Trend Micro, Inc.

# Trend Vision One Applicability Guide for PCI DSS v4.0 Standard

July 4, 2024

Table of Contents

Dear Security Executive,

We have completed an analysis of the capabilities of the Trend Vision One platform related to applicability to the Payment Card Industry (PCI) Data Security Standard (DSS) v4.0 for Trend Micro, Inc. Please note that the applicability guide does not apply to other Trend Micro products or services.

The Trend Vision One platform is a full-featured cybersecurity management platform for devices, workloads, and cloud infrastructure. Key features and functionality of the platform support many of the security requirements of the PCI DSS v4.0 standard applicable to companies that store, process, or transmit credit card data. In particular, the platform supports technical requirements related to device, network, and endpoint security. Some or all of Requirements 1, 2, 5, 6, 7, 8, 9, 10, 11, and 12 can be supported by implementation and best practice operation of Trend Vision One. Applicability to specific subpoint requirements is detailed in Table 1 of this document.

Respectfully submitted,

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA

PCI Security Standards enhance payment security with mature, comprehensive security control requirements, assessment procedures, and supporting materials. The standards define security controls and processes for entities involved in the payment ecosystem, as well as requirements for developers and solution providers to build and securely manage payment devices, software, and solutions for the payment industry.

While there are several standards under the Payment Card Industry Security Standards Council (SSC) umbrella, this applicability guide focuses on the Data Security Standard, which is an actionable framework for developing robust payment account data security processes, including prevention, detection, and appropriate reaction to security incidents. The DSS is intended to be implemented by organizations that store, process, or transmit credit card data or who provide services to entities that store, process, or transmit such data.

PCI DSS was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

| Goals | PCI DSS Requirements |
|---|---|
| Build and Maintain a Secure Network and Systems | 1. Install and maintain network security controls<br>2. Apply secure configurations to all system components |
| Protect Account Data | 3. Protect stored account data<br>4. Protect cardholder data with strong cryptography during transmission over open, public networks |
| Maintain a Vulnerability Management Program | 5. Protect all systems and networks from malicious software<br>6. Develop and maintain secure systems and software |
| Implement Strong Access Control Measures | 7. Restrict access to system components and cardholder data by business need to know<br>8. Identify users and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Log and monitor all access to system components and cardholder data<br>11. Test security of systems and networks regularly |
| Maintain an Information Security Policy | 12. Support information security with organizational policies and programs |

PCI DSS requirements apply to:

The cardholder data environment (CDE), which is comprised of:

- System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and,
- System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

AND

- System components, people, and processes that could impact the security of the CDE.

“System components” include network devices, servers, computing devices, virtual components, cloud components, and software. See PCI DSS “Scope of PCI DSS Requirements” section for examples of “system components.”

### Annual PCI DSS Scope Confirmation

The first step in preparing for a PCI DSS assessment is for the assessed entity to accurately determine the scope of the review. The assessed entity must confirm the accuracy of their PCI DSS scope according to PCI DSS Requirement 12.5.2 by identifying all locations and flows of account data, and identifying all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers, remote access servers, logging servers) to ensure they are included in the PCI DSS scope. All systems and locations should be considered during the scoping process, including backup/recovery sites and fail-over systems.

Trend Vision One can support this process by identifying assets in both Cloud-based and data center-located infrastructure. System inventories created and automatically maintained by Trend Vision One will inform Information Security, IT, and business personnel responsible for PCI compliance during the scope identification and validation activity.

### Summary of Changes for PCI DSS 4.0

Numerous changes were implemented in the latest release of the DSS – version 4. These include:

- The new Customized Approach Objective and accompanying method of meeting most requirements.
- 64 net-new requirements, most with a sunrise of March 31, 2025.
- Clarifying enhancements on most requirements to drive effective mitigation of risks to cardholder data.

Of special note: Several of the net-new requirements are met directly by Trend Vision One product features, as documented in Table 1 below. Overall, Trend Vision One can help with 10 of 12 of the areas defined and required by PCI DSS version 4, as illustrated below.

More information on Trend Vision One can be found on the Trend Micro web site at https://www.trendmicro.com/en_us/business/products/one-platform.html

