WHITE PAPER

Broadcom Inc. VMware vDefend Product Applicability Guide for PCI DSS 4.0.1

Applicability to Assist Payment Card Customers in Regulatory Compliance

COALFIRE OPINION SERIES – Version 1.4

Jason Wikenczy, CISSP, CISA, QSA | Principal
Payments Advisory & Product Guidance

Table of contents

Executive summary

Broadcom Inc. (“Broadcom”) has engaged Coalfire Systems, Inc., or its subsidiaries (“Coalfire”), a respected Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent technical review of VMware vDefend (“VMware vDefend”) in the form of a Product Applicability Guide (PAG). This guide examines a use case for a payment entity’s deployment of VMware vDefend in alignment with technical requirements to the PCI Data Security Standard (PCI DSS) 4.0.1. This paper outlines Coalfire’s methodology for assessment and the approach used for the review, summarizes findings from the review of product capabilities, provides context for the possible use of these capabilities, defines parameters to form a common basis of understanding, and states an opinion as to the usefulness of VMware vDefend within a program of compliance for PCI DSS 4.0.1.

Coalfire opinion

Coalfire has determined that VMware vDefend Firewall with Advanced Threat Protection can be an effective solution when employed in PCI DSS 4.0.1 assessed environments. VMware vDefend comes integrated with many security features and functions that can effectively support numerous PCI DSS technical control requirements.

Introducing the PCI DSS

PCI DSS is a framework that defines the baseline physical, technical, and operational security controls, known as requirements and sub-requirements, necessary for protecting payment card account data. PCI DSS defines two categories of payment card account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and sensitive authentication data (SAD), which includes full track data (magnetic-stripe data or equivalent on a chip), card verification code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs) or PIN blocks entered during the transaction (PCI DSS: Requirements and Testing Procedures, version 4.0.1, March 2024).

PCI DSS requirements “apply to entities with environments where account data (CHD and/or SAD) is stored, processed, or transmitted” (PCI DSS 4.0.1, 2024). These organizations include, but are not limited to, merchants, payment processors, issuers, acquirers, and service providers. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of the people, processes, and technologies that store, process, or transmit CHD or SAD. PCI DSS defines twelve requirements designed to address six objectives, as shown in the high-level overview below:

Objectives	Requirements
Build and maintain a secure network and systems	**1.** Install and maintain network security controls (NSCs) **2.** Apply secure configurations to all system components
Protect account data	**3.** Protect stored account data **4.** Protect CHD with strong cryptography during transmission over open, public networks
Maintain a vulnerability management program	**5.** Protect all systems and networks from malicious software **6.** Develop and maintain secure systems and software
Implement strong access control measures	**7.** Restrict access to system components and CHD by business need to know **8.** Identify users and authenticate access to system components **9.** Restrict physical access to CHD

Objectives	Requirements
Regularly monitor and test networks	**10.** Log and monitor all access to system components and CHD **11.** Test security of systems and networks regularly
Maintain an information security policy	**12.** Support information security with organizational policies and programs

Table 1: PCI DSS 4.0.1 high-level overview

The PCI DSS program is concerned with operations, not components in the abstract. Thus, the hardware and software used in a compliance program, except for point-of-sale (POS) and point-of-interaction (POI) systems, are considered ineligible for component certification because of specific PCI DSS program scope (PCI DSS 4.0.1, 2024).

In place of component certification, de facto analysis of components and ineligible systems reviewed by industry-recognized authorities (e.g., Coalfire) using guidelines and methods identical to the actual assessment and certification processes may serve as a guide for successful use of VMware vDefend in an assessment.

This Coalfire PAG documents the potential use of VMware vDefend as part of an overall technical approach to PCI DSS compliance. Coalfire PAGs have been used since 2014 by various participants in the PCI community to understand how solutions that do not require PCI compliance validation may be successfully used in support of a PCI DSS compliance program.

Payment card industry use of this PAG

This PAG is intended to be used by various PCI entities and other interested parties involved in sales, construction, operation, or infrastructure assessment that use the VMware vDefend suite. This document is intended to help VMware vDefend customers understand the controls built into the core infrastructure space, as well as the general availability of control options that may be implemented by the customer for the workload space.

The following sections explain how this PAG may be used by various entities throughout the PCI DSS life cycle. The entities include merchants and financial institutions, payment solution service providers, infrastructure as a service (IaaS) and platform as a service (PaaS) service providers, designated entities, others who share responsibility with a payment entity, and PCI DSS qualified security assessors (QSAs).

Merchants and financial institutions

PCI DSS requirements provide a framework of standards that, when implemented, support security for payment card transactions flowing from the merchant point-of-use, where payment and authorization transactions are initiated, to the financial institutions that provide the acquisition and settlement of a customer’s purchase. VMware vDefend may be used as a foundation for merchants and financial entities as a solution to support CDE workloads. This PAG is primarily intended to highlight a use case where a VMware vDefend customer could implement security controls into the core infrastructure of VMware vDefend and how those security controls align with PCI DSS requirements.

Service providers, designated entities, and shared PCI DSS responsibility

PCI DSS makes provisions for payment entities to use service providers to store, process, or transmit CHD on behalf of the payment entity or to manage components such as routers, firewalls, databases, physical security, or servers. CHD security is impacted in the course of providing services to PCI entities, and, therefore, such service providers are responsible for compliance with PCI DSS. This is also true of multi-tenant service providers who provide services to multiple payment entities. Requirements under section 12.8 of PCI DSS 4.0.1 are focused on managing the “risk to information assets associated with third-party service provider (TPSP) relationships” (PCI DSS 4.0.1, 2024). Multi-tenant service provider requirements, in addition to PCI DSS requirements, are listed in Appendix A1 of PCI DSS 4.0.1. This

PAG may be useful for service providers using or planning to use VMware vDefend in environments where CHD is stored, processed, or transmitted.

