WHITEPAPER

TANIUM

PCI-DSS 4.0

Meeting the Payment Card Industry Data Security Standard:

How Tanium can help

When creating any software for use with payment processing, The Payment Card Industry Data Security Standard (PCI-DSS) has particular requirements and controls that must be in place to protect data and keep the software and infrastructure safe. The holistic approach covers every aspect, from how the data is collected, handled, and stored to the infrastructure and processes that support it.

The latest PCI-DSS

PCI-DSS has long been regarded as the gold standard for ensuring the security of sensitive cardholder data within the financial and retail industries. Historically, PCI-DSS provided a comprehensive checklist of specific controls organizations must implement to safeguard cardholder information.

In 2022, a significant update was made with the introduction of PCI-DSS version 4.0. This latest version represents a paradigm shift from the traditional prescriptive approach to a more flexible, outcome-based framework. Unlike its predecessors, PCI-DSS v4.0 emphasizes the intent behind each requirement, focusing on the effectiveness of the security controls rather than prescribing the exact methods for their implementation.

This outcome-based approach allows organizations more flexibility in how they achieve compliance, provided they can demonstrate that their methods effectively meet the desired security outcomes. By prioritizing the results and ensuring that the controls fulfill the intended security objectives, PCI-DSS v4.0 encourages innovation and adaptability in protecting cardholder data. Organizations can now tailor their security measures to better fit their specific environments while still adhering to the rigorous standards set forth by the PCI Security Standards Council.

Not all vendors can satisfy all 12 PCI requirements since the PCI-DSS standard addresses every aspect, from how the data is collected, handled, and stored to the infrastructure and processes that support it. This approach, which leans heavily on the human element of people and processes, can be separated into six categories:

1. Build and Maintain a Secure Network and Systems
2. Protect Account Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

How Tanium can help

The human process and physical security requirements make up roughly half of PCI-DSS. Tanium solves nearly all IT infrastructure-related requirements, including 100 percent of the repetitive tasks like monthly patching, weekly file integrity monitoring, quarterly vulnerability scanning, etc.

Many of the PCI-DSS technical requirements below can be met with the Tanium Core platform tiers that include the following Tanium modules: Asset, Discover, Benchmark, SBOM, Enforce, Certificate Manager, and Investigate.

	Core X1	Core X2	Core X3
Tanium Core	✓	✓	✓
Tanium Asset	✓	✓	✓
Tanium Discover	✓	✓	✓
Tanium Benchmark	✓	✓	✓
Tanium SBOM	✗	✓	✓
Tanium Certificate Manager	✗	✗	✓
Tanium Investigate	✗	✗	✓

	PCI-DSS Requirement	How Tanium Helps	Relevant Tanium Modules
1.4	Network connections between trusted and untrusted networks are controlled	• Fully manage the firewalls with blocking rules • Deploy and monitor third-party endpoint firewalls from McAfee and others	• Core X1 • Deploy
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 • Enable only necessary services, protocols, daemons, etc. as required for the function of the system	• Identify servers inside of the PCI scope that are performing multiple functions (running appliances/ servers) • Shutdown unnecessary services • Security configuration templates for known services, protocols, daemons (specific SSL, TLS and/or other services that allow for encryption or secure operation) • Ability to remove unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and web servers, protocols, daemons (specific SSL, TLS and/or other services that allow for encryption or secure operation) • Ability to remove unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and web servers • Author sensors to assess the configuration state of browsers and other applications to ensure they are configured to use strong cryptography • Once an organization has codified their security policies and advertised them with all affected parties then Tanium is used to enforce those policies on all endpoints	• Core X3 • Comply • Deploy • Impact • Integrity Monitor
2.2.3	Primary functions requiring different security levels are managed		
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled		
2.2.6	System security parameters are configured to prevent misuse		
2.2.7	All non-console administrative access is encrypted using strong cryptography		
3.2	Storage of account data is kept to a minimum, and account data is retained only where necessary for the least amount of time and securely deleted or rendered unrecoverable when no longer needed	• Find all the servers, laptops or workstations in your environment • Use Reveal to search for specific PCI account data across an entire enterprise and sensitive information that matches a search string in real time • Identify all PCI servers on the same subnet as known servers with PCI content • Create specific content to find PCI-DSS authentication data on machines where the Tanium agent is installed	• Core X1 • Reveal