## Table 1: Applicability Detail for PCI DSS v4.0

Trend Vision One Applicability by Requirement Number

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 1.2.1 | Configuration standards for NSC rulesets are:<br>• Defined<br>• Implemented<br>• Maintained | **Yes.** Trend Vision One ASRM (Attack Surface Risk Management) cloud Knowledge Base supports definition of configuration standards for NSCs across a collection of frameworks and industry best practices.<br>NSC rulesets can be implemented at the resource level (Endpoint Security, Container Security) and network level (Network Security).<br>Trend Vision One provides policy and configuration benchmarking against NSC rulesets to help ensure implementation is in accordance with defined standards.<br>Customers are responsible for defining configuration standards for all in-scope resources. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 1.2.2 | All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process. | **Yes.** Changes to network connections and NSC configurations can be detected at the resource level (Endpoint Security, Container Security) and network level (Network Security).<br>Trend Vision One can be integrated with major ticketing and workflow systems which support tracking, auditability, and implementation of change control processes.<br>Customers are responsible for defining, implementing, and maintaining change control processes, including necessary workflows and approvals and formalized policies and procedures. |
| 1.2.5 | All services, protocols, and ports allowed are identified, approved, and have a defined business need. | **Yes.** Endpoint Security allows for granular configuration for communication based on source/destination IP, protocols, mac address and ports, for the resources in use at the workload and endpoint level |
| 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. | **Yes.** Resource level (Endpoint Security, Container Security) and network level (Network Security) are applicable. ASRM also monitors security group ports, open port ranges, unrestricted security groups, and alerts to security group changes with overly permissive access.<br>Customers are responsible for determining the minimal services, protocols, and ports required for in-scope environments to function, identifying those deemed insecure, taking measures to mitigate introduced risk, and documenting the business justification, approval, and security features implemented. |
| 1.2.7 | Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective. | **Yes.** Services, protocols, and ports in use can be identified at the resource level (Endpoint Security, , Container Security) and network level (Network Security).<br>Trend Vision One provides capabilities for customers to innovate automation in support of this requirement. For example, consider active reporting and alerting on:<br>• Changes to the configuration of NSCs protecting trusted networks.<br>• Unutilized NSCs<br>• NSCs with marginal or decreased use over time<br>• NSCs without required tags indicating review and approval.<br>Customers are responsible for defining and documenting processes, policies, and procedures for NSC review. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | Customers are responsible for using platform capabilities to review and evaluate NSCs for relevancy and effectiveness across all in-scope system components. |
| 1.2.8 | Configuration files for NSCs are:<br>• Secured from unauthorized access<br>• Kept consistent with active network configurations | **Yes.** Trend Vision One supports policy monitoring and enforcement on constructs capable of defining or modifying NSCs during build, at deployment, and runtime.<br>Capabilities including admission control, compliance monitoring, and integrity monitoring help enforce consistency with intended NSC configurations and secure constructs (configuration files) against unauthorized changes.<br>Customers are responsible for defining and implementing NSCs, associated access requirements, and keeping sources of configuration information current. |
| 1.3 | Network access to and from the cardholder data environment is restricted. | **Yes.** Trend Vision One includes host-based network security (NSC) capabilities in the TippingPoint, and Endpoint Security Products (typical hosted firewall and hosted IDS/IPS capabilities).<br>Trend Vision One also includes ZTNA SWG and TippingPoint which serves as Security Web Gateway and Network IPS. TippingPoint uses Trend Vision One Network Intrusion Prevention to manage the filter. |
| 1.3.1 | Inbound traffic to the CDE is restricted as follows:<br>•To only traffic that is necessary.<br>•All other traffic is specifically denied | **Yes.** Trend Vision One includes host-based network security (NSC) capabilities in the Endpoint Security platform components (typical hosted firewall and hosted IDS/IPS capabilities).<br>Trend Vision One also includes ZTNA Secure Web Gateway and TippingPoint which serves as Secure Web Gateway and Network IPS. TippingPoint uses Trend Vision One Network Intrusion Prevention to manage the filter.<br>Trend Vision One provide capabilities for customization and implementation of NSCs to identify publicly accessible resources, enforce stateful communications, and deny traffic not specifically allowed, via multiple platform components:<br>• Endpoint Security<br>• Container Security<br>• Network Security<br>For AWS environments, integration with AWS Network Firewall supplements support for this requirement. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | Customers are responsible for the design and implementation of environment architecture and the implementation of NSCs in accordance with PCI DSS 4.0 requirements. |
| 1.3.2 | Outbound traffic from the CDE is restricted as follows:<br>• To only traffic that is necessary<br>• All other traffic is specifically denied | **Yes.** Trend Vision One includes host-based network security (NSC) capabilities in the Endpoint Security platform components (typical firewall capabilities). Trend Vision One also includes ZTNA Secure Web Gateway and TippingPoint which serves as Secure Web Gateway and IPS. TippingPoint uses Trend Vision One Network Intrusion Prevention to manage the filter.<br>Trend Vision One provides capabilities for customization and implementation of NSCs to identify publicly accessible resources, enforce stateful communications, and deny traffic not specifically allowed, via multiple platform components:<br>• Endpoint Security<br>• Container Security<br>• Network Security<br>For AWS environments, integration with AWS Network Firewall supplements support for this requirement.<br>Customers are responsible for the design and implementation of environment architecture and the implementation of NSCs in accordance with PCI DSS 4.0 requirements. |