This PAG may also be useful where a designated entity's use of VMware vDefend is involved with the storage, processing, or transmission of CHD, or impacts the security of the CDE. Designated entities constitute an additional category of entities for which PCI DSS is applicable. A designated entity may be any payment entity, including merchants or service providers, that a payment brand or acquirer determines requires additional supplemental validation of existing PCI DSS requirements. Examples of designated entities include those storing, processing, or transmitting large volumes of CHD; those providing aggregation points for CHD; or those who have suffered significant or repeated CHD breaches. Additional requirements for designated entities are found in Appendix A3 of PCI DSS 4.0.1.

PCI DSS QSAs

This PAG and supporting materials may assist a PCI DSS QSA in evaluating the implementation of VMware vDefend during assessment activities that contribute to a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). In the section titled "VMware vDefend applicability to PCI DSS," in this document, Coalfire aligns the technical controls referenced in PCI DSS 4.0.1 with findings for how VMware vDefend provides controls that can meet those requirements. Where applicable, Coalfire references the additional implementation steps documented in this PAG to be performed by the customer when deploying and supporting a PCI DSS compliance program. Other products may be required in conjunction when implementing VMware vDefend to comply with the PCI DSS requirements as intended, and Coalfire notes those products, such as network security controls (NSCs), where applicable.

The guidance in this PAG and supporting materials are intended to provide Coalfire's opinion and are not meant to supplant or compromise the independent judgment required to perform PCI DSS assessments. The PCI SSC Code of Professional Responsibility requires QSA companies and employees to "adhere to high standards of ethical and professional conduct". Coalfire supports and upholds independent QSA judgments that might differ from this opinion.

Objectives of this PAG

This PAG's primary objective is to render an opinion on VMware vDefend's suitability to assist merchants with meeting the requirements of PCI DSS 4.0.1. The following process is intended to illustrate Coalfire's findings and satisfy this objective and will:

- Analyze VMware vDefend and its features using practices identical to an actual payment card assessment and guidance provided in QSA reactions.
- Evaluate the key features of VMware vDefend per control for their ability to support the requirements.
- Make relevant observations and recommendations about each control family and the suggested implementation approaches for VMware vDefend features to support meeting the objectives of these controls.
- State Coalfire's opinion.

Since the review of VMware vDefend review was not conducted on an actual payment card entity running a real-world merchant or service provider workload, Coalfire focused on the technical controls for PCI DSS. Coalfire did not review organizational processes, training, procedures, written supporting materials, or other non-technical controls called for in PCI DSS. The customer is responsible for PCI DSS processes, such as organizational, procedural, and training controls, which pertain to implementation by a real payment card entity.

The role of VMware vDefend

VMware vDefend represents a comprehensive approach to securing private cloud environments. Designed with a focus on micro-segmentation, advanced threat prevention, and actionable security intelligence, VMware vDefend helps organizations strengthen their security posture while supporting compliance with frameworks such as PCI DSS.

Self-regulation and industry standards

The payment card industry operates within a self-regulation framework, relying on standards such as PCI DSS to ensure the protection of cardholder data. These standards are built on the Plan-Do-Check-Act (PDCA) model, which emphasizes a continuous improvement cycle for security controls. VMware vDefend aligns with this approach, offering tools that support the iterative assessment, implementation, and refinement of security measures.

SecOps footprint and operational excellence

For organizations with large security operations (SecOps) footprints, VMware vDefend provides essential capabilities such as intrusion detection and prevention systems (IDS/IPS); network traffic analysis (NTA); network detection and response (NDR) and advanced micro-segmentation, enabling visibility, threat detection, and lateral movement of threat containment. These features help reduce operational complexity and enhance real-time decision-making for security teams.

In the context of PCI DSS, VMware vDefend's offerings facilitate compliance with key security requirements. Key differentiators of VMware vDefend include:

- Micro-segmentation securing east-west traffic within data centers to reduce lateral movement of threats.
- Advanced threat prevention addressing sophisticated attack vectors with tools such as IDS/IPS, NTA, NDR and malware prevention/sandboxing.
- Security intelligence visualizing application topologies and providing granular insights for policy enforcement.
- Tooling to enhance operational oversight, aligning with PCI DSS' emphasis on monitoring and incident response.

VMware vDefend's extensible software defined architecture provides compatibility with existing controls, facilitating both direct compliance and operational enhancements. By bridging the gap between compliance and operational security, VMware vDefend equips organizations to meet the demands of both assessors and evolving cyber threats.

The VMware vDefend solution

vDefend represents a comprehensive approach to securing modern private cloud IT environments, including cloud, multi-cloud, and hybrid cloud deployments. Designed with a focus on micro-segmentation, advanced threat prevention, and actionable security intelligence, vDefend helps organizations strengthen their security posture while supporting compliance with frameworks such as PCI DSS.

Aligning with SecOps workflows, VMware vDefend overlays actionable insights and automation on technical controls to enhance operational efficiency. For organizations managing complex environments, VMware vDefend facilitates the detection, analysis, and remediation of threats while reducing the noise of false positives. This enables security teams to prioritize resources effectively, for faster response times and more efficient operations.

VMware vDefend Firewall

At the core of VMware vDefend's solution is VMware vDefend Firewall, available in Distributed Firewall and Gateway Firewall configurations, each serving distinct but complementary purposes.

The VMware vDefend Distributed Firewall operates at the hypervisor level, providing micro-segmentation to secure lateral (east-west) traffic within environments. This capability can isolate sensitive workloads, such as those in a cardholder data environment, thus helping contain PCI DSS scope. Effective segmentation not only contains PCI scope but also helps simplify threat detection through clearly defined boundaries, reducing noise from outlying systems. With granular policy controls, VMware vDefend Distributed Firewall supports dynamic, workload-specific configurations and policy enforcement, so that security can adapt to changes in the environment.

