the product features was not conducted as part of this white paper. Due to the unique business, technical, security, and governance requirements that every organization has, this paper does not provide detailed recommendations for how to configure Trend Micro Deep Security to meet the applicable portions of the PCI DSS. Consult your organization's Qualified Security Assessor (QSA) or Internal Security Assessor (ISA) to address your organization's unique environment compliance questions.

---

[1] While this paper specifically addresses Trend Micro's Deep Security product, Trend Micro's Hybrid Cloud Security Solution consists of a variety of tools to support organizations compliance efforts whether deployed in an on premise data center or in the Cloud. For additional information, refer to Trend Micro's website at www.trendmicro.com/hybridcloud.

[2] The PCI DSS is available from the PCI Security Standards Council at http://pcisecuritystandards.org. At the time of this writing, the current standard is version 3.2.

PCI DSS V3.2 OVERVIEW

This paper assumes the reader is familiar with the PCI DSS (including relevant guidance publications); card brand requirements; supplemental documents from the PCI Security Standards Council, such as the cloud and virtualization guideline documents[3]; and any specific guidance published by their acquiring bank or processor.

The PCI DSS applies to all organizations globally that store, process, or transmit cardholder account data, regardless of volume.

Merchants and Service Providers are required to validate their compliance by assessing their environment against over 400 specific test controls outlined in the PCI DSS. Failure to meet PCI DSS requirements may lead to fines, penalties, or the inability to process payment cards (credit, debit, prepaid, etc.), in addition to potential reputational loss. In April 2016, the PCI Security Standards Council introduced PCI DSS v3.2 to extend the SSL/early TLS migration requirement deadline, to provide clarifications, and to address evolving requirements. As of **October 31, 2016, PCI DSS v3.1 has expired** and all organizations must be compliant with PCI DSS v3.2; however, all new requirements are best practices until February 1, 2018 to allow organizations an opportunity to prepare to implement these changes.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
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 all personnel

Table 1: PCI Data Security Standard - six categories with twelve total requirements

Previous Versions of PCI DSS

Over the past 12 years, the PCI DSS has undergone multiple changes. The Version 3.0 major version release has been effective since November 2013. Version 3.1 was published effective April 2015, and addresses evolving requirements resulting from vulnerabilities identified in the SSL protocol. Effective June 30, 2018, SSL and early TLS versions are prohibited from use in a PCI-compliant environment.

PCI DSS 3.2 Change - Highlights

Version 3.2 of the Payment Card Industry Data Security Standard was published effective April 2016. Changes introduced included clarification and additional guidance on existing PCI DSS requirements, as well as addressing evolving requirements. Key changes included:

[3] The Information Supplements and Standards documents referenced in this document are available from the PCI Security Council website document library, located at http://pcisecuritystandards.org.

- An update to extend the migration deadline of SSL and early TLS versions. As noted in the PCI DSS 3.2 Appendix A2, to support entities working to migrate away from SSL/early TLS, the following provisions were included:
  - New implementations must not use SSL or early TLS as a security control.
  - All service providers were required to provide a secure service offering by June 30, **2016**.
  - After June 30, **2018**, all entities must have stopped use of SSL/early TLS as a security control and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet).
  - Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
  - POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after June 30, 2018.
- The addition of the PCI DSS Supplemental Designated Entities Validation (DESV) criteria as an appendix to the standard, as well as expanded existing PCI DSS requirements (3, 10, 11, 12) to include DESV controls for service providers specifically.
- There are 9 new sub-requirements introduced in PCI DSS 3.2, affecting requirements 3, 6, 8, 10, 11 and 12. The new requirements are considered best practices through Januay 31, 2018 to allow organizations an opportunity to prepare to implement these changes. Starting February 1, 2018 they are effective as requirements and must be assessed for compliance.

Organizations that focus solely on annual PCI DSS assessments to validate the quality of their cardholder data security programs are missing the intent of PCI DSS, and likely see their PCI DSS compliance state "fall off" between assessments (see Figure 1). These organizations must realize that security is not a project, it is a continuous state. In order to maintain a consistent level of security, organizations must have a well-designed program of security controls and monitoring practices in place to ensure they are meeting the intent of PCI DSS at all times, not just at one point in time during a calendar year.

PCI SSC Information Supplement: Best Practices for Maintaining PCI DSS Compliance (August 2014)

Continual Compliance

Organizations that focus solely on annual PCI DSS assessments to validate the quality of their account data security programs are missing the intent of PCI DSS and are likely see their PCI DSS compliance state "fall off" between assessments (see Figure 1).

As shown in this graphic from PCI SSC *Information Supplement: Best Practices for Maintaining PCI DSS Compliance (August 2014),* a typical organization's compliance co-relates to the compliance assessment cycle. Preparing for the annual arrival of the PCI QSA (Qualified Security Assessor) causes the organization to look at the state of compliance and fix vulnerabilities identified, and the arrival of the QSA ramps up the effort to resolve issues. Once the QSA delivers the Report on Compliance, the organization may begin to let controls relax. This is not necessarily deliberate but the priority for compliance and security may be lowered for the next major project or problem. Establishing routine day-to-day processes and monitoring activities that address compliance are essential to introducing business-as-usual compliance and making your organization's compliance curve flatter and higher as shown in Figure 1 below.

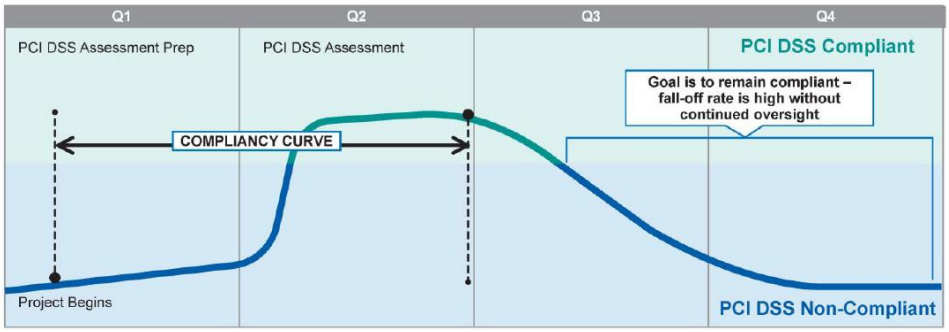

Figure 1: Compliancy Curve

Implementing technologies and procedures for identifying new vulnerabilities and for monitoring to ensure that implemented policies and procedures are working appropriately and haven't been accidently dropped or forgotten is necessary to maintaining ***everyday compliance***.

PCI, VIRTUALIZATION, AND THE CLOUD

Virtualization and cloud technologies offer many advantages. Deploying new systems has become much easier (why else do administrators refer to "throwing up a new server quickly?"). Cost efficiencies may be introduced by using a single physical server to host multiple virtual servers. Containers support incremental development, version control, and process isolation. Serverless architecture can greatly reduce infrastructure cost, while providing application scalability. But with these new capabilities, new layers of technology are introduced that need to be implemented, administered, maintained, and monitored in compliance with PCI DSS. The *Information Supplement: PCI DSS Virtualization Guidelines* (June 2011) identifies four "principles associated with the use of virtualization in cardholder data environments:

a. If virtualization technologies are used in a cardholder data environment, PCI DSS requirements apply to those virtualization technologies.

b. Virtualization technology introduces new risks that may not be relevant to other technologies and that must be assessed when adopting virtualization in cardholder data environments.

c. Implementations of virtual technologies can vary greatly, and entities will need to perform a thorough discovery to identify and document the unique characteristics of their particular virtualized implementation, including all interactions with payment transaction processes and payment card data.

d. There is no one-size-fits-all method or solution to configure virtualized environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented."

> *Use of a PCI DSS compliant CSP does not result in PCI DSS compliance for the client.* ***The client*** *must still ensure they are using the service in a compliant manner, and is also* ***ultimately responsible for the security of their CHD*** *– outsourcing daily management of a subset of PCI DSS requirements does not remove the clients' responsibility to ensure CHD is properly secured and that PCI DSS controls are met.*
>
> *PCI DSS Virtualization Guidelines and PCI DSS Cloud Computing Guidelines*

The introduction of virtualization and cloud computing into cardholder data environments (CDE) can blur the lines of segmentation. This is especially true when hosting systems that handle account data and those that do not are housed on the same virtualized platform, or where applications or systems in a cloud environment have unknown or unclear segmentation controls. However, with attention to the additional risk factors and segmentation testing, virtualized environments and cloud technology solutions can be

implemented with full compliance, as acknowledged in version 3.2 of the PCI DSS, the *Information Supplement: PCI DSS Cloud Computing Guidelines* (February 2013), and the *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* (May 2017).

When implementing the CDE using virtualization or cloud technologies, there are additional risk factors that must be considered and addressed. As noted in the Cloud Computing Guidelines, this is especially true when outsourcing the CDE to a cloud service provider (CSP) for hosting. One of the most important considerations when outsourcing to a CSP, or other service providers, is to define and understand roles and responsibilities. The figure below is provided in the Cloud Special Interest Group, PCI Security Standards Council (2013) *Information Supplement: PCI DSS Cloud Computing Guidelines*.

	Client
	CSP
	BOTH Client and CSP

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

***Note:** The sample responsibilities illustrated in this table do not include consideration for any activities or operations performed outside of a hypothetical cloud service offering. This table provides an example of how PCI DSS responsibilities might be assigned for different service models. However, each CSP ultimately defines their own service, and particular service offerings may or may not be consistent with those illustrated above. Clients and CSPs should clearly document their responsibilities as applicable to their particular agreement.*

IaaS – Infrastructure as a Service, PaaS – Platform as a Service, SaaS – Software as a Service

Figure 2: Shared Responsibility Matrix Example

Another area of significant concern is that of cloud technology nested vendor relationships. For example, one SaaS vendor may utilize a separate PaaS vendor, who may in turn utilize yet another IaaS vendor. This also applies to the vendors that provide security tools used to maintain compliance. The more vendors

in use, the more complexity is introduced into the entity's vendor management program, including those controls required under PCI DSS requirement 12.8.