| 1.3.3 | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:<br>• All wireless traffic from wireless networks into the CDE is denied by default.<br>• Only wireless traffic with an authorized business purpose is allowed into the CDE. | |
| 1.4.1 | NSCs are implemented between trusted and untrusted networks. | |
| 1.4.2 | Inbound traffic from untrusted networks to trusted networks is restricted to:<br>• Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.<br>• Stateful responses to communications initiated by system components in a trusted network.<br>All other traffic is denied. | |
| 1.4.3 | Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. | **Yes.** Endpoint platform components provide network security features for host-based firewall security controls.<br>Trend Vision One provides capabilities to customize, implement, and manage network- and host-based security controls supporting this requirement. Supporting platform modules and components include:<br>• Endpoint Security<br>• Container Security<br>• Network Security<br>Customers are responsible for scope validation and the identification of system components applicable to this requirement. Customers are also responsible for ensuring |
| 1.4.4 | System components that store cardholder data are not directly accessible from untrusted networks. | |
| 1.5 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. | |
| 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 | |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | Internet) and the CDE as follows:<br>• Specific configuration settings are defined to prevent threats being introduced into the entity’s network<br>• Security controls are actively running<br>• 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 | security controls are implemented on in-scope, applicable system components. |
| 2.1 | Processes and mechanisms for applying secure configurations to all system components are defined and understood. | No |
| 2.2 | System components are configured and managed securely. | **Yes.** Trend Vision One ASRM cloud capabilities provides reports to compare Google Cloud, Azure and AWS configurations against CIS benchmarks and other industry standards.<br>Endpoint Security Device Control provides features to control use of attached peripherals with high flexibility (e.g., whitelisting of specific device types and device manufacturers).<br>Additionally, Trend Vision One provides reporting and alerting on key security vulnerabilities like unexpected use or enablement of network services and ports, lack of disk encryption, and other common security configurations across supported products, cloud services, and devices. |
| 2.2.1 | Configuration standards are developed, implemented, and maintained to:<br>• Cover all system components<br>• Address all known security vulnerabilities<br>• Be consistent with industry-accepted system hardening standards or vendor hardening recommendations<br>• Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1<br>• 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 | **Yes.** Trend Vision One provides capabilities for customers to automate the implementation of configuration standards on new systems, in addition to supporting manual methods traditionally utilized to meet this requirement.<br>Scanning for misconfigurations and vulnerabilities can be performed in the CI/CD pipeline, prior to deployment, or manually upon release.<br>ASRM performs configuration benchmarking against standards, frameworks, and industry best-practices. The ASRM Cloud Knowledge Base supports the creation of configuration standards.<br>Periodic and ongoing vulnerability detection is performed across multiple platform modules and components including Container Security. For AWS environments, platform integration with Amazon Inspector supplements vulnerability detection capabilities. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | Inventory capabilities of Trend Vision One including identification of new resources in covered environments. This helps ensure coverage of system components and provides the ability to automate tasks to ensure new systems are configured appropriately.<br>Customers are responsible for:<br>• Defining and implementing configuration standards for all in -scope system components<br>• Updating configurations standards as new vulnerabilities are identified<br>• Ensuring configuration standards are applied to new system components before or immediately after deployment |
| 2.2.4 | Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. | **Yes.** Trend Vision One provides details of services, protocols, daemons, and functions in use, and capabilities for customers to evaluate and manage these elements. Supporting platform modules and components include:<br>• Endpoint Security<br>• Application Control<br>• Container Security<br>• Network Security<br>This information is also useful in identifying the existence of insecure services, protocols, or daemons. The Integrity Monitoring module helps prevent changes to intended implementation.<br>Customers are responsible for determining and implementing the minimal services, protocols, daemons, and functions required and for documenting the business justification for each in use.<br>Customers are also responsible for identifying services, protocols, daemons, and functions deemed insecure, taking measures to evaluate and mitigate introduced risk, and documenting the business justification and security features implemented. |
| 2.2.5 | If any insecure services, protocols, or daemons are present:<br>• Business justification is documented<br>• Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons | **Yes.** Trend Vision One provides details of services, protocols, daemons, and functions in use, and capabilities for customers to evaluate and manage these elements. Supporting platform modules and components include: |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | • Endpoint Security<br>• Application Control<br>• Container Security<br>• Network Security<br>This information is also useful in identifying the existence of insecure services, protocols, or daemons. The Integrity Monitoring module helps prevent changes to intended implementation.<br>Trend Vision One provides capabilities for customers to automate the implementation of configuration standards on new systems, in addition to supporting manual methods traditionally utilized to meet this requirement.<br>Scanning for misconfigurations and vulnerabilities can be performed in the CI/CD pipeline, prior to deployment, or manually upon release.<br>ASRM for Cloud performs configuration benchmarking against standards, frameworks, and industry best practices. The ASRM for Cloud Knowledge Base supports the creation of configuration standards.