VMware vDefend Gateway Firewall is a next generation, software-defined internal firewall that enforces zone-based policies within the private cloud. With its multi-tenancy capability, it enables secure hosting of multiple tenants within an enterprise or service provider environment, while its security zones ensure security policy enforcement. Advanced features include user identification and application Layer-7 identification, and FQDN filtering. Since VMware vDefend Gateway Firewall was designed specifically with VMware vDefend Distributed Firewall in mind, together they offer a layered approach to private cloud lateral security all from a single console. Both offer full integration with VMware vDefend Advanced Threat Prevention technologies and VMware Cloud Foundation.

Both VMware vDefend Firewall configurations can integrate with SecOps workflows, providing visibility and actionable intelligence for proactive and reactive security measures.

VMware vDefend Advanced Threat Prevention

VMware vDefend Advanced Threat Prevention (ATP) integrates capabilities such as IDS/IPS, NTA, network detection and response (NDR), and Malware Prevention (sandbox) into the VMware vDefend Distributed and Gateway Firewalls without adding operational complexity. Each of these features is designed to enhance SecOps incident response and forensic analysis capabilities.

IDS/IPS functionality supports multiple PCI DSS requirements by detecting, alerting to, and mitigating suspicious activities and threats in real-time. By preventing unauthorized access and lateral movement, this feature is instrumental in protecting in-scope systems. For SecOps teams, the ability to correlate IDS/IPS alerts with broader network traffic analysis through NTA and NDR provides deeper context and faster threat validation. NTA and NDR further enhance visibility, using machine learning and behavioral analysis to detect anomalous patterns and potential threats across the network. Malware Prevention provides an additional layer of defense by identifying and blocking malicious files and payloads before they can compromise sensitive systems.

Security Intelligence for VMware vDefend

Complementing the VMware vDefend Firewall and VMware vDefend ATP features is Security Intelligence for VMware vDefend, a tool tailored for proactive security workflows. It provides visibility into application communication and network traffic patterns, allowing teams to identify anomalies and optimize segmentation strategies. With integration into SecOps tools, Security Intelligence for VMware vDefend supports and continuously monitors the environment, provides a Segmentation Assessment report and blast radius, and updates the Security Posture score based on real-time conditions—key components of an effective security program. Its integration with other VMware vDefend technologies allows for continuous monitoring and automated policy recommendations, facilitating ongoing compliance with PCI DSS and other industry standards. By automating policy recommendations and facilitating continuous monitoring, it reduces manual effort and helps maintain compliance in dynamic environments.

Security Intelligence for VMware vDefend is available across both the VMware vDefend Firewall and ATP packages, offering flexibility for users at various stages of the security journey.

Specialized capabilities for SecOps enhancement

The VMware vDefend ATP solution includes Network Detection and Response (NDR) capabilities. The goal of NDR is to simplify SOC monitoring, threat triaging, scoping and threat hunting by managing alert overhead and continuously correlating signals (events) from IDPS, Malware detection/prevention and Anomaly Detection (NTA) into prioritized and actionable campaigns that "connect the attack chain". This allows SecOps teams to focus on the small number of incidents that really matter and ignore the noise. vDefend ATP leverages AI and ML to detect anomalies on the network, identify previously unknown malicious files in the sandbox and to correlate events that make up a complex attack chain. In addition, Intelligent Assist for VMware vDefend is a GenAI-driven co-pilot that further helps security teams to reduce the Mean Time To Detect and (MTTD) and Mean Time to Respond (MTTR) .

Intelligent Assist can explain threats and events in plain English, which allows security, network and virtualization teams to immediately assess the scope and impact of individual threats. Intelligent Assist can also take effective, automatic, and immediate remediation actions once a threat has been deemed a true positive. Security Intelligence continuously collects network and endpoint data, which can be used for threat hunting and forensics without needing to rely on external tools.

The VMware vDefend ATP solution includes Network Detection and Response (NDR) capabilities. The goal of NDR is to simplify SOC monitoring, threat triaging, scoping and threat hunting by managing alert overhead and continuously correlating signals (events) from IDPS, Malware detection/prevention and Anomaly Detection (NTA) into prioritized and actionable campaigns that "connect the attack chain". This allows SecOps teams to focus on the small number of incidents that really matter and ignore the noise. vDefend ATP leverages AI and ML to detect anomalies on the network, identify previously unknown malicious files in the sandbox and to correlate events that make up a complex attack chain. In addition, Intelligent Assist for VMware vDefend is a GenAI-driven co-pilot that further helps security teams to reduce the Mean Time To Detect and (MTTD) and Mean Time to Respond (MTTR) .

Intelligent Assist can explain threats and events in plain English, which allows security, network and virtualization teams to immediately assess the scope and impact of individual threats. Intelligent Assist can also take effective, automatic, and immediate remediation actions once a threat has been deemed a true positive.

Security Intelligence continuously collects network and endpoint data, which can be used for threat hunting and forensics without needing to rely on external tools.

The VMware Web Application Firewall (WAF), included in the VMware Avi Load Balancer solution, plays a key role in enhancing security and compliance by protecting application layers from common vulnerabilities. Its traffic filtering and web application layer protection capabilities support multiple PCI requirements aimed at securing and monitoring workloads. Avi WAF monitoring capabilities feed into broader security programs, supporting SecOps teams in addressing web application-related risks.

VMware vDefend delivers tools for critical PCI DSS compliance activities through integrations with SecOps workflows. VMware vDefend's emphasis on visibility, automation, and actionable intelligence helps detect and respond to perimeter and lateral threats effectively.

