SOLUTION BRIEF

REVERSINGLABS

How RL Supports PCI DSS v4.0

Overview

The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to strengthen global payment security with data and software security standards and resources. PCI SSC has developed a number of standards/frameworks to help safeguard the payment ecosystem, these include:

- Payment Card Industry Data Security Standard (PCI DSS) is designed to increase security controls around account data with Requirement 6 defining the standards for development and maintenance of secure systems and software
- PCI Software Security Framework is designed to assess software and will support organizations and software vendors in meeting PCI DSS Requirement 6
- Secure Software Lifecycle (SLC) Standard that defines required security practices and controls for software producers to integrate into their software pipelines
- Secure Software Standard (SSC) which defines a set of security requirements that organizations can use to confirm that software has been developed using secure practices

PCI DSS version 4.0 was published in March 2022 and replaces version 3.2.1 to "address emerging threats and technologies and enable innovative methods to combat new threats"[1]. All internal software used to store, process, or transmit account data, or may impact the security of account data, is in scope for PCI DSS assessments (for more scoping considerations refer to Section 4 the PCI DSS documentation[2]). Details about the updates can be found in the PCI DSS v4.0 Summary of Changes document[3] and include a new requirement focused on software supply chain security and improving software transparency, for example, Requirement 6.3.2 directs organizations to maintain an inventory of all bespoke, custom and third-party software components. This requirement is a best practice until 31 March 2025, after which it will be enforced.

The Need for More Visibility Into Business and Compliance Risks

Within the last few years, there are several examples of high-profile breaches that were not perpetrated by exploiting a known vulnerability, but by clandestinely compromising different aspects of the software supply chain. In 2023 alone, ReversingLabs discovered over 11,000 malicious software packages across three major open-source repositories: npm, PyPI, and RubyGems that are part of enterprise software supply chains[4]. Many of these malicious components are obfuscated or encrypted, making detection using traditional application security testing (AST) tools nearly impossible.

To make tangible steps towards securing the supply chains of software used to store, process, or transmit account data, organizations need more transparency into software components and detection of malicious changes to those components. Actionable security assessments which can shed light on business and compliance risks are the solution.

ReversingLabs Spectra Assure Delivers Transparency

ReversingLabs Spectra Assure™ fills the compliance and visibility gap by rapidly analyzing every software component and file within a software binary for malware, tampering, vulnerabilities and other indicators of supply chain attacks. What makes Spectra Assure stand out against other solutions is complex binary analysis, which:

- Assesses software without the need for developer's source code, providing insights for both software producers and buyers
- Scans complex files rapidly, as fast as 1 GB in 5 minutes, which enables organizations to assess every software version
- Supports over 400 binary formats to create a comprehensive list of software components
- Verifies third-party and open-source component integrity and provenance using comparisons against trusted binary repositories

Spectra Assure also goes beyond simple inventory listing. The automated analysis delivers a comprehensive risk assessment that identifies threats undetectable by traditional application security and vendor acquisition tools, for example:

- Malware is detected leveraging the largest private threat repository with over 40 billion searchable samples, over 385 billion file hashes, and 16 proprietary detection engines to prevent advanced threats from spreading throughout the software supply chain
- Tampering is identified as soon as the application changes in a suspicious way, or when a reproducible build fails verification
- Exposed secrets are reported with automatic prioritization of active SaaS login credentials and noise reduction powered by threat repository data to improve remediation effectiveness
- Vulnerabilities actively exploited by malware are reported, helping organizations focus their remediation efforts based on the level of risk

The analysis indicates exactly which software components contain the identified risks. It also automatically generates a plan for addressing those risky components by recommending manageable projects.This enables more effective risk management which is the overall goal of PCI security standards.

How RL Supports PCI DSS v4.0

Spectra Assure supports important aspects of PCI DSS requirements related to software supply chain security, specifically preventing malware from being deployed, assessing the safety of software developed internally and by third-parties, and delivering a comprehensive inventory of their software components.