We recommend the tools available in the PCI Cloud Guidelines and Third-Party Security Assurance information supplements be used to improve segmentation control testing, clarify shared responsibilities, and aid in management of vendor relationships. Questions about specific PCI impacts should be addressed to the client's QSA.

SECURITY FOR THE PCI COMPLIANT ENVIRONMENT

To provide the security necessary for PCI compliance, a variety of security tools must be deployed and security processes and procedures implemented. As noted in the diagram below, Trend Micro's Deep Security product can help with a wide range of requirements for security under PCI DSS v3.2.

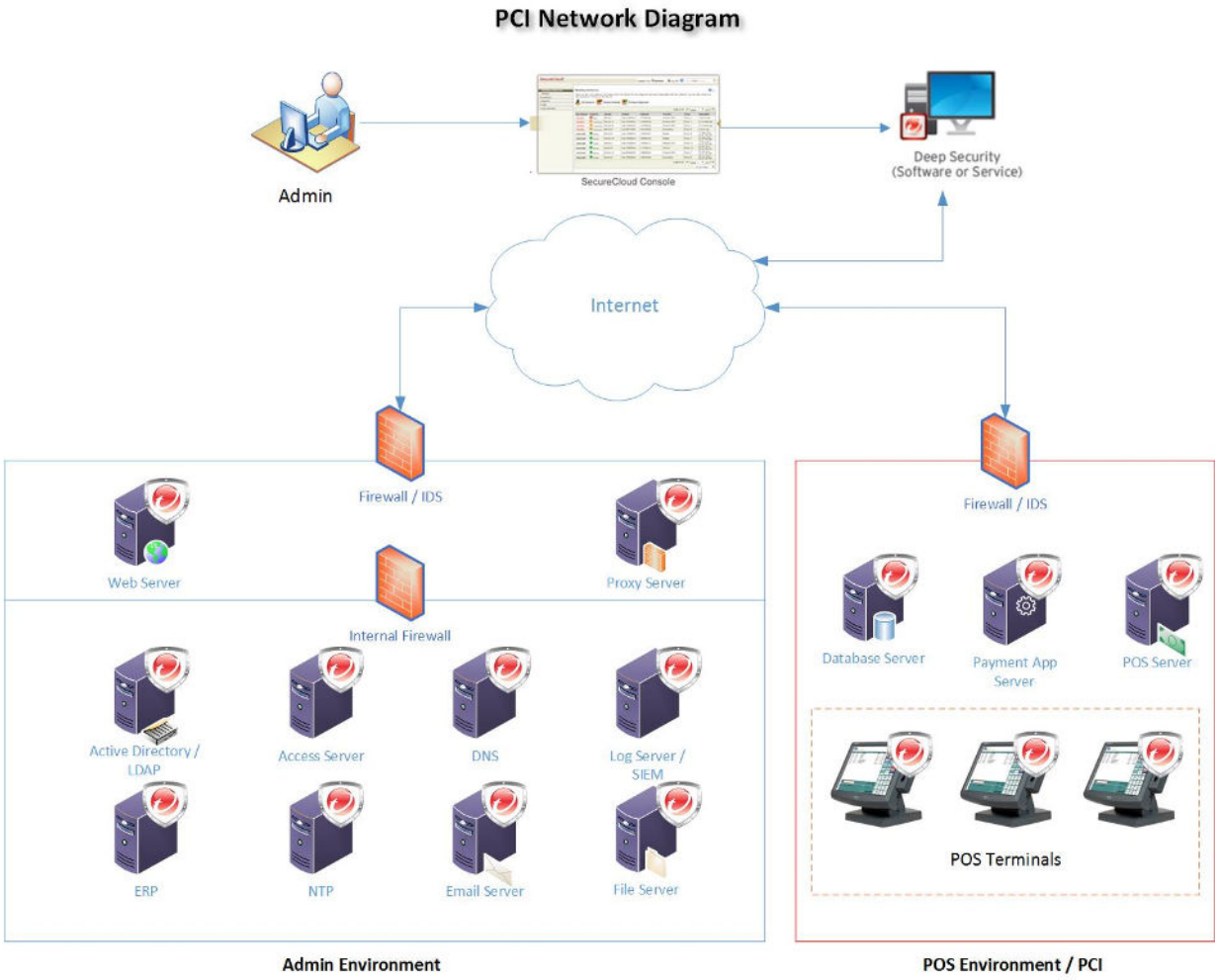

Figure 3: Security for a PCI Compliant Environment

Different deployment models might be used for payment processing - a traditional data center with physical servers managed internally; a modern data center with a combination of physical and virtual systems, as well as some cloud processing (often called a hybrid architecture); or cloud-centric design where much of the control over systems and security is delegated to a Cloud Service Provider – ensuring that appropriate

security and controls are in place is the organization's responsibility. All PCI DSS controls must be in place to achieve compliance no matter what technology is deployed or what data center deployment model is used. Below is an overview table of security tools required for PCI DSS compliance.

TREND MICRO ROLE	REQUIRED SECURITY TOOL	DESCRIPTION	PCI DSS RQMT.
	Perimeter Firewalls	Protect and control network connections from outside attack.	1
	Internal Firewall	Protect and control internal network connections and network traffic. *Deep Security's host-based firewalls can add extra protection to a server and supplement segmentation in the cardholder data environment.*	1
	Personal Firewall	Firewall protection for laptops and other systems used to access an organization's network remotely. *Deep Security agent placed on the remote system can allow for host-based firewall protection managed by the organization.*	1
	Configuration Management	Systems configuration management for servers and desktops. *Deep Security scans and policies can be used to supplement administrator's efforts to ensure servers are appropriately configured.*	2
	At Rest Encryption	Strong encryption for account data at rest.	3
	Key Management	Key management tools for securing encryption keys.	3
	Transmission Encryption	Strong encryption for transmission of account data over open or public networks.	4
	Anti-Virus Software Servers and Workstations	Malware prevention for all operating systems' vulnerability to viruses and other malicious exploits. *Deep Security provides anti-virus/anti-malware for common exploits, including ransomware.*	5
	Vulnerability and Patch Management	Tools and processes used to monitor for newly identified vulnerabilities and managing patching to address changes to firewalls, systems, and critical security components. *Deep Security can be used as an industry resource for identified new vulnerabilities or as a control to protect outdated OS and application versions and can assist an administrator to identify outstanding patches, as well as implementing protection until patches can be applied ("virtual patching").*	6
	Software Change Control System	Change management for applications, software, and network components, including scheduling, documenting, logging, and approving of an organization's technology changes. *Deep Security's integrity monitoring can help to flag changes in configuration and software, which can be supported using Deep*	6

		Security application control functionality, including approval and rollback of application control decisions.	
	Web Application Firewall (WAF) *Optional for PCI DSS, alternative controls possible.*	HTTP web application traffic filter that monitors for and blocks many common web application attacks. *Deep Security can supplement compliance activities and help address many of the most common web application attacks; however, it does not independently fully address this requirement.*	6
	Authentication and Access Control	Network and systems logon credentials authentication and access control systems – usually Active Directory or LDAP. *Deep Security user and role functionality supports compliant enforcement of access policies pertaining to the security functionality provided by the Deep Security platform.*	7 & 8
	Remote Access	Provides remote access into an organization's internal network.	8 & 12
	Two-Factor Authentication	Required for remote access into cardholder data environment.	8
	Physical Security Controls	Physical controls used to secure the data center, including such technology as access badges, trap doors, camera, security guards, etc.	9
	Tape Backup or Backup Management	Data/systems backup technology to removable tapes/disks.	9
	Time and Date Synchronization	Time management services.	10
	Log Management, Monitoring and Central Log	Central log server and SIEM (Systems Information & Event Management) system to provide for secure log storage and monitoring of networks and systems. *Deep Security provides log storage and reporting through its administrator's console. Additionally, Deep Security will share logs with organization's SIEM/central log server.*	10
	Intrusion Detection & Intrusion Prevention Systems (IDS/IPS)	Network and system intrusion prevention through identification, monitoring, and alerts. *Deep Security provides host-based IDS/IPS based upon policies created by the administrator.*	11
	File Integrity Monitoring (FIM)	Monitor critical server configurations and log files from unauthorized modification/changes. *Deep Security provides file integrity monitoring based upon policies created by the administrator.*	11
	External Scanning (ASV)	Quarterly external scanning requirements that must be performed by ASV.	11
	Internal Scanning Tool	Quarterly internal scanning and reporting. *Deep Security can supplement full network internal scanning by scanning and reporting identified vulnerabilities on servers with the Deep Security Agent running.*	11
	Penetration Testing	Tools and resources for annual penetration tests.	11

		Deep Security can be one of the many tools used to perform required penetrations tests.	
	Wireless IDPS *Optional for PCI DSS, alternative controls possible.*	Wireless intrusion detection and prevention systems monitor wireless networks for unauthorized wireless access points.	11

Table 2: Common Security Components used to Address PCI DSS 3.2 Requirements

OVERVIEW OF TREND MICRO DEEP SECURITY

The problem: Merchants and service providers supporting payment card processing face the complexity of complying with the PCI DSS v3.2 in what can be a complex operating environment. Information Technology (IT) departments are finding that the business needs, strict deadlines, and budget constraints are driving them to "data centers" that are far more complex to manage than the traditional data centers of the past. The modern data center can include:

- Physical and virtual systems, including containers
- Multiple operating systems, current and legacy
- Technology located at company-owned data centers, at shared hosting providers, or in the cloud
- Shared responsibility for administration and management of technology, where some, or all, systems and network administration activities have been delegated to an outside service provider – and possibly multiple service providers

All of these variables must be coordinated while managing day-to-day operating responsibilities, as well as ensuring that security appropriate to the business and technology risk is in place and relevant compliance standards are addressed.

The Payment Card Industry Data Security Standard (PCI DSS) was developed with the intent of reducing the risk of handling account data and is one of the most rigorous standards established to date. Virtualization and cloud computing can create additional challenges in achieving compliance with PCI DSS, but does not inherently prevent compliance.

Trend Micro's Solution: Trend Micro's Hybrid Cloud Security Solution, powered by Trend Micro Deep Security, concentrates on ongoing monitoring of an organization's environment to identify and address vulnerabilities and potential security issues. Refer to Figure #4 below for a typical architecture of how Trend Micro addresses the challenges of a modern data center.