<br>Periodic and ongoing vulnerability detection is performed across multiple platform modules and components including Container Security and ASRM.<br>For AWS environments, platform integration with Amazon Inspector supplements vulnerability detection capabilities.<br>Inventory capabilities of Trend Vision One include identification of new resources in covered environments. This helps ensure coverage of system components and provides the ability to automate tasks to ensure new systems are configured appropriately.<br>Customers are responsible for  determining and implementing the minimal services, protocols, daemons, and functions required and for documenting  the business justification for each in use.<br>Customers are also responsible for identifying services, protocols, daemons, and functions deemed insecure, taking measures to evaluate and mitigate introduced risk, and documenting the business justification and security features implemented.<br>Customers are responsible for defining and implementing configuration standards for all in-scope system components, including system-specific security parameters. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 2.2.6 | System security parameters are configured to prevent misuse. | **Yes.** Trend Vision One provides capabilities for customers to automate the implementation of configuration standards on new systems, in addition to supporting manual methods traditionally utilized to meet this requirement.<br>Scanning for misconfigurations and vulnerabilities can be performed in the CI/CD pipeline, prior to deployment, or manually upon release.<br>ASRM performs configuration benchmarking against standards, frameworks, and industry best practices. The ASRM cloud Knowledge Base supports the creation of configuration standards.<br>Periodic and ongoing vulnerability detection is performed across multiple platform modules and components including Container Security and ASRM. For AWS environments, platform integration with Amazon Inspector supplements vulnerability detection capabilities.<br>Inventory capabilities of Trend Vision One include identification of new resources in covered environments. This helps ensure coverage of system components and provides the ability to automate tasks to ensure new systems are configured appropriately.<br>Customers are responsible for defining and implementing configuration standards for all in-scope system components, including system-specific security parameters |
| 2.2.7 | All non-console administrative access is encrypted using strong cryptography. | **Yes.** Trend Vision One implements strong cryptography on all administrative interfaces to the Vision One platform.<br>Trend Vision One can support secure implementation of non-console administrative access to the platform.<br>Trend Vision One provides capabilities to detect and mitigate insecure non-console administrative access at the resource level (Endpoint Security, Container Security) and network level (Network Security), as well as to supplement with security event monitoring (ASRM).<br>Customers are responsible for ensuring in-scope interfaces (e.g., browser-based and APIs) are adequately secured to ensure administrative authorization factors cannot be intercepted from network transmissions.<br>As the Vision One platform supports early versions of the TLS protocol for non-PCI use cases, customers are responsible for ensuring that all connections to the Vision One management interfaces use TLSv1.2 or later. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 2.3 | Wireless environments are configured and managed securely. | **Yes.** Trend Micro’s mobile security capabilities include robust protection against diverse and evolving cyber threats across 4G/LTE and 5G wireless networks. It offers integration into both IT and Communication Technology (CT) domains to protect wireless networks. The solution covers Endpoint, Radio Access Network (RAN), Multi Access Edge Computing (MEC), and 5G Core (5GC) with a zero-trust management and a joint defense (endpoint + network) strategy, enabling organizations to have visibility over wireless devices and ensure that devices are secure, including in-transit data protection. |
| 3.1 | Processes and mechanisms for protecting stored account data are defined and understood. | No |
| 3.2 | Storage of account data is kept to a minimum. | No |
| 3.3 | Sensitive authentication data (SAD) is not stored after authorization. | No |
| 3.4 | Access to displays of full PAN and ability to copy PAN is restricted. | No |
| 3.5 | Primary account number (PAN) is secured wherever it is stored. | No |
| 3.6 | Cryptographic keys used to protect stored account data are secured. | No |
| 3.7 | Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented. | No |
| 4.1 | Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented. | No |
| 4.2 | PAN is protected with strong cryptography during transmission. | **Yes.** ZTSA Private Access provides Secure Access Service Edge (SASE) capabilities to connect remote users to internally hosted applications using TLS-encrypted tunnels, including for applications using unencrypted protocols such as HTTP or Telnet.<br>Using forward proxy-based technologies, ZTSA Secure Web Gateway (SWG) provides inspection and policy enforcement capabilities for user access to public web sites.<br>Customers are responsible for:<br>• Enabling the “Encrypt application traffic using unencrypted protocols” in their ZTSA Private Access configurations.  This ensures end-to-end encryption for clear-text protocols, including when transiting |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | over Trend Micro-managed ZTSA Private Access system components.<br>• Creating ZTSA SWG rules which disable inspection and policy enforcement for traffic which could contain CHD. This ensures that the traffic is not decrypted by the SWG infrastructure and uses the original website's TLS session for end-to-end encryption. |
| 5.1 | Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood. | No |
| 5.2 | Malicious software (malware) is prevented, or detected and addressed. | **Yes.** Trend Vision One provides on-demand and runtime protection for hybrid cloud environments. Capabilities to discover and block multiple threat types (e.g., virus, malware) across all endpoint implementations: endpoints, servers, virtual machines, containers, and storage. |
