

# Move beyond periodic scanning: Achieve continuous PCI DSS readiness

Traditional vulnerability programs rely on point-in-time scans that leave blind spots between assessments. Armis Centrix™ for Vulnerability Management Detection and Response continuously discovers, assesses, and prioritizes vulnerabilities across your entire attack surface, helping security teams maintain ongoing PCI DSS alignment while accelerating remediation.

PCI DSS v4.0.1, outlined in 6 core goals and 12 requirements, raises the bar for continuous security monitoring, risk management, and evidence-based compliance. Organizations need more than quarterly scans to keep pace with dynamic environments, emerging threats, and expanding asset inventories. Armis Centrix™ for Vulnerability Management Detection and Response provides the continuous, comprehensive monitoring for all connected assets, including those traditional scanners miss. The result is a continuous, evidence-based vulnerability management program that closes the loop from detection to response, supporting autonomous awareness, security, monitoring, and reporting in alignment with best practice guidance.

## Key benefits of continuous vulnerability detection

- Real-time identification of vulnerabilities across the attack surface
- Discovery of all assets traditional scanners miss
- Faster identification of emerging vulnerabilities
- Prioritized remediation with validated business and asset context
- Continuous evidence collection for audit readiness
- Reduced risk exposure with automated response workflows

## The core PCI DSS detection principles:

### Assess the entire attack surface

- Inventory of all assets, data, and access points, even those traditional scanners miss.
- Continuous detection of emerging risks as they appear on any system or asset.
- Customizable detection policies including asset discovery using ICMP, SNMP, and other protocols, vulnerability detection scans, network-based scans using authentication protocols, exploit verification, or adaptive policy scans.

### Monitor for any network changes

- Continuous, evidence-based assessment and validation of risk exposure.
- Always-on alerts for any notable changes in security posture.
- Validated results with deep asset context eliminates false positives/negatives.

### Establish a vulnerability remediation program

- Autonomous security and remediation workflows.
- Context-aware risk assessment and prioritization based on business context.
- Critical/high patches applied within one month of release.

### Report on efficacy and security

- Demonstrate PCI DSS compliance via comprehensive reports on risk exposure, resolution, and MTTR.
- Ongoing awareness, reporting, and exposure management demonstration, not just point-in-time snapshots of risk.
- Report on asset inventory, response, risk changes, and remediation time.

### Maintain a consistent approach

- Comprehensive coverage of all assets in real-time.
- Assess on change, maintaining dynamic, event-driven security coverage without disruption.
- Establish and maintain a clear vulnerability management policy, from detection to prioritization and response.



## Now part of the ServiceNow Blueprint for Autonomous Security

Everything you just read now runs inside something bigger. Armis is part of the [ServiceNow Blueprint for Autonomous Security](#), where asset intelligence, exposure findings, identity context, and AI-driven remediation all land on the same platform to get work done.

Armis Centrix™ for Vulnerability Management Detection and Response now lives under Continuous Vulnerability Detection, the ServiceNow pillar for catching and closing exposure before it turns into an incident. Same engine, same coverage, new place on the map.

### Armis Centrix™ for Vulnerability Management Detection and Response supports PCI DSS alignment

| Clause          | Requirement                                                                                      | Armis Centrix™ for Vulnerability Management Detection and Response delivers                                                                                                                           |
|-----------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.3.1           | Vulns identified from industry sources, risk-ranked with customer-defined high/critical          | Aggregated intelligence from sources like NVD, vendor advisories, and CISA KEV, the Armis proprietary AI-powered vulnerability database (AVID), and enriched description and remediation information. |
| 6.3.2           | Inventory of third-party and open-source components                                              | Continuous inventory of all assets, including IT, IoT, OT, code, cloud, third-party, and open-source components.                                                                                      |
| 6.3.3           | Critical/high patches applied within one month of release                                        | Automated remediation workflows for AI-powered security (delivered via ServiceNow Unified Exposure Management)                                                                                        |
| 11.3.1          | Internal scans at least every 3 months; high-risk and critical vulns resolved; rescan to confirm | Internal scan and rescan evidence, continuous event-based assessment, risk scoring and validation, prioritization of high-risk and critical vulns, automatic assignment and resolution workflows.     |
| 11.3.1.1        | All <i>other</i> applicable vulns managed on a cadence justified by a targeted risk analysis     | Validated vulnerabilities with lower risk scores fed into policy-based prioritized remediation workflows.                                                                                             |
| 11.3.1.2        | Internal scans performed as <b>authenticated</b> scans                                           | Scheduled or continuous authenticated scans                                                                                                                                                           |
| 11.3.1.3        | Scan after any significant change                                                                | Continuous and event-driven assessment identify changes against an established baseline                                                                                                               |
| 12.5.1 / 12.5.2 | Accurate CDE asset inventory and annual scope confirmation                                       | Real-time asset inventory of all system components including hardware and infrastructure, cloud and virtual assets, and applications. Board-ready reporting capabilities.                             |
| 11.3.2          | Quarterly passing external scan by an ASV                                                        | Continuous Vulnerability Detection delivered via ServiceNow — pending PCI SSC listing                                                                                                                 |



### Continuous compliance starts with continuous awareness

Security teams need continuous awareness of assets, vulnerabilities, and risk exposure to maintain a resilient security posture. Armis from ServiceNow delivers a closed-loop vulnerability management program that improves security outcomes and supports PCI DSS requirements from detection through resolution

Get the big picture on today's security challenges—and how Armis helps solve them.

[Explore Armis Centrix™ Today](#)

**Armis from ServiceNow protects the entire attack surface and manages an organization's cyber risk exposure in real time.**

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

+1 888 452 4011 | [armis.com](https://armis.com)