Trend Micro's solution addresses merchant's challenges of ensuring that security and compliance controls are in place and working by monitoring for vulnerabilities and protecting in-scope applications and data. Deep Security is licensed by Trend Micro as software running on premise, as a software appliance through leading marketplaces like Amazon Web Services (AWS) and Microsoft Azure, or as a hosted service provided directly by Trend Micro.

The Deep Security cloud service has been validated as a PCI DSS 3.2 compliant level 1 service provider and is hosted in a PCI DSS certified secure data center that includes physical controls such as man-traps, electronic monitoring, 24/7 on-site security, restricted accesses to servers, and biometric security for access to cages. Questions regarding applicability of these controls for an organization's security, business, and account data processing needs should be addressed to the organization's QSA.

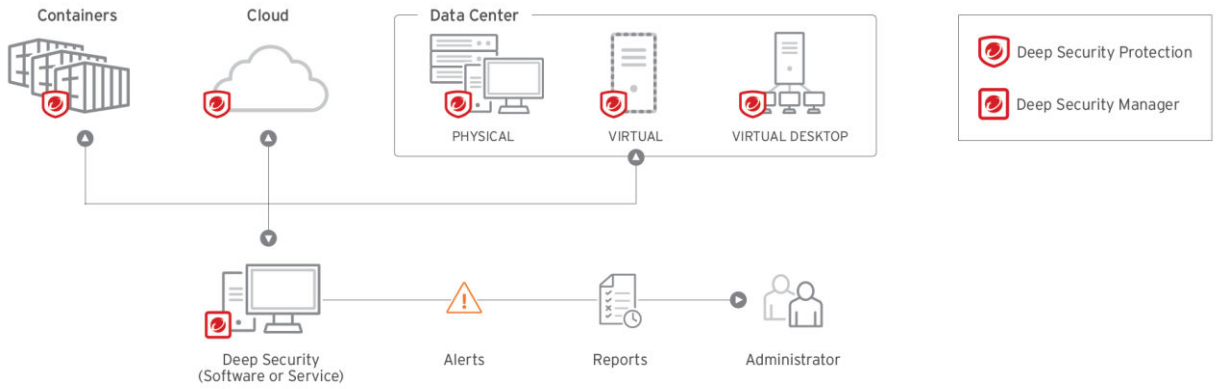

Figure 4: Trend Micro Addresses Challenges of the Modern Data Center

TREND MICRO DEEP SECURITY

Deep Security secures workloads (in physical, virtual, cloud, or container environments) and helps to protect sensitive card data through a wide range of host-based security controls. A central management console gives a state-of-the-environment picture with the ability to easily drill down for details and allows administrators to implement policies for firewall rules, vulnerability shielding, system integrity, application control, and alert generation, as well as assign administration roles for Deep Security activities. When deployed in a virtualized, cloud, or hybrid environment, new virtual machines (running on traditional hypervisors or a container engine), will automatically be detected, providing a dynamic view of the environment and ensuring the security administrator is aware of changes introduced to the IT environment.

Deep Security delivers the following host-based security controls:

- **Malware Prevention:** including anti-malware, behavioral monitoring, and Web reputation services. This control is integrated with the Trend Micro Smart Protection Network for global threat intelligence, protecting servers from sophisticated attacks, including ransomware, in server environments by isolating malware from critical operating system and security components.
- **Intrusion Detection & Prevention (IDS/IPS)**: for each server across physical, virtual, or cloud environments (including those hosting containers), examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack. This enables automated protection against known but unpatched vulnerabilities (ex: Microsoft SMB vulnerability CVE# that enabled WannaCry and EternalRocks) by virtually patching (shielding) them from an unlimited number of exploits. It can also protect against threats like ransomware, detecting both lateral movement in a data center and attacks from compromised end users against enterprise file servers.
- **Bidirectional Host-based Firewall:** decreases the attack surface of physical, cloud, and virtual servers with fine-grained filtering, policies per network, and location awareness for all IP-based protocols and frame types. It provides logging of firewall events at the host, enabling compliance and audit reporting per server/VM/cloud workload (especially useful for public cloud deployments).
- **Application Control:** locks down servers so only allowed (whitelisted) applications can run. This can help to stop unauthorized applications from execution, which can prevent certain attacks like ransomware from taking over a system.
- **Integrity Monitoring:** monitors critical operating system and application files (directories, registry keys, and values) to detect and report unexpected changes in real time. Integrity monitoring

simplifies administration by greatly reducing the number of potential system events to deal with through automated cloud-based whitelisting from Trend Micro Certified Safe Software Service.

- **Log Inspection:** collects, analyzes, and reports on operating system and application logs in over 100 log file formats, identifying suspicious behavior, security events, and administrative events across your data center. Logs can also be sent to leading SIEMs like IBM QRadar, HP ArcSight, and Splunk.

For additional information, refer to the Trend Micro Website.

DEPLOYMENT MODELS

Trend Micro provides flexible deployment alternatives based upon the organization's technical environment.

For organizations that are using VMware virtualization technology, Deep Security can be installed both at the hypervisor as well as at the server level using agents, depending on the organization's architecture and configuration. For non-VMware deployments, Deep Security agents are deployed on all servers that an organization wants to monitor and protect with Deep Security, including physical, virtual, cloud, and container workloads. For both approaches, the Deep Security Manager can be installed on a Windows or Linux server. Running a Deep Security recommendation scan will then create vulnerability analysis and recommendations that are available to the administrator from the management console. The Deep Security administrator configures the Deep Security Firewall, IDS/IPS, Application Control, Integrity Monitoring, Malware Prevention, and Log Inspection modules based upon business needs.

MODERN DATA CENTER

Most organizations have embraced virtualization technology, whether VMware, Microsoft, or others. The modern data center needs tools that support hybrid architectures that include physical, virtual, and cloud workloads running a variety of operating systems. As represented in Figure 5, Trend Micro's Deep Security can support the modern data center's need to secure critical applications, data, and servers and can address many of the requirements of PCI DSS 3.2.

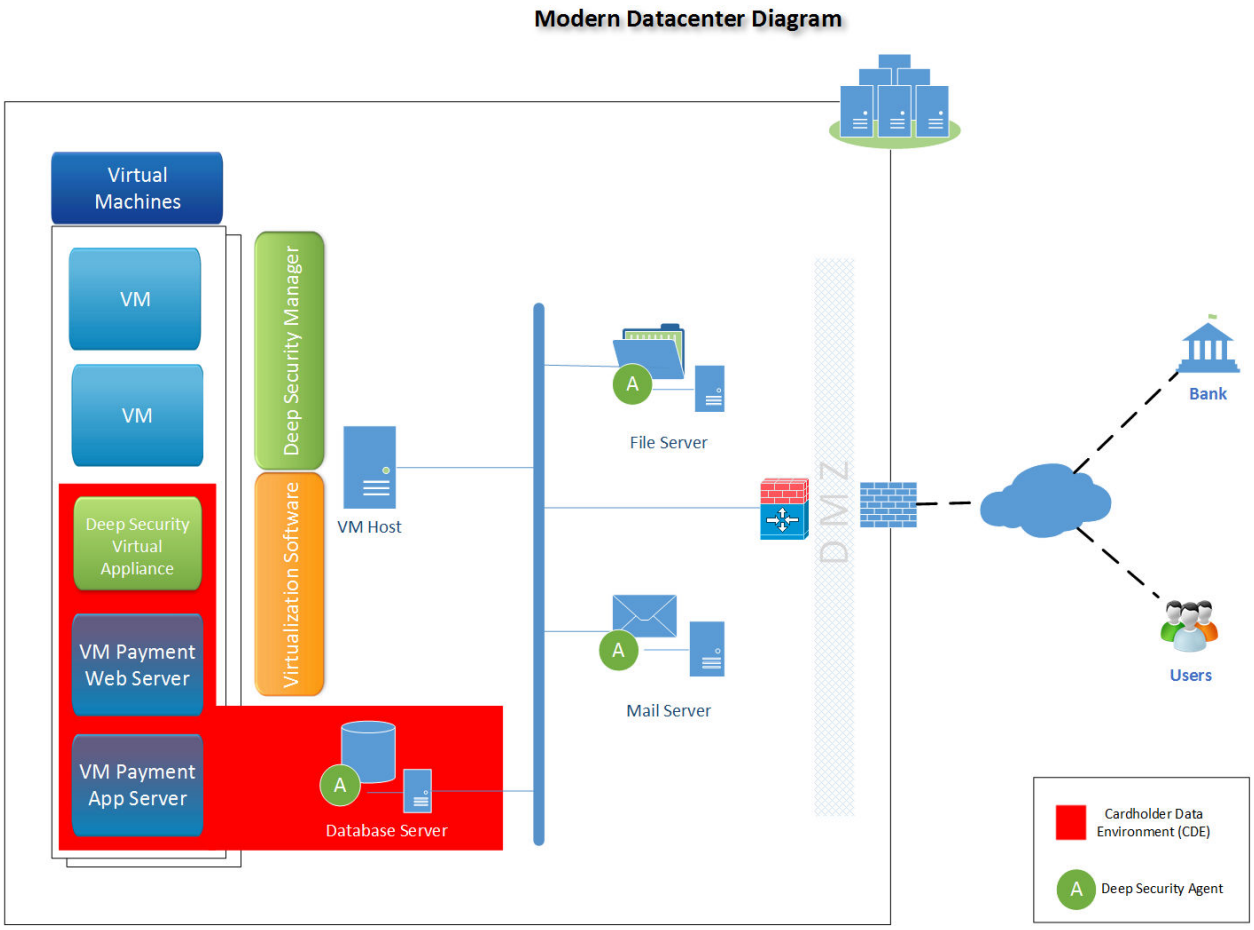

Figure 5: Modern Data Center – Trend Micro Deployment Model

PCI Considerations when deploying in a modern data center:

When running in a virtualized environment, there are Deep Security components implemented on the hypervisor and on virtual machines, with virtual machines monitored by Deep Security typically being protected from the hypervisor level (or host OS level for cloud and container workloads). Organizations can also deploy Deep Security in a combined mode of operation, which has some controls like IPS and Integrity Monitoring deployed as an agent on the VM and Anti-malware (a high intensity control) deployed at the hypervisor layer for efficiency. Deep Security automatically identifies virtual machines and applies policies. Physical servers monitored by Deep Security will need the Deep Security Agent. Systems administrators can use the Deep Security console to run vulnerability scans, implement scanning and host-based firewall policies, monitor the state of the systems. The Deep Security console provides a graphics-based user interface, supporting drill down capability to detailed data and system log records.