PCI DSS Requirements v4.0	ReversingLabs Response
Requirement 5: Protect All Systems and Networks from Malicious Software	
5.2 Malicious software (malware) is prevented, or detected and addressed.	
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	Spectra Assure detects and prevents malicious code embedded in custom or commercial software or updates from being deployed on enterprise systems and networks. Spectra Assure analyzes the entire software package (components and files) for malware. Software components analyzed include bespoke, custom, third-party, open-source, and commercial components. Spectra Assure identifies malicious software by leveraging the largest private threat repository with over 40 billion searchable samples, over 385 billion file hashes, 16 proprietary detection engines and actionable alerts curated by a world-class team of threat researchers. The comprehensive risk assessment report (which also assesses other supply chain risks such as tampering, malware-exploited vulnerabilities and exposed secrets) is easily shared with software suppliers to facilitate remediation. When malware is detected, Spectra Assure can fail the software build or package, preventing further software delivery steps from executing, which could include deployment to production systems, effectively stopping malware from affecting the security of the cardholder data environment (CDE).
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	The solution's code base is updated frequently and Spectra Assure automatically checks for updates before scanning.[5]

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.	The threat repository is constantly updated with new information gleaned from our threat research team and the more than 11 million files scanned every day by ReversingLabs technology. Organizations can configure Spectra Assure to run against every build (real time) or periodically by tuning their software delivery pipeline steps.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **Applicability Notes** This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	Organizations have full control over how frequently Spectra Assure scans binaries both in the software delivery pipeline and before software is deployed (periodically or on demand, or both) so they can ensure it aligns with organizational risk appetite.
Requirement 6: Develop and Maintain Secure Systems and Software	
6.2 Bespoke and custom software is developed securely.	
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle. **Applicability Notes** This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.	To support software developers, Spectra Assure can be integrated at any point in the Software Development Lifecycle (SDLC) where software binaries are added, produced or released. Automated version difference reporting provides a real-time feedback loop that informs developers of issues requiring remediation before release. The solution also assesses the software's risk level and generates a customizable remediation roadmap based on industry best practices, which promotes collaboration between software producers and consumers on software risk and remediation.

6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	Organizations can use Spectra Assure to augment code review processes by identifying software supply chain threats that traditional vulnerability detection tools are not designed to find (e.g. malware, suspicious software changes, and other indicators of software tampering) prior to being released. With a comprehensive view of both software supply chain threats from Spectra Assure and vulnerabilities from application security tools, organizations can focus their remediation efforts on the most critical threats to the security of the cardholder data environment (CDE). Spectra Assure's differential analysis can verify that appropriate corrections are made prior to release.
6.3 Security vulnerabilities are identified and addressed.	
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 (CERT s). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings, at a minimum, identify all vulnerabilities considered to be a high- risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. **Applicability Notes** This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.	Spectra Assure rapidly analyzes software (in as little as a minute for small components or an hour for multi-gigabyte package) and produces: • A comprehensive software bill of materials (SBOM) of the final release build, including bespoke, custom, third-party, open-source, and commercial components • A risk report that locates malware, tampering, vulnerabilities, and other exposures within each SBOM item and file from the final build New security vulnerabilities are identified using industry-recognized sources for security vulnerability information such as: • NIST National Vulnerability Database (NVD) • OSV.dev - a vulnerability database that aggregates & indexes vulnerability data from a variety of sources that leverage the Open Source Vulnerability (OSV) data format • CISA Known Exploited Vulnerabilities (KEV) Catalog To help developers prioritize and facilitate remediation reported vulnerabilities include information about: • Malware actively exploiting the vulnerability • The vulnerability's data source (e.g. OSV.dev, NIST NVD, CISA KEV) • Severity, risk priority and estimated level of remediation effort ranking of High, Medium and Low

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. **Applicability Notes** This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	Spectra Assure generates a comprehensive software bill of materials (SBOM) by analyzing the entire software binary being released or deployed. The inventory includes bespoke, custom, and third-party software components from open source platforms, commercial providers, as well any software developed by third-party organizations. This approach of assessing the software binary is independent of items declared in developer's build manifests and can create a more complete inventory to facilitate vulnerability, patch and vendor risk management. The inventory can be shared with other tools by exporting it using CycloneDX and Software Package Data Exchange (SPDX) industry standard formats.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

We'll Show You How To Reduce Software Supply Chain Risks With ReversingLabs

REQUEST A DEMO

www.reversinglabs.com

References:

[1] https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/
[2] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
[3] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf
[4] ReversingLabs State of Software Supply Chain Security 2024 Report
[5] https://docs.secure.software/cli/commands/update

RL REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com