VMware vDefend's focus on micro-segmentation, advanced threat detection, and security intelligence positions it as a strategic solution for organizations seeking to strengthen their security posture. By addressing unauthorized access and lateral movement of both perimeter and internal threats, VMware vDefend supports the broader PCI DSS compliance initiative while providing a foundation for more advanced security frameworks.

Scope and approach for review

Coalfire began by examining the PCI DSS 4.0.1 requirements and identifying them as either organizational (non-technical) or technical. A requirement was determined as either organizational or technical based on a review of the requirement's narrative, testing procedures, and guidance.

Organizational requirements include documented policies, procedures, and standards that were not considered directly applicable to the technical solution. Examples of these non-technical requirements include maintaining facility visitor logs, verifying an individual's identity before granting physical or logical access, performing periodic physical asset inventories, and other elements that VMware vDefend could not satisfy.

Evaluation of PCI DSS controls and scoring system

Once identified, technical requirements were assessed to determine applicability to VMware vDefend for the PCI DSS use case. If the achievement of the required objectives was more likely to be met using an external and non-adjacent mechanism, the requirement was determined to be notional to VMware vDefend and excluded.

Where the requirement was determined as applicable, Coalfire assessed the capability of VMware vDefend to address the requirement. In keeping with the desire to present the information compactly, Coalfire used Harvey Balls (https://en.wikipedia.org/wiki/Harvey_Balls) to assign each applicable requirement a qualitative category of capability, including whether the solution had a fractional capacity to support a percentage of the controls.

The table below is a key for the scoring given to each requirement in the scoring tables below:

Symbol	Description	Definition
●	Full coverage	Fully supports or directly addresses the requirement
◑, ◕	Partial coverage	Supports some aspects of the requirement but not entirely
◔	Potential coverage	May indirectly support the performance of related activities

Table 2: Key for scoring PCI DSS support capabilities

VMware vDefend applicability to PCI DSS

This section details Coalfire's compliance findings for VMware vDefend, along with the corresponding customer requirements and responsibilities, as reviewed in Coalfire's analysis.

It is essential to understand that products and technologies do not themselves provide PCI compliance but can support and assist with a customer's compliance. Coalfire's review of VMware vDefend's applicability to PCI DSS is based on the solution's capacity to either provide compliance with the specific PCI DSS controls or support an entity's requirements in concert with other operational and technical means necessary to meet PCI DSS testing requirements.

In this overall scoring representation, notional controls that would be required and supplied by a system outside of VMware vDefend (and therefore be entirely the customer's responsibility) are omitted for clarity.

VMware vDefend findings

Requirement 1: Install and maintain NSCs

Requirement 1 focuses on installing and maintaining NSCs to safeguard the CDE, including firewalls, segmentation, and traffic restrictions. VMware vDefend's Distributed and Gateway Firewalls enable granular traffic control and network segmentation, supporting key sub-requirements for restricting inbound and outbound traffic to/from the CDE.

VMware vDefend provides robust support for network segmentation, traffic control, and protocol security under Requirement 1 but does not address policy documentation or procedural aspects of NSC management.

PCI Req.	PCI DSS Requirements	Platform Compliance Comments	Score
1.2	**NSCs are configured and maintained.**		
1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	VMware vDefend Distributed Firewall allows detailed configuration of rulesets. VMware vDefend allows entities to add annotations/comments within the product when creating rules. Entities using the product are independently responsible for the creation and management of the network security configuration standard, which is required to align with the established rulesets.	◕
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	VMware vDefend Distributed Firewall supports technical enforcement of rule changes. Entities using the product are independently responsible for the creation and management of change control procedures utilized during changes for network connections and configurations.	◕
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Security Intelligence for VMware vDefend provides visibility into network connections using the built in Security Intelligence tooling. Entities using the product are independently responsible for the documentation requiring that network diagrams and data flows are kept current. Security Intelligence does generate diagrams that gives visibility into network connections. Flow information is displayed, and events detected by Network Traffic Analysis are also represented on the diagram.	◕
1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.	VMware vDefend Distributed Firewall enforces granular control over allowed services, protocols, and ports.	●
1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Provides controls for securing and restricting the use of insecure protocols via VMware vDefend Distributed and Gateway Firewalls.	●
1.2.7	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Configuration review requires external processes; VMware vDefend supports validation but not full compliance.	◑
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	Security Intelligence for vDefend supports monitoring configuration changes of NSCs. vDefend DFW and GFW configuration files are encrypted, with access controlled via API/UI/CLI authenticated with RBAC support.	●
1.3	**Network access to and from the CDE is restricted.**		
1.3.1	Inbound traffic to the CDE is restricted to only traffic that is necessary. All other traffic is specifically denied.	Supported via Distributed and Gateway Firewalls with granular inbound traffic rules.	●

PCI Req.	PCI DSS Requirements	Platform Compliance Comments	Score
1.3.2	Outbound traffic from the CDE is restricted to only traffic that is necessary. All other traffic is specifically denied.	Supported by Distributed Firewall's outbound traffic controls.	●
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	Wireless networks are not explicitly addressed; segmentation controls could indirectly support.	◔
1.4	**Network connections between trusted and untrusted networks are controlled.**		
1.4.1	NSCs are implemented between trusted and untrusted networks.	Supported via segmentation capabilities in the Distributed Firewall.	●
1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. All other traffic is denied.	Supported via Gateway Firewall with stateful traffic inspection.	●
1.4.3	Anti-spoofing measures are implemented to detect and block forged source Internet Protocol (IP) addresses from entering the trusted network.	Anti-spoofing is supported by Distributed Firewall configurations.	●
1.4.4	System components that store CHD are not directly accessible from untrusted networks.	Micro-segmentation isolates CHD systems from untrusted access.	●
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	VMware vDefend supports the disclosure of internal IP addresses and routing information only to authorized personnel by restricting access to the material. Access is limited to only administrative staff with access to vCenter, NSX policies, IP's for VMs, and routing information. Entities using the product are independently responsible for the organization policy and procedural documentation that requires the disclosure of internal IP addresses and routing information only to authorized parties.	◕
1.5	**Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.**		