| 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. | **Yes.** Trend Vision One provides anti-malware capabilities across multiple modules and components including:<br>• Endpoint Security<br>• File Security<br>• Network Security<br>• ASRM<br>Anti-malware attributes are summarized as follows:<br>• Detection of malware, spyware, grayware, viruses, and Trojans<br>• Scanning includes checks for compressions and known exploit code<br>• Clean, delete, or quarantine malicious files<br>• Terminate processes and delete other system objects that are associated with identified threats<br>• Real-time and on-demand protection<br>• Protection for unknown threats and zero-day attacks through Predictive Machine Learning<br>Customers are responsible for deployment on all in-scope systems deemed necessary for anti-malware deployment and for performing a documented threat evaluation of all other system components deemed not at risk to malicious software.<br>Trend Vision One security events are retained and available for 32 days and system events for 91 days. Export capabilities and SIEM integrations are available for customers requiring longer retention periods. |
| 5.2.2 | The deployed anti-malware solution(s):<br>• Detects all known types of malware<br>• Removes, blocks, or contains all known types of malware | |
| 5.2.3 | Any system components that are not at risk for malware are evaluated periodically to include the following:<br>• A documented list of all system | No |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
|  | components not at risk for malware<br>• Identification and evaluation of evolving malware threats for those system components<br>• Confirmation whether such system components continue to not require anti-malware protection |  |
| 5.3 | Anti-malware mechanisms and processes are active, maintained, and monitored. | **Yes.** Trend Vision One provides anti-malware capabilities across multiple modules and components including:<br>• Endpoint Security<br>• File Security<br>• Network Security<br>• ASRM<br>Anti-malware attributes are summarized as follows:<br>• Detection of malware, spyware, grayware, viruses, and Trojans<br>• Scanning includes checks for compressions and known exploit code<br>• Clean, delete, or quarantine malicious files<br>• Terminate processes and delete other system objects that are associated with identified threats<br>• Real-time and on-demand protection<br>• Protection for unknown threats and zero-day attacks through Predictive Machine Learning<br>Customers are responsible for deployment on all in-scope systems deemed necessary for anti-malware deployment and for performing a documented threat evaluation of all other system components deemed not at risk to malicious software.<br>Trend Vision One security events are retained and available for 32 days and system events for 91 days. Export capabilities and SIEM integrations are available for customers requiring longer retention periods. |
| 5.3.1 | The anti-malware solution(s) is kept current via automatic updates. |  |
| 5.3.2 | The anti-malware solution(s):<br>• Performs periodic scans and active or real-time scans OR<br>• Performs continuous behavioral analysis of systems or processes |  |
| 5.3.3 | For removable electronic media, the anti-malware solution(s):<br>• Performs automatic scans of when the media is inserted, connected, or logically mounted<br>OR<br>• Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted |  |
| 5.3.4 | Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. |  |
| 5.4 | Anti-phishing mechanisms protect users against phishing attacks. | **Yes.** Trend Vision One Email and Collaboration Security provides capabilities to detect, alert, and block phishing attacks. Advanced analysis capabilities of current threat activity can help determine if broader, more advanced attacks are imminent or underway. Trend Vision One can also simulate realistic phishing attacks and identify security risks in your organization using Phishing Simulation Assessment. This allows companies to simulate a phishing attack by simply choosing a phishing email template, select your employees, launch your simulation, and monitor the results. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 5.4.1 | Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. | **Yes.** Trend Vision One includes Predictive Machine Learning and Intrusion Prevention which are effective in detecting and protecting against security events originating from phishing attacks. |
| 6.1 | Processes and mechanisms for developing and maintaining secure systems and software are defined and understood. | No |
| 6.2 | Bespoke and custom software are developed securely. | No |
| 6.3 | Security vulnerabilities are identified and addressed. | **Yes.** Trend Vision One consolidates multiple industry methodologies for sourcing cybersecurity vulnerabilities (e.g., CVE, MITRE, OWASP) and provides targeted/filtered reporting for your specific assets. |
| 6.3.1 | Security vulnerabilities are identified and managed as follows:<br>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs)<br>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact<br>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment<br>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. | **Yes.** ASRM detects critical and high-risk vulnerabilities, as well as high impact (not considered critical or high risk).<br>Container Security performs runtime vulnerability scanning and provides results based on severity and/or CVE score, including contextual data, and a fix if available. Vulnerability data is automatically updated as a component of the platform.<br>Endpoint Security identifies vulnerabilities through the Intrusion Prevention component. Results include detailed information about the vulnerability detected, Common Vulnerability Scoring System (CVSS), and/or severity.<br>Network Security uses Intrusion Prevention Filtering from available threat intelligence packages for vulnerability identification. Vulnerability results include CVE and severity, as well as context for the finding and remediation. Threat intelligence filters can be automatically updated with the auto-sync feature or manually distributed at any time using an API.<br>Endpoint Security, Container Security, and Network Security provide capabilities for active patching, when patches are available, and virtual patching using the resource/service/network layers until security patches are released.<br>For AWS environments, platform integration with Amazon Inspector supplements vulnerability scanning capabilities. By default, relays provide security updates released weekly.<br>Trend Vision One Intrusion Detection capability features controls to detect web application vulnerabilities in operating systems and application code. Endpoint Security integrates with the AWS WAF to detect and stop edge attacks. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
|  |  | Optionally, manual updates can be provisioned.<br>Customers are responsible for ensuring identified vulnerabilities are monitored, cataloged, and risk evaluated. Critical and high-risk vulnerabilities are resolved as part of the three-month scan cycle and residual vulnerabilities addressed according to targeted risk analysis results. Where continuous or real-time scanning  is unavailable, manual scans are performed after significant changes (as defined in the PCI DSS v4.0). |