Other PCI considerations:

- Shared responsibility: Shared roles and responsibilities are important to understand when service providers are involved in the delivery of payment processing. When using a hosted data center, the data center might only be responsible for physical control (Requirement 9). If the hosted service provider provides basic network capabilities, their involvement could include perimeter firewalls, network segmentation up to the organizations entry-point and ensuring that wireless network monitoring (Requirement 11.1) is conducted. If the hosted service provider is responsible for

administering the operating system, the hosted service provider's scope of responsibility will include systems configuration management (Requirement 2), anti-malware administration (Requirement 5), access control and authentication (Requirement 7 and 8), IDS and file integrity monitoring (Requirement 11), and providing centralized log server and log monitoring (Requirement 10), but often the business organization is responsible for some portion of these activities. While delegation of specific controls can be assigned to a service provider, it is the organization's responsibility to ensure that all service providers are managing and administering the CDE in a PCI compliant way. Deep Security vulnerability checking can provide valuable information about the state of compliance.

- Physical controls, as outlined in Requirement 9, must be in place to protect all processing, transmission, and storage of account data. Note that in a hosted data center, these physical controls will be provided by the data center service provider. If possible, the hosted data center should be a PCI-compliant service provider; if not, certain physical controls may be brought into scope during the organization's annual PCI assessment.
- Network segmentation to reduce cardholder data environment assessment scope
  - Deep Security provides a host-based, stateful inspection firewall capability, but perimeter network firewalls are still needed. The host-based firewall capability is provided by agents running on the physical or virtual servers communicating with Deep Security policies or by the hypervisor interface for virtual machines. This host-based firewall functionality could provide internal network segmentation for an organization's cardholder data environment.
  - When deploying Trend Micro to support the CDE, it isn't necessary to install Deep Security within the CDE network segment, since account data is not transmitted, stored, or processed by Deep Security. However, all Trend Micro components should be installed in a network on servers, whether physical or virtual, that meet configuration requirements identified in DSS Requirements 1 and 2 since critical security functions for the CDE will be supported by these components.
- Network controls as required by PCI DSS Requirement 1: Deep Security provides host-based firewall capabilities, as well as host-based IDS/IPS . When running at a hosted service provider that protects the perimeter with a network firewall, Deep Security's host-based firewall and IDS/IPS capabilities for internal traffic monitoring could fulfill Requirement 1 and 11.4 controls. Complex internal networks could have the need for additional network firewalls/IDS.
- Application vulnerability protection required by PCI DSS Requirements 6.5 and 6.6: An organization can supplement their secure coding practices by utilizing Deep Security's IDS/IPS control that includes vulnerability protection capabilities to detect many of the common coding vulnerabilities in software-development processes noted in Requirement 6.5. While Deep Security's application vulnerability protection capabilities do not provide the full set features required by the PCI DSS Requirement 6.6 for a web application firewall, they can protect systems against many of the Requirement 6.5 OWASP Top 10 vulnerabilities as well as other application-based vulnerabilities. If an organization does not have a traditional Web Application Firewall in place and instead performs periodic application vulnerability reviews as required by Requirement 6.6, the organization can supplement the periodic application vulnerability reviews using Deep Security IDS/IPS and application vulnerability protection to provide continuous protection for many common vulnerabilities in between scans. Deep Security can detect and protect against many web application vulnerabilities from the current OWASP Top 10 (6 of 10) at the time of this document's publication, as well as others (refer to the Deep Security Documentation for additional details).

- Intrusion Detection and Prevention and Patching as required by DSS Requirements 11 and 6: Deep Security identifies exploits using its host-based IDS/IPS functionality enhanced with virtual patching. Deep Security's virtual patching blocks vulnerability exploits automatically before vendor patches can be deployed. When using containers, the Deep Security IDS/IPS installed on the host OS can support proactive detection and mitigation of certain vulnerabilities between commits. Deep Security virtual patching can be an effective tool in an organization's DSS-required vulnerability management and patching strategy.
- Authentication and Access Controls as required by DSS Requirements 7 and 8: While Deep Security has application accounts/passwords, it is recommended that the organization's active directory or LDAP is used for authentication, including password controls (Requirement 8). Access controls for Deep Security administration, policy configuration, and log monitoring and reporting are addressed by access roles defined within Deep Security.
- Logging and log monitoring as required by DSS Requirement 10: Deep Security provides a consolidated log monitoring tool for systems under its control. Network devices and network firewalls are not included in Deep Security's scope of influence, so additional logging and log monitoring functionality will be needed for these network components. Deep Security's log sharing capability should be used to offload system logs to an organizations central log server where the organization's SIEM system can be used to monitor the complete CDE infrastructure.
- PCI DSS v3.2 Documentation Requirements: PCI DSS v3.2 identifies extensive documentation requirements. When deploying Trend Micro functionality in the CDE, the documentation must include the use of Deep Security in its scope, including: host-based firewall configuration standards, system configuration settings included in Deep Security policies, access request procedures that include approved access to use Deep Security, and change control procedures for Deep Security policy changes that impact operations of the CDE or other in-scope systems.

CLOUD DEPLOYMENT

For the organization running in the Cloud, Trend Micro provides security administrators or compliance officers the ability to automate the security of applications, data, and servers to address PCI requirements.

The solution has been optimized for leading cloud providers, including AWS and Microsoft Azure, and supports key platforms such as AWS Linux, Windows, Suse, Red Hat, CentOS, and Ubuntu. The solution is also compatible with cloud management tools such as Chef, PuppetLabs, SaltStack, AWS OpsWorks, and Ansible, as well as leading analytical tools like Sumo Logic.

As seen in Figure 6, when using Trend Micro's security controls, organizations can protect their cloud workloads and data and leverage built-in reporting to help with compliance requirements.

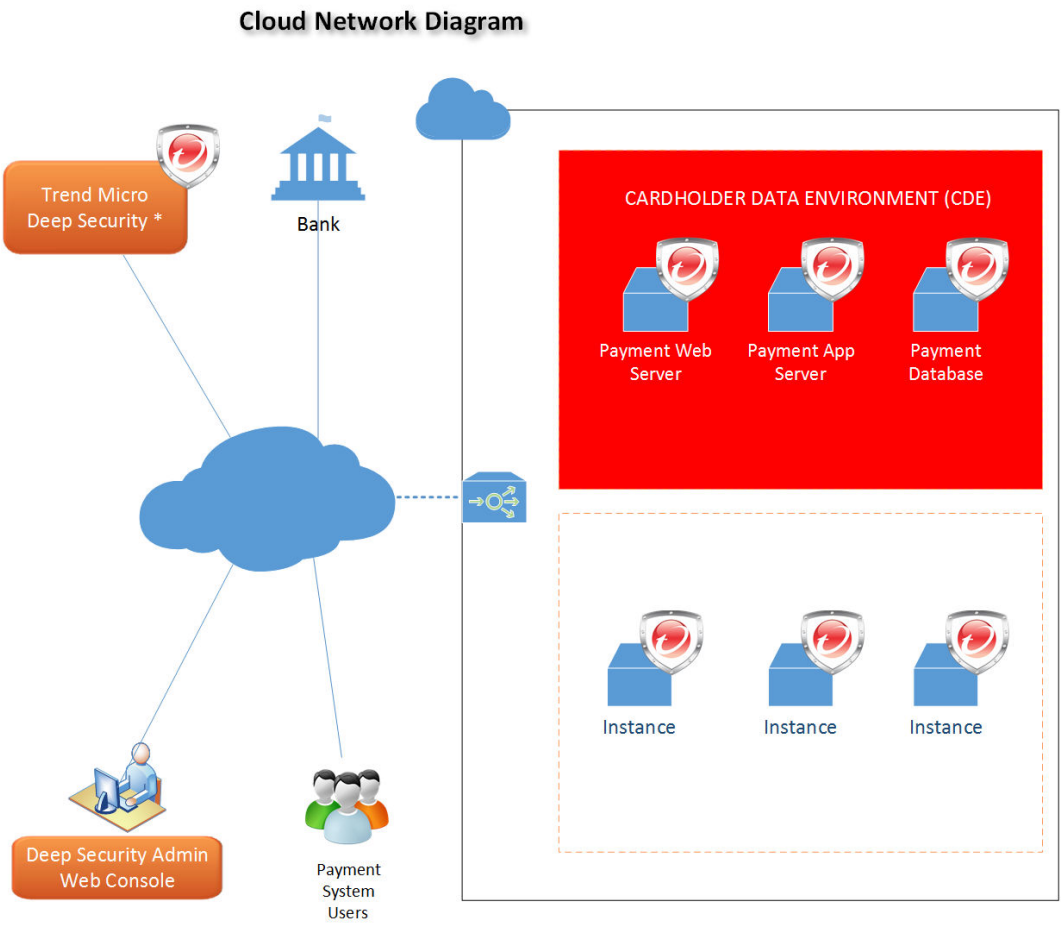

Figure 6: Cloud Processing – Trend Micro Deployment Model

PCI Considerations when deploying in the Cloud:

While Trend Micro has partnered with several cloud service providers (CSP) to enable Deep Security to work seamlessly in conjunction with the CSP's features, an organization's CDE running in another CSP can be supported with Deep Security using either Trend Micro's Deep Security service option or by installing Deep Security on a virtual machine in the cloud or on an in-house server, if the organization has a hybrid data center. A Deep Security Agent is installed (typically through automated scripting supported by the platform) on each cloud-based system that needs Deep Security's protection.

Systems administrators can use Deep Security's central management console to monitor for PCI compliance while deployed in a CSP by running vulnerability scans, implementing scanning and host-based firewall policies, and monitoring the state of the systems. The Deep Security console provides a graphics-based user interface, supporting drill down capability to detailed data and system log records.