PCI Req.	PCI DSS Requirements	Platform Compliance Comments	Score
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Supports securing network connections between untrusted devices and the CDE through Distributed Firewall and segmentation. vDefend Firewall supports AD-integrated identity firewall for user-level controlled access to applications. Furthermore, the Gateway Firewall as well as Bare Metal firewall can be used to secure non-VM assets (i.e. endpoint devices).	◕

Table 3: VMware vDefend PCI DSS 4.0.1 Requirement 1 scoring

Requirement 2: Apply secure configurations to all system components

Requirement 2 focuses on applying secure configurations to all system components, including hardening standards, disabling unnecessary functionality, and managing insecure protocols. VMware vDefend's Distributed Firewall allows the application of secure configurations by enabling the restriction of unnecessary services, protocols, and ports. VMware vDefend facilitates the logical isolation of system components, supporting secure configurations for environments with differing security levels.

VMware vDefend supports secure network configurations and segmentation under Requirement 2 but does not address system-level hardening, account management, or encryption requirements beyond its own interface.

PCI Req.	PCI DSS Requirements and Platform	Platform Compliance Comments	Score
2.2	**System components are configured and managed securely.**		
2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	Security Intelligence for vDefend aids an organization in validating network configurations. Entities using the product are independently responsible for documenting their organization's policy, procedure, and configuration standards that align with technical security controls provided by Security Intelligence for vDefend product.	◕

PCI Req.	PCI DSS Requirements and Platform	Platform Compliance Comments	Score
2.2.3	Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component. *OR* • Primary functions with differing security levels that exist on the same system component are isolated from each other. *OR* • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	Micro-segmentation supports isolating functions with different security levels.	●
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Supported by Distributed Firewall for restricting services and protocols.	●
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Security features in Distributed Firewall mitigate risks of insecure protocols.	●
2.2.6	System security parameters are configured to prevent misuse.	Supported through network security controls and secure configurations.	●
2.2.7	All non-console administrative access is encrypted using strong cryptography.	VMware vDefend supports encrypted administrative access to its own interface via Hypertext Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) 1.2+.	●

Table 4: VMware vDefend PCI DSS 4.0.1 Requirement 2 scoring

Requirement 3: Protect stored account data

Requirement 3 and its sub-requirements focus on the storage, protection, and management of CHD and cryptographic keys, which are beyond the scope of VMware vDefend's functionality. While VMware vDefend indirectly supports Requirement 3 by securing environments in which CHD is processed or stored, it does not directly fulfill any of the technical controls specified in this requirement.

Requirement 4: Protect CHD with strong cryptography during transmission over open, public networks

Requirement 4 focuses on securing CHD in transit using cryptography, a function performed by the VMware vDefend Gateway Firewall. The VMware vDefend Gateway Firewall supports an organization’s unified approach to protecting cardholder data while transmitted across open, and public networks.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
4.2	**PAN is protected with strong cryptography during transmission.**		
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This is a best practice until 31 March 2025. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	The VMware vDefend Gateway Firewall supports IPSEC VPN tunneling in order to encrypt transmissions of sensitive data across a secure tunnel. Entities using the product are independently responsible for documenting their organization's policy and procedure documentation that align with technical security controls provided by the Security Intelligence for vDefend product.	◕

Requirement 5: Protect all systems and networks from malicious software

Requirement 5 focuses on protecting systems and networks from malware through the deployment, maintenance, and monitoring of anti-malware solutions. VMware vDefend's ATP includes anti-malware capabilities for detecting and blocking malicious files and behavioral threats in network traffic. ATP performs real-time scans and behavioral analysis, aligning with the requirement for active malware protection.

VMware vDefend partially supports Requirement 5 through its ATP features for network-level malware detection and prevention but does not address endpoint protection or operational processes for malware management.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
5.2	**Malicious software (malware) is prevented, detected, and addressed.**		
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	vDefend supports malware detection and prevention at the Distributed Firewall, and detection at the Gateway, to limit malware inbound to an organization. Entities using the product are independently responsible for documenting their organization's policy, procedure, and configuration standards that align with technical security controls provided by Security Intelligence for vDefend.	◕
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	Both Signature and Behavioral-based detection techniques are used to detect and prevent previously seen or unseen malware.	●
5.3	**Anti-malware mechanisms and processes are active, maintained, and monitored.**		

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	Supported through the Malware Prevention feature of ATP.	●
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans. *OR* • Performs continuous behavioral analysis of systems or processes.	vDefend supports malware detection and prevention at the Distributed Firewall, and detection at the Gateway to limit malware inbound to an organization. Products support continuously detecting and intercepting malware files destined for endpoints. Entities using the product are independently responsible for documenting their organization's policy, procedure, and configuration standards that align with technical security controls provided by Security Intelligence for vDefend.	◕
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	VMware vDefend logs anti-malware activities through both the Distributed and Gateway malware protection components. vDefend customers are entitled to VMware's integrated solution, Aria Operations for Logs, in order to meet and exceed retention requirements for anti-malware logs.	●
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Supported through secure configuration controls in Malware Prevention.	●

Table 5: VMware vDefend PCI DSS 4.0.1 Requirement 5 scoring

Requirement 6: Develop and maintain secure systems and software

Requirement 6 focuses on developing and maintaining secure systems and software, including vulnerability management, secure coding practices, patch management, and protection for public-facing web applications. VMware vDefend does not facilitate the development or maintenance of bespoke or third-party software, nor is it utilized to implement secure coding practices. While VMware vDefend can detect network vulnerabilities and provide segmentation for security, it does not manage software patches or apply fixes to identified vulnerabilities.