	PCI-DSS Requirement	How Tanium Helps	Relevant Tanium Modules
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks	• Create specific content to assess the configuration state of browsers and other applications to ensure they are configured to use strong cryptography • SSL/TLS configuration validation (PCI Appendix G) • Note: Special cases here for systems on Wi-Fi networks; identifying systems on Wi-Fi that are in the PCI scope groups would be an important "subgroup" within the PCI scope group	• Core X2
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored	• Enable, configure, and monitor Windows Defender (or many other third-party anti-malware) on laptops, desktops and servers • Send audit logs to external systems such as SIEM or syslog • Create content to validate the permission settings of users on each system • Remove local administrator accounts from all endpoints • Create content to watch for disabled agents and alert, deploy, or restart action	• Core X2
5.3.1	Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI-DSS Requirement 10.7		
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 period		
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	• Scan all devices for known security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks • Tanium utilizes Security Content Automation Protocol (SCAP) compliant content, such as standards published by the Defense Information Systems Administration (DISA) or the Center for Internet Security (CIS) • Prioritize CVE according to IT environment requirements and additional prioritization with CISA-KEV to provide better visibility into the most critical vulnerabilities • Supports vulnerability assessment scanning based on organization policies • Guardian notifies SOC and IT teams of critical incidents that apply to their environment and includes resolution actions • Tanium SBOM inventories and scans all third-party catalogs and libraries incorporated into bespoke and custom software to identify CVEs and creates and inventory	• Core X3 (SBOM, Investigate) • Comply • Patch • Threat Response • Impact • Guardian
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		

	PCI-DSS Requirement	How Tanium Helps	Relevant Tanium Modules
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • 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 • 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)	• Assess and install patches on Windows, Linux, and macOS devices • Define custom workflows and schedule patches based on rules or exceptions built around patch lists, block lists, and maintenance windows • Use rules to dynamically populate lists of patches, patches are added when they meet adhere to the defined rule • Ensures patch management is up to date and meets compliance standards	• Core X2 • Patch • Provision • Deploy • Comply
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	• Watch for changes to log data and alert when any changes are made	• Core X1 • Integrity Monitor
10.6.1	Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time	• Ensure NTP is configured correctly across all systems • Ensure time synchronization is configured properly to a standard NTP server	• Core X1
10.7.2 & 10.7.3	Failures of critical security control systems are detected, alerted, and addressed promptly	• Continuously records key system activity for forensic and historical analysis • Find specific activity across every device in an enterprise and drill down into process and user activity in real time • Investigate alerts from external sources, such as Microsoft Defender and Deep Instinct • Found compromised devices are isolated to prevent additional compromise, data leakage, and lateral movement	• Core X3 • Threat Response • Impact
11.2.1	Authorized and unauthorized wireless access points are managed	• Discover and identify all devices on the network, including wireless access points, whether or not the Tanium Agent is installed on that device • Integrate with Palo Alto Networks firewalls to block unauthorized access points from connecting	• Core X2
11.2.2	An inventory of authorized wireless access points is maintained		

	PCI-DSS Requirement	How Tanium Helps	Relevant Tanium Modules
11.3.1 and all related subsections	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 PCI-DSS 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	• Reduce the lag between vulnerability scans • Perform vulnerability assessments quarterly or more often • Perform vulnerability assessments on any "significant change" • Identify significant vulnerability changes and fix, if necessary • Vulnerability scans conducted at least every three months to identify and address vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data	• Core X2 • Integrity Monitor • Patch • Provision • Deploy • Comply
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files • To perform critical file comparisons at least once weekly	• Monitor an alert on unauthorized modifications of critical files • Examine system settings, monitored files, and results from monitoring activities to verify the use of a change-detection mechanism • Examine settings for the change-detection mechanism to verify it is configured in accordance with all elements specified in this requirement	• Core X2 • Integrity Monitor • Comply

	PCI-DSS Requirement	How Tanium Helps	Relevant Tanium Modules
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 • Resulting 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	• Perform risk analysis for all PCI devices that are managed by Tanium and produce reports • Graphical assessment and compliance automatically updated with drill down detail and contextual information • Once an organization has codified their security policies and advertised them with all affected parties then Tanium is used to enforce those policies on all endpoints (for those capabilities listed in this document)	• Core X3
12.3.2	A targeted risk analysis is performed for each PCI-DSS requirement that the entity meets with the customized approach		
12.5.1	Maintain an inventory of system components that are in scope for PCI-DSS		• Core X1