Other considerations:

- Shared responsibility: When using a CSP, many activities usually performed by the business organization's IT department become the CSP's responsibility. It's important for an organization to clearly understand the boundaries between CSP responsibilities and the organization's responsibilities to ensure that all PCI DSS control requirements are addressed and that monitoring

activities are performed to ensure that CSP is meeting its obligations (Requirements 12.8). This is especially relevant for services such as serverless functions and SaaS applications which may operate on third-party or fourth-party platforms and/or infrastructure. Remember, while some activities might be delegated to the CSP, **the business is always responsible for its own PCI DSS compliance**. Consult the *Information Supplement: Third-Party Security Assurance* (March 2016) for details on monitoring CSP compliance and the use of a PCI DSS responsibility matrix to confirm individual and shared responsibilties.

- Physical controls, as outlined in Requirement 9, must be in place to protect all processing, transmission, and storage of account data. If possible, the CSP data center should be a PCI compliant service provider; if not, the physical controls could become in-scope during the organization's annual PCI assessment.
- Network segmentation to reduce cardholder data environment assessment scope:
  - Deep Security's host-based firewall capabilities can supplement network-based firewall to provide segmentation-reducing scope of the CDE environment and, within the CDE, can be used to provide further network controls to reduce risk to the CDE's most critical components, such as the payment data database.
  - In order to be effective as a segmentation control, any control must provide adequate isolation, and be tested according to PCI DSS requirement 11.3.4. For additional information, refer to the PCI SSC's *Information Supplement: Guidance for Scoping and Network Segmentation* (May 2017).
  - Where application functions operate outside an entity's clearly identified virtual networking environment (e.g., serverless), CSP segmentation controls and compliance status pertaining to these compute functions must be clearly identified and understood.
  - All Trend Micro components should be installed within a network on servers, whether physical or virtual, that meet configuration requirements identified in PCI DSS Requirements 1 and 2. While it's not necessary to put the components into the CDE, the configurations and rules should meet the PCI DSS networking/firewall and configuration standard requirements.
- Network controls required by PCI DSS Requirement 1: Deep Security provides a host-based, stateful inspection firewall capability, but perimeter network firewalls are still needed; these are typically provided and controlled at some level by the CSP. Deep Security provides host-based IDS/IPS, as well as host-based firewall capabilities, which are important controls for the cloud. When running at a CSP that protects the perimeter with a network firewall, Deep Security's host-based firewall and IDS/IPS capabilities for monitoring traffic in the organization's virtual network could fulfill Requirement 1 and 11.4 controls.
- Application vulnerability protection required by PCI DSS Requirements 6.5 and 6.6: An organization can supplement their secure coding practices by utilizing Deep Security's IDS/IPS control that includes vulnerability protection capabilities to detect many of the common coding vulnerabilities in software-development processes noted in Requirement 6.5. While Deep Security's application vulnerability protection capabilities do not provide the full set features required by the PCI DSS Requirement 6.6 for a web application firewall, they can protect systems against many of the Requirement 6.5 OWASP Top 10 (6 of 10) vulnerabilities as well as other application-based vulnerabilities. If an organization does not have a traditional Web Application Firewall in place and instead performs periodic application vulnerability reviews as required by Requirement 6.6, the organization can supplement the periodic application vulnerability reviews using Deep Security IDS/IPS and application vulnerability protection to provide continuous protection for many common vulnerabilities in between scans. Deep Security can detect and protect against many web

application vulnerabilities from the current OWASP Top 10 at the time of this document's publication as well as others (refer to the Deep Security Documentation for additional details).

- Intrusion Detection and Prevention and Patching as required by DSS Requirements 11 and 6: Deep Security identifies exploits using its IDS/IPS functionality enhanced with virtual patching. Deep Security's virtual patching blocks vulnerability exploits automatically before vendor patches can be deployed. When using containers, the Deep Security IDS/IPS installed on the host OS can support proactive detection and mitigation of certain vulnerabilities between commits. Deep Security virtual patching can be an effective tool in an organization's DSS-required vulnerability management and patching strategy.
- Authentication and Access Control as required by DSS Requirements 7 and 8: While Deep Security has application accounts/passwords, it is recommended that the organization's active directory or LDAP be used for authentication, including password controls (Requirement 8). Access controls for Deep Security administration, policy configuration, and log monitoring and reporting are addressed by access roles defined within Deep Security.
- Logging and Log Monitoring as required by PCI DSS Requirement 9: Deep Security provides a consolidated log monitoring tool for systems under its control. Network devices and network firewalls are not included in Deep Security's scope of influence. If possible, Deep Security's log sharing capability should be used to offload system logs to the central log server where the organizations SIEM system can be used to monitor the complete CDE infrastructure. It is recommended that the business organizations review log monitoring activities with their QSA to determine whether the organization can meet its PCI DSS Requirement 10 control requirements by using Deep Security exclusively.
- PCI DSS v3.2 Documentation Requirements: PCI DSS v3.2 identifies extensive documentation requirements. When using Trend Micro functionality in the CDE, the documentation must include Deep Security in its scope, including: host-based firewall configuration standards, system configuration settings included in Deep Security policies, access request procedures that include approved access to use Deep Security, and change control procedures for Deep Security policy changes that impact operations of the CDE or other in-scope systems.

APPLICABILITY OF TREND MICRO'S HYBRID CLOUD SECURITY SOLUTION IN A PCI DSS COMPLIANT ENVIRONMENT

As with any solution, there is a specific set of PCI DSS requirements that apply directly to Trend Micro's Deep Security. In order to effectively address PCI DSS requirements, organizations need a clear understanding of where account data is stored, whether stored inside an organization, at a managed on premise data center, or at a cloud service provider such as AWS or Azure. Many of the requirements, such as conducting background checks on employees or ensuring all security policies and procedures are documented, are not applicable to specific software solutions like Deep Security. While some indirect requirements may only be applicable in certain architectures or implementations, many of the requirements of the PCI DSS are directly applicable to Trend Micro's solution regardless of how it's implemented. In fact, Trend Micro's solution can help organizations meet compliance for eight of the twelve PCI DSS 3.2 requirements.

Of additional importance, using Deep Security's broad set of controls, including host IDS/IPS and firewall, to define the scope of the CDE can reduce the scope of annual PCI assessments, lowering the impact of the assessment and streamlining the process of maintaining continuous compliance. The centralized Deep

Security management console can provide administrators and managers a "real time" analysis of the state of physical, virtual, cloud and container workloads in the CDE and highlight identified vulnerabilities so that they can be addressed quickly.

The table below is a high-level summary of where Trend Micro can help organizations with PCI DSS v3.2 compliance.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
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 all personnel

Table 3: High Level Overview

Table 4 across the following pages goes into more detail on how Trend Micro can help organizations with PCI DSS v3.2 compliance.

To find out more about the Trend Micro Hybrid Cloud Security Solution, please visit: http://www.trendmicro.com/hybridcloud.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
Requirement 1: *Install and maintain a firewall configuration to protect cardholder data*			
Organizations must deploy their cardholder data environment in a network compliant with Requirement 1. This requires that necessary policies, procedures, and firewall/router configuration standards be documented and approved by appropriate management and that controls as documented are implemented. Trend Micro's Deep Security can support compliance with Requirement 1 controls. While an organization will need a perimeter firewall that is not completely supported by Deep Security, Deep Security provides stateful inspection and internal network protection that is configurable based upon the needs of the organization and can be used to: • segment the cardholder data environment from other network zones, • control the type of traffic allowed between the cardholder data environment and other network zones, and • provide internal firewalls between cardholder data environment components (for instance, to secure the database used to store account data and other components such as the web server or POS systems located in retail outlets).			
1.1.1	A formal process for approving and testing all network connections and changes to the	✓	While not supporting the formal change process, an organization will need to ensure that the change control process includes updates to policies maintained within Deep Security. Deep Security can supplement change

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
	firewall and router configurations.		control processes when the management console is used to identify newly created virtual network components and notifies the administrator. Information provided on this management console can be used to review all policy changes introduced by administrators. This feature can be used to ensure that required change control procedures were followed and that all changes have been appropriately approved and required change control documentation in place.
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	✓	While Deep Security does not create network diagrams, Deep Security can detect the addition of new servers or VMs. When new components are identified, it can be configured to send email notifications to the administrator so that network diagrams can be updated and to ensure that appropriate Deep Security policies have been implemented.
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	O	While a perimeter network firewall should be installed at Internet egress/ingress points, the Deep Security Host Based Firewall can support 1.1.4 when an organization applies appropriate firewall rules to create DMZ rules within internal network zones. To fully comply with 1.1.4, an organization must still include the requirement for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone within their documented firewall configuration standard. For organizations using a shared hosting provider or cloud service provider, the service provider might have perimeter firewalls that are managed by the service provider and Deep Security Agent can provide host-based firewall rules to provide additional protection. To fully comply with 1.1.4, an organization will need to maintain documentation about firewall rules that are "inherited" from the service provider or other firewalls that impact access to the organizations cardholder data environment (CDE).
1.1.5	Description of groups, roles, and responsibilities for management of network components.	O	While organizations must create necessary documentation to comply with 1.1.5, Deep Security provides preconfigured roles for administering Deep Security policies, including roles for administering firewall and intrusion detection. Roles include Full Access and Auditor. Additional roles can be created. For multi-tenant implementations, roles can be used to assign different organizational entities control over the policies that impact their environment without the ability to impact another "tenant".