Software development and patching processes are outside the scope of VMware vDefend's network-focused capabilities. Only vulnerability detection and segmentation features align indirectly with a few PCI DSS sub-requirements.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
6.3	**Security vulnerabilities are identified and addressed.**		

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke, custom, and third-party software (for example, operating systems and databases) are covered.	IDS/IPS can detect and block known vulnerabilities that align with CVE identifiers. All threat detections are ranked/scored, and where applicable, a CVSS scoring is assigned within the product, as well as, Mitre Attack T/T. Entities using the product are independently responsible for documenting their organization's policy, procedure, and configuration standards that align with technical security controls provided by Security Intelligence for vDefend.	◕
6.4	**Public-facing web applications are protected against attacks.**		

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis, and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: - At least once every 12 months and after significant changes. - By an entity that specializes in application security. - Including, at a minimum, all common software attacks in Requirement 6.2.4. - Ranking all vulnerabilities in accordance with requirement 6.3.1. - Correcting all vulnerabilities. - Re-evaluating the application after the corrections. *OR* • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: - Is installed in front of public-facing web applications to detect and prevent web-based attacks. - Is actively running and up to date as applicable. - Is generating audit logs. - Is configured to either block web-based attacks or generate an alert that is immediately investigated.	vDefend's Avi WAF, in conjunction with, the VMware vDefend's core offering with the Gateway and Distributed IDS/IPS provide protection against exploits and known web application vulnerabilities.	◕

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Is actively running and up to date as applicable. • Is generating audit logs. • Is configured to either block web-based attacks or generate an alert that is immediately investigated.	VMware Avi WAF supports this requirement if deployed. It is available as part of VMware Avi Load Balancer and is a complementary technology to VMware vDefend.	◔
6.5	**Changes to all system components are managed securely.**		
6.5.3	Pre-production environments are separated from production environments, and the separation is enforced with access controls.	Supports separation of pre-production and production environments with micro-segmentation and automated policy enforcement. Isolation is accomplished through vDefend's Distributed Firewalls.	◕

Table 6: VMware vDefend PCI DSS 4.0.1 Requirement 6 scoring

Requirement 7: Restrict access to system components and CHD by business need to know

Requirement 7 focuses on user access control, which is beyond VMware vDefend's network security scope. VMware vDefend does not manage user roles, privileges, or access control models required to enforce least privilege principles for CHD.

VMware vDefend's involvement is limited to enabling network segmentation for broader access control strategies.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
7.2	**Access to system components and data is appropriately defined and assigned.**		
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	VMware vDefend supports segmented access controlled via API/UI/CLI authenticated with RBAC support. Entities using the product are independently responsible for documenting their organization's policy, procedure, and standards that align with technical security controls provided by Security Intelligence for vDefend.	◕

Table 7: VMware vDefend PCI DSS 4.0.1 Requirement 7 scoring

Requirement 8: Identify users and authenticate access to system components

Requirement 8 pertains to user identity, access control, and authentication, which are supported through VMware Identity Firewall (IDFW) capabilities.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
8.2	**User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.**		
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	VMware's Identity Firewall (IDFW) supports an organization's efforts for ensuring that all access to components in the card environment is restricted to unique personnel. IDFW (Identity based access to applications/data) is available for both VDI/RDSH VMs (through Guest-Introspection on Distributed Firewall) as well as Physical machines (through Log Scraping on GFW/DFW). Products also enable an organization to check with multiple users within the same compute VM, workloads with terminal services, as well as detect the escalation of privileges by the user.	●

Requirement 9: Restrict physical access to CHD

Requirement 9 addresses physical security controls to restrict access to CHD. It includes measures for secure facilities, physical access management, and the handling of media containing CHD. VMware vDefend does not manage physical access to systems, facilities, or CHD storage media.

Requirement 10: Regularly monitor and test networks

Requirement 10 focuses on logging and monitoring, ensuring that access to CHD and system components is recorded, retained, and reviewed to detect and respond to suspicious activities. VMware vDefend relies on integration with external log management tools (e.g., VMware Log Insight or SIEM systems) for centralized logging and retention. VMware vDefend does not directly log user access to CHD or system components; its logging is specific to network events and security alerts. VMware vDefend does not provide file integrity monitoring or tamper detection for audit logs.

Logging and retention of user activity and audit logs are outside VMware vDefend's core functionality. VMware vDefend supports logging network-related events but relies on external tools for full compliance.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
10.3	**Audit logs are protected from destruction and unauthorized modifications.**		
10.3.1	Read access to audit log files is limited to those with a job-related need.	vDefend Firewall can effectively restrict access to logs through its segmentation policies.	●
10.3.2	Audit log files are protected to prevent modifications by individuals.	vDefend Firewall and Security Intelligence can help in monitoring access to 3rd party logs. Access to generated logs Read-Only and are controlled by RBAC policies.	◕

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	With the product, there are two applicable logs to support an organization's logging processes. Security Services Platform Audit Log (audit_log.log). There is no preset retention time for the audit logs, however, there is a 30mb file size limit. Once the product reaches 30mb, the log gets rotated; the product can store a max of 10 files. Audit logs can then be forwarded to an external syslog server for longer-term retention. NSX Audit Log (nsx-audit.log). There is no preset retention time for the audit logs. Log retention is based on log rotation, currently 1mb rotated at most 10 times. Audit logs can be forwarded to an external syslog server for longer-term retention.	◑
10.5	**Audit log history is retained and available for analysis.**		
10.5.1	Retain audit log history for at least 12 months, with at least the most recent 3 months immediately available for analysis.	With the product, there are two applicable logs to support an organization's logging processes. Security Services Platform Audit Log (audit_log.log). There is no preset retention time for the audit logs, however, there is a 30mb file size limit. Once the product reaches 30mb, the log gets rotated; the product can store a max of 10 files. Audit logs can then be forwarded to an external syslog server for longer-term retention. NSX Audit Log (nsx-audit.log). There is no preset retention time for the audit logs. Log retention is based on log rotation, currently 1mb rotated at most 10 times. Audit logs can be forwarded to an external syslog server for longer-term retention.	◑