| 6.3.2 | An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. | **Yes.** Trend Vision One Container Security builds a Software Bill of Materials (SBOM) of all content running in the container.  The Artifact Scanner (TMAS) updates and monitors the status of software assets in the container. |
| 6.3.3 | All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:<br>• Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release<br>All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release) | **Yes.** Endpoint Security, Container Security, and Network Security provide capabilities for active patching, when patches are available, and virtual patching using the resource/service/network layers until security patches are released.<br>For AWS environments, platform integration with Amazon Inspector supplements vulnerability scanning capabilities. By default, relays provide security updates released weekly.<br>Optionally, manual updates can be provisioned.<br>Customers are responsible for ensuring identified vulnerabilities are monitored, cataloged, and risk evaluated. Critical and high-risk vulnerabilities are resolved as part of the three-month scan cycle and residual vulnerabilities addressed according to targeted risk analysis results. Where continuous or real-time scanning  is unavailable, manual scans are performed after significant changes (as defined in the PCI DSS v4.0). |
| 6.4 | Public-facing web applications are protected against attacks. | **Yes.**  Trend Vision One Intrusion Detection capability features controls to detect web application vulnerabilities in operating systems and application code. Endpoint Security integrates with the AWS WAF to detect and stop edge attacks. |
| 6.5 | Changes to all system components are managed securely. | No |
| 7.1 | Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. | No |
| 7.2 | Access to system components and data is appropriately defined and assigned. | No |
| 7.3 | Access to system components and data is managed via an access control system(s). | No |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 8.1 | Processes and mechanisms for identifying users and authenticating access to system components are defined and understood | No |
| 8.2.1 | All users are assigned a unique ID before access to system components or cardholder data is allowed. | **Yes.** Trend Vision One supports SSO using SAML. SAML SSO establishes a trust relationship between Trend Vision One federating identification and authentication to the customer's identity provider. Trend Vision One continues to support a native sign-on through the web interface, which is separate from SAML SSO, but as this method does not support multi-factor authentication, only SAML-based federation should be used for environments requiring PCI DSS compliance.<br>Customers are responsible for configuring Trend Vision One access control settings according to all PCI DSS requirements. |
| 8.2.2 | Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis. | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend  Vision One telemetry can support customer initiatives to identify the existence and use of group, shared, and generic accounts. |
| 8.2.6 | Inactive user accounts are removed or disabled within 90 days of inactivity. | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend  Vision One provides telemetry that can support customer's ability to identify inactive accounts. |
| 8.3 | Strong authentication for users and administrators is established and managed. | No |
| 8.3.1 | All user access to system components for users and administrators is authenticated. | Yes. In addition to supporting IAM federation to customer's identity providers, Trend  Vision One native access controls provide unique identification via username and password/passphrase.<br>Only SAML-based federation should be used for environments requiring PCI DSS compliance. |
| 8.3.2 | Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend  Vision One native access hashes all user passwords according to industry standard password hashing algorithms.<br>Only SAML-based federation should be used for environments requiring PCI DSS compliance. |
| 8.3.4 | Invalid authentication attempts are limited. | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend  Vision One native access controls provide limitations for invalid authentication attempts to support this requirement.<br>Also, only SAML-based federation should be used for environments requiring PCI DSS compliance. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | Customers are responsible for configuring Trend Vision One access control settings according to all PCI DSS requirements. |
| 8.3.6 | If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet a minimum level of complexity: | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend Vision One native access controls provide password/passphrase complexity capabilities to support this requirement.<br>Customers are responsible for configuring access control policy settings according to all PCI DSS requirements. |
| 8.3.9 | If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>OR<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | **Yes.** In addition to supporting IAM federation to customer's identity providers, Trend Vision One native access controls provide password/passphrase rotation capabilities to support this requirement.<br>Vison One ZTSA monitors and controls users access to assets as well as alerts for passwords that have not been changed in a long time<br>Trend Vision One XDR helps the security team identify potentially compromised accounts or roles.<br>Customers are responsible for configuring access control policy settings according to all PCI DSS requirements. |
| 8.4 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. | **Yes.** Trend Vision One supports MFA set in customer's IdP via SSO/SAML. |
| 8.4.1 | MFA is implemented for all non-console access into the CDE for personnel with administrative access. | **Yes.** Trend Vision One supports SSO using SAML to support MFA requirements as established and implemented by the customer. |
| 8.4.2 | MFA is implemented for all access into the CDE. | **Yes.** Trend Vision One supports SSO using SAML to support MFA requirements as established and implemented by the customer. |
| 8.4.3 | MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:<br>• All remote access by all personnel, both users and administrators, originating from outside the entity's network.<br>• All remote access by third parties and vendors. | **Yes.** Trend Vision One supports SSO using SAML to support MFA requirements as established and implemented by the customer. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 8.5 | Multi-factor authentication (MFA) systems are configured to prevent misuse. | |