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
1.1.7	Requirement to review firewall and router rule sets at least every six months.	○	While 1.1.7 is an administration procedure required by PCI, the Deep Security management console can be used to support 1.1.7 for firewall rules deployed in Deep Security. The console can be used to compare the documented configuration standard to implemented policies.
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	○	An organization's firewall administrator can use the Deep Security Firewall to create firewall rules to restrict traffic between untrusted networks and defined cardholder data environments (CDE) as required by 1.2. *Note: Scoping and segmenting an organization's cardholder data environment is an important concept of PCI DSS. Segmenting an entity's network to isolate only those components that are necessary for processing, storing, and transmitting account data can reduce the scope of the CDE, which must meet ALL PCI DSS v3.2 requirements and must be included in the annual PCI DSS assessment. Using Deep Security Firewall rules to reduce scope of the CDE is feasible based upon an organization's account data processing requirements and how the network is designed and segmented. Questions regarding the scope of an organization's cardholder data environment should be addressed with the organization's QSA.*
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	★	An organization's firewall administrator can use the Deep Security Firewall to implement firewall rules to restrict traffic to that which is necessary for cardholder data environment as required by 1.2.1.b. and that all other traffic is explicitly denied as required by 1.2.1.c.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	○	While the Deep Security Firewall is a host-based Firewall and a perimeter network firewall is recommended, the Deep Security Firewall can be configured to be a DMZ that limits inbound traffic to only authorized systems components with approved services, protocols, and ports. For instance, if a network-based perimeter firewall is provided by a hosted service provider or cloud service provider, Deep Security's host-based firewall can be used to configure DMZ rules into the cardholder data environment and other internal network zones that are appropriate for addressing the segmentation to create a secure cardholder data environment zone(s).
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide	★	An organization's firewall administrator can use the Deep Security Firewall to implement firewall rules to

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
	authorized publicly accessible services, protocols, and ports.		limit inbound Internet traffic to IP addresses within the DMZ as required by 1.3.1.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	★	An organization's firewall administrator can use the Deep Security Firewall to implement firewall rules that prohibit any direct inbound Internet traffic into the cardholder data environment and limit inbound Internet traffic to only IP addresses within the DMZ.
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.		An organization's firewall administrator can use the Deep Security Firewall to implement firewall rules to prevent internal addresses from passing from the Internet into the DMZ.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	★	An organization's firewall administrator can use the Deep Security Firewall to implement firewall rules that prohibit unauthorized outbound traffic from the cardholder data environment to the Internet as required.
1.3.5	Permit only "established" connections into the network.	★	The Deep Security Firewall is a stateful inspection firewall that only permits "established connections" into hosts enabled with this control.
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	★	An organization can use Deep Security Firewall rules to segregate the CDE from the DMZ and other untrusted network zones. To further protect account data, network zones between database and servers storing account data can be segregated from other components such as web or application servers. *Note: This is often a CDE scoping concern for an organization addressing PCI compliance and network segmentation; organization specific questions should be addressed to an organization's QSA.*
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees) and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running.	★	By installing the Deep Security Agent on the device, configuration policies defined in the Deep Security manager can be applied to the laptop or employee owned devices. Configuration settings can include: • Firewall Rules and Stateful Configuration • Intrusion Prevention Rules • Log Inspection Rules • Integrity Monitoring Rules Deep Security assigns unique fingerprints between the Agent and the Manager, which ensures that only the Deep Security Manager can update the agent. All logged events are communicated back to the Deep Security Manager when the heartbeat communication between the two systems occurs.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
	• Personal firewall (or equivalent functionality) is not alterable by users of the portable device.		
Requirement 2: *Do not use vendor-supplied defaults for system passwords and other security parameters*			
Deep Security (software or service) can be used to monitor the security of systems on an organization's network. Once a computer is added to the Deep Security Manager, the administrator can run a "recommendation scan" for security vulnerabilities that need to be addressed. The administrator can decide to automatically implement scan recommendations or address vulnerabilities manually. Periodic scheduled or unscheduled scans can be used to identify newly introduced vulnerabilities. Deep Security does not update security parameters on the system's operating systems but makes recommendations for protections that can be provided by Deep Security's protection modules: • Intrusion Prevention • Integrity Monitoring • Log Inspection When Deep Security is deployed in house, it's essential that software be deployed on secure systems (whether virtual or physical) that meet the control requirements outlined in Requirement 2.			
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. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	O	While each organization must develop and document their own configuration standards based upon the needs of the business and hardening standard that meets those needs, Deep Security can be used to assess security vulnerabilities during Deep Security scans and recommend changes to reduce/mitigate the risk. An organization can configure policies in Deep Security to address the organization's approved configuration standard(s) for virtual systems. With information provided by Deep Security, an organization can improve their configuration standards, and periodic vulnerability scanning can be used not only to identify and resolve systems vulnerabilities, but to also ensure that documented configuration standards are up-to-date. Deep Security's integrity monitoring component can be used to identify when virtual systems configuration files change, thus indicating that the system configuration might be drifting from the organization's approved configuration and associated hardening standard.
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers,	★	Deep Security supports an organization's use of virtualization technology to allow for one primary function per virtual system component or container. Using Deep Security's host-based firewall, different network zones within the CDE can be implemented to provide an additional level of security based upon the

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
	database servers, and DNS should be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*		virtual machine's role. For instance, the database server could be restricted to database calls from the application or web server.
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	○	Deep Security can virtually patch vulnerabilities in unsecured protocols identified in 2.2.3 with its Intrusion Prevention capabilities, and the Deep Security Firewall can be used to block protocols considered insecure and not needed. To address DSS v3.2 requirements regarding limiting the use of insecure SSL and TLS versions, Deep Security can detect versions of protocols and cipher suites used, block transmission to force a change, or generate an alert to notify the administrator that a change is required to address potential compliance issues.
2.3	Encrypt all non-console administrative access using strong cryptography. *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	★	Access to Deep Security's web management console requires HTTPS and supports the use of TLS 1.2 when connecting. As Deep Security has a wide consumer base that does not all require PCI DSS compliance, the Deep Security web management console also allows connections using TLS 1.0 from older browsers. Ensuring that users of the Deep Security web management console are using current web browsers that connect with 1.2 is the responsibility of organizations and should be validated by the organization's QSA during their own PCI DSS validation assessment. Trend Micro has documented a risk mitigation and migration plan for the continued support of TLS 1.0 with a plan discontinue support based on the requirements noted in PCI DSS 3.2, Appendix A2. If other non-console administrative tools allow unsecure ports to access the tool, Deep Security can identify this access and, if appropriate, firewall rules to prohibit access via unsecure protocols could be implemented.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	○	Using Deep Security's visibility tools, an administrator can identify all components defined to the cardholder data environment CDE and review network traffic in and out of the CDE allowed by Deep Security policy to ensure that an organization's inventory of in-scope components is complete.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
			Additionally, Deep Security tracks all virtual systems through the System Event audit trail, an inventory of approved protected systems configured into Deep Security, when a new system is found, and an alert can be generated so that the formal system inventory can be updated once the component is approved. *Note: Network components and physical servers without a Deep Security agent will not be included in the Deep Security inventory, so additional procedures to address these components will need to be considered in the organization's inventory management processes.*
Requirement 3: *Protect stored cardholder data*			
Deep Security does not directly support Requirement 3. Deep Security's capability to identify all systems in a virtual environment and monitoring traffic between these servers can be a useful tool for identifying potential data creep outside of the organization's identified CDE.			
Requirement 4: *Encrypt transmission of cardholder data across open, public networks*			
Trend Micro products do not directly support the encryption of account data; the data transmission controls surrounding the payment transaction and other account data transmission controls are entirely dependent upon the user's architecture and processes for implementing and managing certificates on their websites.			
Requirement 5: *Protect all systems against malware and regularly update anti-virus software or programs*			
Deep Security provides technology to fully support compliance with Requirement 5 of PCI DSS v3.2, used as a malware detection and prevention tool with the organization's malware threat risk analysis and anti-virus policies and procedures.			
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	★	Deep Security provides anti-malware technology for the following platforms (5.1): Microsoft Windows and variants of Linux (examples include RedHat, SUSE, Amazon, and Ubuntu). For a complete list, refer to Trend Micro's website. To ensure all commonly affected systems are running malware prevention, an administrator can assign malware policies using Windows Active Directory interface to identify all Windows systems in the domain or use the Deep Security discovery feature to identify all systems found on the network. Deep Security uses Trend Micro's Smart Protection Network global threat intelligence for up-to-date malware prevention. Maintained by Trend Micro security experts, this cloud-based threat knowledge base is provided with Deep Security. Administrators can customize response to identified threats, including placing identified virus in quarantine and/or deletion. (5.1.1)

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	★	Deep Security is configured to detect and remove or quarantine viruses based upon administrator policies. As mentioned above, Deep Security uses Trend Micro's Smart Protection Network to ensure that known types of malicious software are addressed by Deep Security anti-malware functionality.
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current • Perform periodic scans • Generate audit logs, which are retained per PCI DSS Requirement 10.7	★	Deep Security provides full compliance for Requirement 5.2 and all sub-requirements when configured properly, including: • Use of the global threat intelligence for up-to-date definitions of threats • Defining scans to meet business needs for real-time or manual scan schedules • Generate audit logs of Deep Security malware administration activity and logs of threats identified and actions taken accessed via the Deep Security console, custom reports, sent to syslog/central log servers for retention.
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. *Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	★	Through Deep Security policies, an organization's malware administrator can control which systems must run malware prevention functionality, prohibiting it from being turned off locally. Deep Security assigns unique fingerprints between the Agent and the Manager, which ensures that only the Deep Security Manager can update the agent controlling malware on the system. If malware prevention software needs to be disabled temporarily for testing or troubleshooting, Deep Security allows policy changes to disable anti-virus and audit log of the activity created. The organization will need to ensure that appropriate processes are in place to ensure approvals are obtained for temporarily disabling AV and for re-enabling AV when testing or troubleshooting is complete.
Requirement 6: *Develop and maintain secure systems and applications*			
Deep Security is outside the scope of the application development process but can support an organization's vulnerability and patch management procedures as required in Requirements 6.1 and 6.2. It can also supplement sections 6.5 and 6.6.			
6.1	Establish a process to identify security vulnerabilities, using	O	While an organization should use more than one tool to identify vulnerabilities, Deep Security can be used to