Table 8: VMware vDefend PCI DSS 4.0.1 Requirement 10 scoring

Requirement 11: Test security of systems and networks regularly

Requirement 11 focuses on regularly testing security systems and processes, including vulnerability scans, penetration testing, and detection of unauthorized changes or wireless access points. VMware vDefend does not perform vulnerability scans, penetration tests, or compliance validation; these require separate tools or services. VMware vDefend does not manage or monitor wireless access points. While VMware vDefend supports intrusion detection and prevention (e.g., IDS/IPS), it does not provide file integrity monitoring or change detection for critical files.

VMware vDefend's alignment with Requirement 11 is limited to intrusion detection, vulnerability monitoring, and segmentation validation capabilities.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
11.3	**External and internal vulnerabilities are regularly identified, prioritized, and addressed.**		
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	ATP enables internal vulnerability detection on hosts and traffic flows. All threat detections are ranked/scored, and where applicable, a CVSS scoring is assigned within the product, as well as, Mitre Attack T/T.	●
11.4	**External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.**		
11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • A documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.	VMware vDefend facilitates segmentation validation but does not support methodology definition.	◑

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
11.4.2	Internal penetration testing is performed: • Per the entity's defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party. Organizational independence of the tester exists (not required to be a QSA or ASV).	Segmentation capabilities support testing but not test execution.	◑
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	vDefend Distributed Firewall supports a micro-segmentation strategy that enforces least privilege access and helps achieve zero-trust network security by isolating workloads and restricting traffic flow.	●

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
11.4.6	*Additional requirement for service providers only*: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	vDefend Distributed Firewall supports a micro-segmentation strategy that enforces least privilege access and helps achieve zero-trust network security by isolating workloads and restricting traffic flow.	●
11.5	**Network intrusions and unexpected file changes are detected and responded to.**		
11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	IDS/IPS uses application-aware traffic inspection to monitor internal and external network boundaries. It detects and prevents threats using signature-based detection, protocol decoders, and anomaly detection, with alerting capabilities for suspected compromises. IDS/IPS provides real-time monitoring and alerting for CDE perimeters and critical points.	●
11.5.1.1	*Additional requirement for service providers only*: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	IDS/IPS and Malware Prevention support detection of various types of covert channels used for communication and exfiltration of information. Entities using the product are independently responsible for documenting their organization's policy, procedure, and standards that align with technical security controls provided by VMware vDefend's Security Intelligence product.	◕

Table 9: VMware vDefend PCI DSS 4.0.1 Requirement 11 scoring

Requirement 12: Support information security with organizational policies and programs

Requirement 12 focuses on establishing and maintaining a comprehensive information security policy, including risk management, security awareness, and vendor management. VMware vDefend does not establish, publish, or manage information security policies or risk management programs. VMware vDefend does not assist with third-party service provider compliance or contractual obligations. While VMware vDefend provides alerting capabilities (e.g., IDS/IPS), it does not include a predefined incident response plan.

Organizational-level policies and procedures are beyond the scope of VMware vDefend's technical network security capabilities. VMware vDefend's alignment with Requirement 12 is limited to supporting customer-defined incident response and alerting processes, telemetry supporting risk assessment, and housekeeping capabilities facilitating asset management.

PCI Req	PCI DSS Requirements	Platform Compliance Comments	Score
12.3	**Risks to the CDE are formally identified, evaluated, and managed.**		
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • An analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	Supports tagging assets for identification and generates reporting and analytics for visibility and security policy refinement. VMware vDefend's Security Segmentation report allows organizations to setup their risk profile to support the organization's PCI risk assessment.	◑

Table 10: VMware vDefend PCI DSS 4.0.1 Requirement 12 scoring

Customer responsibilities for PCI DSS use of VMware vDefend

To minimize the impact on compliance initiatives and maintain the security posture of the in-scope environment, customers must address specific responsibilities and considerations when integrating VMware vDefend into their PCI DSS program. The following guidance highlights key areas of focus.

Shared responsibility model

Customers must recognize that VMware vDefend operates within a shared responsibility framework. While VMware vDefend provides technical capabilities (e.g., firewalls, IDS/IPS, segmentation), customers retain ultimate responsibility for implementing, configuring, and monitoring controls to meet PCI DSS requirements.

Configuration and management

Customers must define and maintain firewall rules, segmentation policies, and access controls to align with their PCI DSS scope. This includes isolating the CDE and implementing least privilege principles. Customers must ensure only required services, protocols, and ports are enabled, and insecure ones are restricted or mitigated. Firewall and segmentation configurations must be reviewed to confirm they remain effective.

Logging and monitoring

Customers are responsible for integrating VMware vDefend-generated logs with a centralized logging solution (e.g., VMware Log Insight, SIEM tools) to meet logging and retention requirements. Customers must ensure that logs are retained for at least 12 months, with the most recent 3 months readily available for analysis. Access to logs and configuration settings must be limited to personnel with a job-related need, ensuring compliance with logging access controls.

Vulnerability and risk management

While VMware vDefend's ATP can detect vulnerabilities, customers must correlate identified risks with CVSS scoring systems and prioritize remediation efforts. VMware vDefend does not manage system patching; customers must ensure all system components are patched according to PCI DSS timelines. Customers must perform targeted risk analyses for configurations and identified vulnerabilities to justify their frequency of review and remediation actions.