| 8.6 | Use of application and system accounts and associated authentication factors is strictly managed. | |
| 9.1 | Processes and mechanisms for restricting physical access to cardholder data are defined and understood. | No |
| 9.2 | Physical access controls manage entry into facilities and systems containing cardholder data. | No |
| 9.3 | Physical access for personnel and visitors is authorized and managed. | No |
| 9.4 | Media with cardholder data is securely stored, accessed, distributed, and destroyed. | No |
| 9.5 | Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. | No |
| 10.1 | Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented. | No |
| 10.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. | **Yes.** Sending logs into Vision One enables the security team to easily find the suspicious activities via the Trend Micro product logs and cloud service provider audit logs like CloudTrail. |
| 10.2.1 | Audit logs are enabled and active for all system components and cardholder data. | **Yes.** Trend Vision One records security events and system events across all modules. A security event means a platform rule or condition is triggered within a module.<br>System events include platform-related and administrative actions, such as agent software being upgraded or an administrator logging in, and administrative actions performed by individual, application, and system accounts, including:<br>• Invalid request to access audit data<br>• Authentication failed<br>• User creation/deletion/update<br>• Audit start/shutdown<br>• System-level creation/deletion<br>Trend does not have visibility to customer audit logs that are not specifically enabled and made available to the Trend Vision One platform. |
| 10.2.1.2 | Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. | |
| 10.2.1.3 | Audit logs capture all access to audit logs. | |
| 10.2.1.4 | Audit logs capture all invalid logical access attempts. | |
| 10.2.1.5 | Audit logs capture all changes to identification and authentication credentials including, but not limited to:<br>• Creation of new accounts<br>• Elevation of privileges<br>• All changes, additions, or deletions to accounts with administrative access | |
| 10.2.1.6 | Audit logs capture the following:<br>• All initialization of new audit logs<br>• All starting, stopping, or pausing of the | |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | existing audit logs | Trend Vision One provides capabilities for customers to automate the configuration and validation of audit log settings for cloud-based environments.<br>**Yes.** Trend Vision One security and system event details include time, severity, event identifier, event name, target, origin, user/action, resolver, and description.<br>Customers are responsible for:<br>• Ensuring all in-scope system components have audit log settings configured to meet PCI DSS 4.0 requirements.<br>• If using the DLP features in endpoint security products, disabling the "Forensic Evidence Collection" feature as this results in full PAN being stored in Vision One for PCI-related DLP detections. |
| 10.2.1.7 | Audit logs capture all creation and deletion of system-level objects. | |
| 10.2.2 | Audit logs record the following details for each auditable event:<br>• User identification<br>• Type of event<br>• Date and time<br>• Success and failure indication<br>• Origination of event<br>• Identity or name of affected data, system component, resource, or service (for example, name and protocol) | |
| 10.3 | Audit logs are protected from destruction and unauthorized modifications. | **Yes.** Sending logs into Vision One enables security teams to easily find the suspicious activities via the Trend Micro product logs and CSP audit logs like CloudTrail<br>Trend Vision One security and system events are immutable. |
| 10.3.2 | Audit log files are protected to prevent modifications by individuals. | |
| 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. | |
| 10.3.4 | File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. | |
| 10.4 | Audit logs are reviewed to identify anomalies or suspicious activity. | **Yes.** As well, sending logs into Vision One enables the security team to easily find the suspicious activities via the Trend Micro product logs and CSP audit logs like CloudTrail<br>Audit log inspection is performed by Trend Vision One, including Endpoint Security, Container Security, ASRM, and Network Security. For AWS environments, Trend Vision One platform integration with Amazon Inspector supplements these capabilities.<br>Security monitoring (audit log review) correlates audit logs generated from across the Trend Vision One modules and from customer infrastructure. Trend platforms do not have visibility of customer infrastructure audit logs that are not specifically enabled and made available. |
| 10.4.1 | The following audit logs are reviewed at least once daily:<br>• All security events<br>• Logs of all system components that store, process, or transmit cardholder data and/or SAD<br>• Logs of all critical system components<br>• Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers) | |
| 10.4.2 | Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. | |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | | Customers are responsible for reviewing detected security events at least daily to be fully compliant with this requirement. Audit logs and detected events can be moved into other systems of record, such as a SIEM, using available platform integrations. |
| 10.5 | Audit log history is retained and available for analysis. | **Yes.** Audit log inspection is performed by Trend Vision One, including Endpoint Security, Container Security, ASRM, and Network Security. For AWS environments, Trend Vision One platform integration with Amazon Inspector supplements these capabilities.<br>Security monitoring (audit log review) correlates audit logs generated from across the Trend Vision One modules and from customer infrastructure. Trend platforms do not have visibility of customer infrastructure audit logs that are not specifically enabled and made available.<br>Customers are responsible for reviewing detected security events at least daily to be fully compliant with this requirement. Audit logs and detected events can be moved into other systems of record, such as a SIEM, using available platform integrations.<br>Trend Vision One XDR can collect Trend Micro products logs and forward to 3rd party SIEMs to make it easy to retain the logs<br>Security events are retained and available for 32 days and system events for 91 days. Customers can hold data for up to a year as an add-on. Export capabilities  and integrations are available for customers requiring longer retention periods. |