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
	reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.		identify security vulnerabilities in an organization's network and servers, including assessing risk associated with the vulnerability. Deep Security will assign a risk ranking and provide other information, including CVSS score, CVE reference number, and recommendations (6.1.a). Using Deep Security's virtual patching feature, an administrator can apply policies that shield the environment from the vulnerability until a patch is available from the software vendor.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	O	Deep Security's vulnerability scans can be used to identify when operating system security patches and other critical software security patches are not up-to-date. By identifying such vulnerabilities, including CVSS score for the vulnerability, an organization can use the information in their patch management process to identify critical patches and schedule patches based upon criticality. (6.2.b) Using Deep Security's virtual patching feature, an administrator can apply policies that shield the environment from the vulnerability until a patch is available from the software vendor. As a critical security component, it is important that Deep Security updates are regularly applied; Deep Security provides updates automatically with its Deep Security Relay feature that ensures Deep Security software is up-to-date. Administrators can schedule a task in Deep Security to update the software periodically to ensure the most up-to-date version of Deep Security is in place.
6.4.2	Follow change control processes and procedures for all changes to system components	O	Deep Security application control provides role-based access control for administration privileges that supports an organization's procedures for separation of duties (6.4.2). Changes to Deep Security application control settings support permissions-driven back-out ("undo") functionality, which is necessary for a compliant change control process (6.4.5.4).
6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities and understanding how	✓	An organization can supplement their secure coding practices by utilizing Deep Security's IDS/IPS control and its application vulnerability monitoring feature to detect: • Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP, and XPath injection flaws as well as other injection flaws. (6.5.1) • Buffer overflow. (6.5.2)

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
	sensitive data is handled in memory. • Develop applications based on secure coding guidelines. *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*		• Insecure communications. (6.5.4) Deep Security can identify deprecated Transport Protocols improper error handling. • Improper error handling. (6.5.5) Deep Security can block errors and also provides the ability to replace default errors with user configurable custom messages in response. • High risk vulnerabilities identified in the vulnerability identification process. (6.5.6) • Cross-site scripting (XSS). (6.5.7) • Improper access control. (6.5.8) Deep Security can detect Failure to Restrict URL Access: Allowed Resources OR Disallowed Resources.
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: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. *Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	✓	Deep Security's IDS/IPS application vulnerability protection feature does not provide the full set features required by the PCI DSS 6.6 for a web application firewall; however, it does protect against many of the 6.5 OWASP Top 10 vulnerabilities and other application-based vulnerabilities. If an organization does not have a traditional Web Application Firewall in place and instead performs periodic application vulnerability reviews as required, the organization can supplement their periodic application vulnerability reviews using Deep Security Application protection in between scans. Deep Security can detect and protect against many web application vulnerabilities from the current OWASP Top 10 at the time of this document's publication, as well as others (refer to the Deep Security Documentation for additional details) including: • A1: Injection – Deep Security: Generic SQL Injection Prevention. • A2: Cross-Site Scripting (XSS) – Deep Security: Generic Cross-Site Scripting (XSS) Prevention. • A6: Security Misconfiguration – Deep Security: Addressed on a case by case basis including several specific CVEs. • A8: Failure to Restrict URL Access – Deep Security: Allowed Resources OR Disallowed Resources.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
			• A9: Insufficient Transport Layer Protection – Deep Security: Identifies deprecated Transport Protocols. • A10: Un-validated Redirects and Forwards – Deep Security: Addressed on a case by case basis including several specific CVEs.
Requirement 7: *Restrict access to cardholder data by business need to know*			
Deep Security does not directly support access control to cardholder account data, but access to Deep Security administrator activities are controlled within Deep Security. Deep Security restricts administrative activities performed within the Deep Security console that configure firewall, IDS, and FIM rules and scanning policies. While direct access by administrators to virtual systems is not controlled by the Deep Security access restrictions, activities that are performed by administrators that generate event logs would be captured by Deep Security and included in management console and log inspection/monitoring activities performed by Deep Security.			
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	✓	Access control to systems and cardholder data is usually controlled through the organization's access control systems and will not be impacted by Deep Security. Deep Security does supplement role-based access control for administration privileges that are used through the Deep Security management console, including supporting multi-tenant capabilities, which provides separation of Deep Security administration responsibilities to a single tenant environment.
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	✓	While roles controlling access to systems and cardholder data are controlled through the organization's access control systems, Deep Security has two pre-defined roles for administrators controlling security administration activities performed within Deep Security: all access (global administrator) and audit (view only). Within Deep Security, an organization can define Deep Security administration activities based upon business need. Large organizations can define administrators to sub-segments of an organization's virtual network, thus restricting administrative activities to the assigned network segment.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	✓	While Deep Security does not address direct access by systems administrators to a system, an organization should consider Deep Security administrators as privileged users that control security features within a CDE. An organization can define roles that limit Deep Security administration access based upon customized access rules defined to the role. For instance, in a multi-tenant environment, each tenant could have a unique role that is assigned to their Deep Security

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
			administrator and allows updates to Deep Security to only defined accounts. Additional roles include Auditor, which enables read-only access to application and system event logs. *Note: Privileged operating system access is not controlled by Deep Security and must be managed at the operating system level; though, Deep Security scanning rules can be used to identify changes made by the operating system administrator that do not meet policies defined in Deep Security.*
7.1.3	Assign access based on individual personnel's job classification and function.	○	An organization can define roles that limit Deep Security administration access based upon customized access rules defined to the role. For instance, in a multi-tenant environment, each tenant could have a unique role that is assigned to their administrator and allows updates to Deep Security to only defined accounts. *Note: privilege operating system access is not controlled by Deep Security and must be managed at the operating system level; though, Deep Security scanning rules can be used to identify changes made by the operating system administrator that do not meet policies defined in Deep Security.*
7.1.4	Require documented approval by authorized parties specifying required privileges.	✓	An organization's access control procedures must include a process for approving and monitoring access control rights; these procedures will need to include access requests for adding and changing access rights to the Deep Security manager. Available Deep Security event logs can be used to monitor granted or changed Deep Security privileges to ensure documented process for granting access is enforced.
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: 7.2.1 Coverage of all system components 7.2.2 Assignment of privileges to individuals based on job classification and function. 7.2.3 Default "deny-all" setting.	○	Deep Security only provides an access control mechanism to activities administered through the Deep Security management console. Access control rules are limited to those controlled by Deep Security, so an organization's application and operating system access control mechanisms will continue to be used. Within Deep Security, privileges can be assigned by on job responsibilities using Deep Security's role-based access controls. Except for the initial global admin and audit account, Deep Security policies for all new users are defined as deny-all until rules are explicitly defined to grant access.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
Requirement 8: *Identify and authenticate access to systems components*			
Deep Security supports SAML and can interface with an organization's Active Directory or LDAP for authentication, which is the recommended configuration. If Deep Security for a Service is used, application authentication built into the product can be used. Trend Micro does not provide authentication services to cardholder data environment components.			
Requirement 9: *Restrict physical access to cardholder data*			
Trend Micro does not support physical access control requirements identified in Requirement 9. Organizations running their cardholder environment on-premises must provide the required physical access mechanism. If an organization is running their cardholder data environment in a Shared Hosting Provider or other service provider, the organization should have contractual obligations about use of appropriate physical controls and establish a process for monitoring compliance of the service provider to Requirement 9. If using Trend Micro Deep Security service (which is certified as a Level 1 Service provider), it is important to ensure that log records which might be stored in the service contain no account data.			
Requirement 10: *Track and monitor all access to network resources and cardholder data*			
Deep Security stores logs of Deep Security activities and collects the event logs from systems in its control. Logs are stored in the Deep Security database. On-premise implementations can configure log storage period to meet their needs. Logs are viewable by drilling down to details using the management console or by creating reports. It is recommended that logs are shared with the organization's SIEM so that all of the organization's logs can be monitored from a single, central log repository. Deep Security supports integration with leading SIEMs like IBM Q-Radar and HP ArcSight, as well as Splunk.			
10.1	Implement audit trails to link all access to system components to each individual user.	○	Deep Security provides audit trails from firewall, intrusion prevention, integrity monitoring, anti-malware, web reputation, and log monitoring, as well as logging Deep Security administrator activities including access controls to Deep Security software and maintaining policies for Deep Security's use and management. Additionally, Deep Security's log inspection engine can analyze third-party log files, providing a framework to parse, analyze, rank, and correlate events across systems, including Windows and Linux. Individual users are active directory or LDAP user accounts and date/timestamps used by Deep Security are derived from the organizations central time server, so logs from other systems can be correlated with Deep Security logs when Deep Security logs are loaded into the organization's SIEM solution.
10.2.	Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual user accesses to cardholder data	★	Deep Security collects logs from Windows and Linux systems identified to Deep Security and logs of Deep Security administrator activity. It collects event logs and includes them in Deep Security manager console and log reports. If the event is captured by the system, the log will be collected by Deep Security.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
	10.2.2 All actions taken by any individual with root or administrative privileges 10.2.3 Access to all audit trails 10.2.4 Invalid logical access attempts 10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges 10.2.6 Initialization, stopping, or pausing of the audit logs 10.2.7 Creation and deletion of system-level objects.		
10.3	Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource.	○	Deep Security collects logs from virtual Windows and Linux systems identified to Deep Security. The log content is controlled by the virtual system and is made available to Deep Security users of the console or reports. If the event data is captured by the virtual system, the data will be available in Deep Security. Event/log entries generated by Deep Security include all PCI DSS 10.3 required information (10.3.1 – 10.3.6). *Note: An organization using both physical and virtual systems in the CDE will need to capture events/log records from physical systems.*
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. - Critical systems have the correct and consistent time	○	All computers where Deep Security software runs should be synchronized with the organization's NTP server. Deep Security log records are stored with UTC providing synchronization by date/timestamp of log records. While log records are stored with UTC, the timestamp is converted to user's time zone when displayed on the console.
10.5	Secure audit trails so they cannot be altered. 10.5.1 Limit viewing of audit trails to those with a job-related need. 10.5.2 Protect audit trail files from unauthorized modifications.	○	Deep Security access capabilities include limiting access to viewing and editing audit trail logs based on user role. Log records collected by the Deep Security agent are stored in the agent's file system encrypted until moved to the Deep Security manager database. Log/event files collected by the Deep Security Agent are encrypted to prevent tampering. Logs are passed to the management server as part of Deep Security