Incident response

Customers are responsible for configuring and responding to all alerts provided by VMware vDefend. This includes incorporating these alerts into an incident response plan to address potential security events. Customers must maintain records of incidents, actions taken, and resolution to support ongoing compliance and audits.

Policy and procedure alignment

Customers must update security policies, diagrams, and procedures to reflect the integration of VMware vDefend into the environment, ensuring alignment with PCI DSS documentation requirements. They must train relevant staff in using and managing VMware vDefend in the context of PCI DSS requirements.

Scope validation

Customers must perform a review of the CDE and segmentation boundaries post-implementation of VMware vDefend to ensure that its integration does not inadvertently alter scope or introduce new risks. They must ensure segmentation controls that are implemented using VMware vDefend are validated through annual penetration testing.

Conclusion and Coalfire opinion

VMware vDefend is a network security and threat prevention solution designed to enhance workload protection, enable segmentation, and mitigate risks through features such as IDS/IPS, ATP, and distributed firewall capabilities. Coalfire reviewed VMware vDefend for its efficacy in assisting payment card entities with PCI DSS 4.0.1 compliance and provides the following opinion for its use with a compliance program:

Coalfire concludes that VMware vDefend is effective in providing support for PCI DSS payment entities' objectives and requirements. VMware vDefend's capabilities for micro-segmentation, intrusion detection and prevention, protocol and port control, and network traffic analysis render it a suitable solution for addressing network security controls, intrusion detection, and vulnerability identification requirements for PCI DSS.

This opinion applies to payment entities, including merchants and service providers, based on the observed PCI DSS controls supported by VMware vDefend and its shared responsibility model. While VMware vDefend provides technical capabilities for securing and monitoring in-scope environments, customers must take ownership of configurations, policy management, and supplementary controls required for full compliance.

VMware vDefend should be implemented in alignment with an organization's mission, values, policies, procedures, business objectives, and its general approach to security and security planning as defined by its Governance, Risk Management, and Compliance (GRC) program. This opinion is dependent on many underlying presumptions (i.e., caveats), which are expectations of a complete risk management program and are summarized here:

- Selection of a supporting risk management framework.
- Creation and adoption of risk management policies and supporting procedures underlying the PCI DSS requirements.
- Adherence to VMware best practices for VMware vDefend and other supporting vendors used in an actual deployment.
- Implementation of organizational controls supporting the roles, responsibilities, policies, procedures, baselines, and mandates, as applicable.
- Use of physical controls to manage and secure access to the facilities and monitor visitor and staff access, provide surveillance, and other supporting activities.
- Use of security response team staff, training, and supporting technology to perform ongoing cybersecurity vigilance.
- Presence of required risk management teams and associated information technology staff to support the cybersecurity program, workloads, and business operations.

A comment regarding regulatory compliance

Coalfire disclaims the generic suitability of any technology or service to establish regulatory compliance. Payment entities and other user organizations attain compliance through implementation and maintenance of a GRC program, not via the use of a specific technology or service. This is true for all entities subject to PCI DSS and user organizations targeting compliance with other standards, regulations, or mandates.

Additional information, resources, and references

This section contains a description of the links, standards, guidelines, and reports used for the materials used to identify and discuss the features, enhancements, and security capabilities of VMware vDefend.

Broadcom resources

- Architecture and capabilities of the VMware vDefend suite, focusing on its integration with Security Intelligence for secure private cloud environments.

https://www.vmware.com/docs/vmware-secure-private-cloud-with-vmware-VMware vDefend

- Features of the Distributed and Gateway Firewalls, including micro-segmentation and automated policy enforcement for network security.

https://www.vmware.com/docs/vmw-VMware vDefend-firewall-1

- Advanced threat detection capabilities, including IDS/IPS, Malware Prevention, and anomaly detection for traffic flows.

https://www.vmware.com/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall

- Security Intelligence's features for monitoring, visibility, and analytics that support segmentation, tagging, and compliance reporting.

https://www.vmware.com/docs/vmware-nsx-intelligence-solution-brief

- Insights into the network traffic analysis tools within Security Intelligence, emphasizing application-aware traffic inspection and protocol decoders.

https://www.vmware.com/docs/vmware-nsx-network-traffic-analysis

- IDS/IPS features for detecting and mitigating threats at the network perimeter and internal boundaries.

https://www.vmware.com/docs/vmware-nsx-distributed-ids-ips-solution-overview

- Advanced sandboxing capabilities for analyzing and preventing malware and other threats.

https://www.vmware.com/docs/vmw-nsx-sandbox-solution

PCI DSS and PCI SSC references

- The version of the PCI DSS referenced in this document is 4.0.1, which may be accessed via the following link:

https://www.pcisecuritystandards.org/document_library

- An information supplement from the PCI SSC is the guidance for PCI DSS Scoping and Network Segmentation. The guidance document may be found at the following link:

https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf

- PCI DSS scoping and segmentation practices and their applicability to modern network architectures.

https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/PCI-DSS-Scoping-and-Segmentation-Guidance-for-Modern-Network-Architectures.pdf

- Details of the PCI SSC Cloud Special Interest Group updates to virtualization and cloud Information Supplement, developed as PCI SSC Cloud Computing Guidelines, April 2018, are available at the following link:

https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

Coalfire resources

- Coalfire corporate information is available at the following link:

https://www.coalfire.com/about

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the author

Jason Wikenczy | *Principal, Payments Advisory & Product Guidance*

Leveraging his experience in financial audit, cloud security, and business information technology, Jason employs a security-centric approach to assurance and compliance initiatives across a diverse set of industries. From government and energy to healthcare, insurance, and retail, Jason has an established record of helping clients achieve their business objectives while upholding strong security standards.

About Coalfire

The world’s leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.