Identifying the Problem

Any merchant, business or financial institution storing, processing and transmitting cardholder data must comply with the Payment Card Industry Data Security Standard (PCI DSS), as it was created to mitigate the risk associated with handling cardholder information. Demonstrating and maintaining PCI DSS compliance remains one of the most extensive challenges facing businesses today.

Organizations must define their risk tolerance within a sustainable compliance policy if they plan to build and maintain secure systems and applications, as is outlined in the PCI standard. Though most businesses rely on multiple scanning tools to identify vulnerabilities across different phases of the software development lifecycle (SDLC), finding the right solution to gain a comprehensive, continuous view of risk remains elusive. Further, juggling an array of scanning tools creates fragmentation among teams and muddles risk visibility, two things organizations must avoid if they hope to meet PCI DSS requirements.

Meeting the Compliance Challenge

Today, every business is in the software business, as organizations are tasked with building, maintaining and deploying bullet-proof software with minimal risk. Software development and application oversight are both critical components of the PCI standard, particularly in the context of two requirements:

Requirement 6: Develop and maintain secure systems and applications. Software must be built securely, code vulnerabilities remediated and web applications tested for security gaps.

Requirement 11: Regularly test security systems and processes. Testing for vulnerabilities (including pentesting) to remediate issues and validate corrective action is crucial.

Finding ZeroNorth

Even with a clear picture of PCI DSS compliance, identifying how technology can fit the needs of a specific environment remains critical. The ZeroNorth platform offers a broad set of capabilities to deliver application and infrastructure security, ideally suited to support PCI DSS compliance.

From AppSec to SecOps, ZeroNorth delivers a unified platform of risk-based vulnerability orchestration across the SDLC. This coordinated visibility enables companies to assess risk, prioritize critical business applications and gain the needed flexibility to rapidly onboard new testing solutions—without slowing down the pace of business.

Because the PCI requirement has identified application security as a cornerstone, the ZeroNorth platform directly impacts the ability to build, maintain and test the security of systems and products. By ingesting data from existing scanning tools, while allowing businesses to leverage current ones, ZeroNorth delivers open source scan tools to close any security gaps in scanning capabilities.
## Platform Proof Points

Find a comprehensive view of risk, as required by PCI Requirement 6:
Develop and maintain secure systems and applications, including the ability to define and produce effective PCI compliance policies.

Maintain secure systems and applications, as required by PCI Requirement 6:
Orchestration eradicates the challenge of siloed data and fragmented workflows to help create a robust cybersecurity program around security systems and applications.

Regularly test security system and processes, as required by PCI Requirement 11:
Remove fragmented workflows between teams and regularly test security systems and processes through practical assessment and mitigation of risk.

Accurately assess threats, as required by PCI Requirement 11:
Automation within vulnerability orchestration empowers businesses to consistently implement and manage project workflows across individual discovery tools.

### PCI-DSS Requirement (AppSec-specific)

| Req. 6.3 | Develop software applications following best practices and incorporating security through the SDLC |
| Req. 6.3.2 | Review custom code prior to release to production to identify and remediate vulnerabilities |
| Req. 6.5 | Address common coding vulnerabilities during the software development process |
| Req. 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis, leveraging vulnerability security assessments |
| Req. 11.3 | Implement penetration testing, both inside and outside the network |

### AppSec Activity (ZeroNorth capabilities)

| Orchestrates scanning tools leveraged across the SDLC and enables customers to quickly identify and remediate high-risk vulnerabilities. Open source tools (e.g., SCA, SAST, DAST) embedded directly into the platform fill security gaps in a scanning portfolio. |
| Ingests data from commercial SAST tools and orchestrates them to ensure custom code is secure. SCA tools may be leveraged to verify the security of open source components. Open source scanning tools (e.g., SCA, SAST, DAST) embedded in the platform enable customers to fill potential gaps in their scanning portfolio. |
| Ingests data from commercial web application vulnerability scanning tools and allows customers to continually orchestrate with open source tools to identify vulnerabilities in web applications and jump-start key initiatives. |
| Ingests, correlates and prioritizes results from various penetration testing tools, as well as third party manual test results. |

Learn how your organization can meet PCI compliance and reduce risk.
Contact [secure@zeronorth.io](mailto:secure@zeronorth.io) for more information or to request a demo.