| 10.5.1 | Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis. | |
| 10.6 | Time-synchronization mechanisms support consistent time settings across all systems. | No |
| 10.7 | Failures of critical security control systems are detected, reported, and responded to promptly. | **Yes.** Trend Vision One Unusual Product Status feature reports unexpected or atypical status for third party products integrated with the platform.<br>ASRM detects and alerts on cloud account configurations that deviate from expected standards (e.g., CIS Level 1)" |
| 10.7.1<br>10.7.2 | Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:<br>• Network security controls<br>• IDS/IPS | **Yes.** Trend Vision One monitors the status of deployed security functions and modules that are components of the platform and alerts the customer to status. Critical security controls provided through the platform include:<br>• Network security controls<br>• IDS/IPS<br>• Change-detection mechanisms |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | • Change-detection mechanisms<br>• Anti-malware solutions<br>• Physical access controls<br>• Logical access controls<br>• Audit logging mechanisms<br>• Segmentation controls (if used)<br>• Audit log review mechanisms<br>• Automated security testing tools (if used) | • Anti-malware solutions<br>• Logical access controls<br>• Audit logging mechanisms<br>• Segmentation controls<br>• Audit log review mechanisms |
| 11.1 | Processes and mechanisms for regularly testing security of systems and networks are defined and understood. | No |
| 11.2 | Wireless access points are identified and monitored, and unauthorized wireless access points are addressed. | No |
| 11.3 | External and internal vulnerabilities are regularly identified, prioritized, and addressed. | No |
| 11.4 | External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. | No |
| 11.5 | Network intrusions and unexpected file changes are detected and responded to. | **Yes.** The TippingPoint (data center) product and Workload and Endpoint Security solutions provide intrusion detection and prevention (IDS/IPS) features and capabilities. |
| 11.5.1 | Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows:<br>• All traffic is monitored at the perimeter of the CDE<br>• All traffic is monitored at critical points in the CDE<br>• Personnel are alerted to suspected compromises<br>• All intrusion-detection and prevention engines, baselines, and signatures are kept up to date | **Yes.** Trend Vision One performs host- and network-based intrusion prevention through multiple security modules.<br>Endpoint Security provides host-based intrusion prevention with extended coverage through the Container Protection component.<br>Network-based intrusion prevention is provided by the Network Security module.<br>Deployment options enable perimeter and ingress/egress monitoring, as well as east-west traffic. Modules providing intrusion prevention support alerts and notifications to suspect events.<br>Host-based intrusion prevention rules are updated weekly by default. Optionally, manual updates can be provisioned.<br>Network threat intelligence filters can be automatically updated with an auto-sync feature or manually distributed at any time using an API.<br>Host- and network-based intrusion prevention capabilities include blocking command-and-control domains and offending sessions. |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| 11.5.2 | A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:<br>• To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.<br>• To perform critical file comparisons at least once weekly. | **Yes.** Trend Vision One performs integrity monitoring through Endpoint Security and ASRM. Endpoint<br>Security monitors for suspicious changes in the host operating system of Amazon EC2 instances, including the addition of suspicious artifacts, and IoAs. Using a baseline secure state as a reference, Endpoint Security integrity monitoring scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files. Custom rules can be created as well. Unexpected changes trigger an event log and a customer-configured alert notification.<br>The customer is required to define critical files, resources, and workflow for analysis, in addition to configuring alerts. |
| 11.6 | Unauthorized changes on payment pages are detected and responded to. | No |
| 12.1 | A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current. | No |
| 12.2 | Acceptable use policies for end-user technologies are defined and implemented. | No |
| 12.3 | Risks to the cardholder data environment are formally identified, evaluated, and managed. | No |
| 12.4 | PCI DSS compliance is managed. | No |
| 12.5 | PCI DSS scope is documented and validated. | No |
| 12.6 | Security awareness education is an ongoing activity. | **Yes.** Trend Vision One platform includes an anti-phishing training program to support security awareness in the enterprise. |
| 12.6.3.1 | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:<br>• Phishing and related attacks.<br>• Social engineering. | |
| 12.7 | Personnel are screened to reduce risks from insider threats. | No. |
| 12.8 | Risk to information assets associated with third-party service provider (TPSP) relationships is managed. | No |
| 12.9 | Third-party service providers (TPSPs) support their customers' PCI DSS compliance. | No |
| 12.10 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. | **Yes.** Trend Vision One Case Management tools support incident response teams by providing notifications of suspicious network traffic activities. |
| 12.10.5 | The security incident response plan includes | **Yes.** Trend Vision One provides security event data across |

| PCI DSS Requirement # | Defined Approach Requirements | Addressed by Trend Vision One |
|---|---|---|
| | monitoring and responding to alerts from security monitoring systems, including but not limited to:<br>- Intrusion-detection and intrusion-prevention systems<br>- Network security controls<br>- Change-detection mechanisms for critical files<br>- The change-and tamper-detection mechanism for payment pages<br>- Detection of unauthorized wireless access points | all platform modules.<br>Customers are responsible for establishing monitoring and response processes for detected security events.<br>Platform integrations with ticketing and workflow solutions provide a mechanism  to automate elements of incident response including:<br>- Detection<br>- Analysis<br>- Containment<br>- Eradication<br>- Prevention<br>Trend Vision One audit logs and detected events can be moved into other systems of record, such as a SIEM, using available platform integrations to support incident alerting and response processes. |