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. 10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. 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).		manager-to-agent heartbeat check process. At this time, if configured in Deep Security, records will be sent to the organization's central log server/SIEM system. Deep Security provides the option to pass log records using common criteria certificate to ensure that records are not altered or lost during transmission.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	○	Deep Security can be a critical component in an organization's log monitoring program through information provided by its management console and custom reports (10.6). The Deep Security's log inspection rules can be customized to meet the review criteria specific to the organizations business, with email alerts generated when someone in the organization needs to review/research anomalies or suspicious activity identified by Deep Security. Additionally, logs generated by Deep Security can be loaded to an organization's SIEM system to provide consolidated log storage and reporting.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	○	The Deep Security administrator can instruct all managed computers to send logs to a centralized Syslog computer or configure individual computers independently, putting control of log retention on to the organization. Within Deep Security, logs are by default retained for 53 weeks, but can be configured for longer retention. If using the Deep Security SaaS option, it is recommended that an organization use the option to have log records sent to the organization's central log server for longer term retention to meet the requirement for at least one-year retention.
10.8	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	✓	While an organization must ensure that policies and operational procedures are appropriately documented, Deep Security's management console can be used to supplement this documentation with information on actual log policies and monitoring procedures implemented for compliance to the operational procedures. (10.8)
Requirement 11: *Regularly test security systems and processes*			

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance O partially supports compliance ✓ supplements control requirement			
While Trend Micro is not a PCI Authorized Scanning Vendor (ASV), Deep Security can provide more frequent vulnerability scanning assisting in an organization's everyday compliance efforts. With administrator defined scheduling, systems vulnerability scans can occur frequently and vulnerabilities addressed as issues are identified. Deep Security's console highlights problems with easy to read graphs and icons and provides the ability to drill down to details needed to research issues. Organizations requiring PCI compliance must address their external scanning requirements with a PCI ASV. Internal scanning requirements will need to be supplemented based upon the scope of the cardholder data environment. For an organization's specific compliance requirements associated with their specific environment, an organization should contact their QSA.			
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, or product upgrades).	O	Deep Security supplements an internal scanning process. Unlimited vulnerability scanning can provide more vulnerability checking than might be possible by other internal scanning options. While Deep Security scans do not include an indicator for PCI compliance, common vulnerabilities will be identified and can be addressed prior to "formal" quarterly internal scanning. Note that scans will only capture vulnerabilities of virtual Windows and Linux systems; other components will need to be addressed in the organization's quarterly vulnerability scanning process. *Note: External scanning is not supported and external scanning must be supported by a PCI Approved Scanning Vendor (ASV).*
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment, as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	O	Deep Security's host-based firewall solution supplements network-based firewalls IDS/IPS solutions by including host-based intrusion detection/prevention (see *Deployment Models* in this paper for more details). Deep Security monitors network traffic into each system to prevent and alert personnel of suspected compromises. Administrators can create policies and actions for intrusion detection and prevention, such as automatically blocking traffic or removing a system from network should a suspected compromise occur. Deep Security's security updates shield systems against newly discovered vulnerabilities with updates delivered automatically to the organization when available. Additionally, Deep Security's Recommendation Scan feature can provide valuable information to prevent possible compromises in the future by scanning host systems to identify applications that might be vulnerable and by recommending rule changes to address the vulnerability.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized	★	Deep Security can be configured to monitor identified critical operating systems, application and configuration files (11.5.a), and registry on virtual systems that have been modified; administrators can configure monitoring

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
	modification (including changes, additions, and deletions) of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).		for real-time change monitoring or periodic monitoring, which supports the DSS requirement for monitoring for unauthorized changes to critical files at least weekly (11.5.b), and can define criteria for alerting appropriate responders when critical files have been modified. (11.5.1) *Note: If there are critical systems or components not included in Deep Security Policies, an additional FIM tool may be required.*
Requirement 12: *Maintain a policy that addresses information security for all personnel*			
For the most part, Trend Micro's functionality does not support the policy documentation requirements of Requirement 12. Deep Security email alerts could supplement the vendor monitoring activities (12.8.4) and the incident response plan activities (12.10), as identified below. Along with the rest of the cardholder data environment, the use of all Trend Micro tools must be covered by and managed in accordance with all of the organization's policies and procedures. However, discussion of these policies and procedures is outside the scope of this paper and organizations should consult with their own QSA regarding their coverage and compliance.			
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	○	Depending upon the services provided by an organization's service providers, Deep Security can partially support the monitoring activities of service providers. For hosted sites and cloud service providers, Deep Security can be installed on a virtual machine or host OS, or as a SaaS running at Trend Micro and used to monitor virtual and physical server configurations. Using scanning policies that can be configured by the organization rather than the service provider being monitored, scans can identify vulnerabilities in virtual and physical system configurations for systems running the Deep Security agent.

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
			Note: Monitoring of firewalls and routers cannot be performed by Deep Security.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	○	While a fully documented Incident Response Plan is required by 12.10, Deep Security partially supports or supplements an organization's incident response planning through its intrusion prevention/detection and file integrity management technology and alerts. Organizations can build use of Deep Security monitoring into the Incident Response Plan requirement (12.10), including • Using the Deep Security intrusion detection policies to generate specific incident responses such as isolating impacted system from the organizations network when intrusion is detected (12.10.1) • Using Deep Security initiated email alerts (12.10.3) • Using intrusion-detection, intrusion- prevention, firewalls, and file-integrity monitoring functionality (12.10.5) to identify and alert when intrusion is detected.
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers			
Deep Security can assist a Shared Hosting Provider in meeting the additional requirements for securing the hosted entities environments as required in Appendix A. *Note that Deep Security only supports access controls for Deep Security management activities and log storage and monitoring for activities administered through Deep Security console; additional tools will be necessary to completely address Appendix A requirements.* Below is general information about how Deep Security can support a Shared Hosting Providers compliance with PCI DSS Appendix A Due to the complexity of Shared Hosting Providers, it is recommended that discussions between Trend Micro, the shared hosting provider, and the shared hosting provider's QSA be held to address the shared hosting provider's unique technical environment.			
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	○	Deep Security supports a Shared Hosting Provider's compliance with A.1.1 through use of its multi-tenancy capabilities. Deep Security allows an organization to create multiple distinct management environments by creating a unique tenant for each entity the Shared Hosting Provider supports. When a new tenant is created by an administrator, "medium isolation" of settings, policies, and events for the tenant is provided within the Deep Security management database server. Deep Security can provide "high isolation" when a Shared Hosting Provider uses a separate database server for each tenant.
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data	○	Shared Hosting Providers can choose to use medium or high isolation by either using a single database server to support multiple tenants or by using a unique database server for each tenant. Logs are stored in the

DSS REQ.	REQUIREMENT DESCRIPTION	DEEP SECURITY	EXPLANATION/CONSIDERATIONS
★ fully supports compliance ○ partially supports compliance ✓ supplements control requirement			
	environment and consistent with PCI DSS Requirement 10.		Deep Security database. Access rules can be used to provide tenant-based access to Deep Security logs and policies stored in a medium isolation implementation. A Shared Hosting Provider could choose to use individual tenant log servers as an alternative for providing complete segregation of logs within Deep Security. Deep Security provides configurable retention for logs stored in the database configured on-premises. If the Deep Security SaaS is used to support the Shared Hosting Provider, the organization should transmit and store logs in the organization's SEIM.

Table 4: Applicability of PCI DSS 3.2 Controls to Trend Micro's Deep Security

CONCLUSION

While there are additional scoping concerns and risks associated with virtualization and cloud computing, it is possible to implement a PCI DSS compliant solution within these types of environments, and Trend Micro's Deep Security product supports this.

The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of Trend Micro Deep Security in the clients CDE and the context in which it is implemented. Organizations must ensure that it is clearly understood which entity is responsible for each PCI DSS control requirement, that appropriate service provider monitoring activities are in place to monitor that security, and operating controls are in place and active "everyday."

Deep Security can be an important tool in an organization's effort to maintain continual PCI DSS v3.2 compliance. Firewall, IDS/IPS, application control, and malware prevention capabilities provide system and network level protection, while log monitoring and vulnerability scanning provide the ability to identify problems that need to be addressed by the systems administrator. The administrator can use the Deep Security management console's graphical interface to monitor for compliance issues and, if necessary, drill down to log details, allowing for a more thorough investigation. Automated virtual patching capabilities ensure significant vulnerabilities are addressed (shielded) quickly, allowing time for systems administrators to test and schedule vendor patches.

Trend Micro Deep Security not only supports the implementation of PCI DSS control requirements, it includes features that can facilitate the users desire to mitigate the risks of implementing their CDE in a CSP.

REFERENCES & RESOURCES

1. Cloud Special Interest Group, PCI Security Standards Council. (February 2013). Information Supplement: PCI DSS Cloud Computing Guidelines
2. Virtualization Special Interest Group, PCI Security Standards Council. (June 2011). Information Supplement: PCI DSS Virtualization Guidelines
3. PCI Security Standards Council. (August 2013) Data Security Standard and Payment Application Data Security Standard, Version 3.0 Change Highlights
4. AWS PCI DSS Level 1 FAQs: AWS website
5. Amazon Web Services. (Novermber 2013). Amazon Web Services: Risk and Compliance
6. Microsoft. (January 2014). Windows Azure TM Customer PCI Guide: Microsoft website
7. PCI Security Standards Council. (April 2015) Payment Card Industry (PCI) Data Security Standard – Summary of Changes from PCI DSS Version 3.0 to 3.1
8. PCI Security Standards Council. (April 2016) Payment Card Industry (PCI) Data Security Standard – Summary of Changes from PCI DSS Version 3.1 to 3.2
9. PCI Security Standards Council PCI Perspectives Blog - PCI DSS 3.2: What's New? Posted by Laura Johnson on April 28, 2016 in TLS/SSL and interview and PCI DSS: https://blog.pcisecuritystandards.org/pci-dss-32-is-here
10. Third-Party Security Assurance and Shared Responsibilities Special Interest Groups, PCI Security Standards Council. (March 2016). Information Supplement: Third-Party Security Assurance PCI DSS Virtualization Guidelines
11. PCI Security Standards Council. (May 2017). Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation
12. Best Practices for Maintaining PCI DSS Compliance Special Interest Group. (August 2014). Information Supplement: Best Practices for Maintaining PCI DSS Compliance

ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. www.trendmicro.com

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com

WP_TREND_MICRO_AND_PCI_DSS_V3_2_COMPLIANCE_082017