LEARNING THE LANDSCAPE

While the security associated with cardholder data has improved, we continue to see breaches resulting in compromised data. Clearly, many organizations today still struggle with how to protect this sensitive information.

As a result, major credit card companies, such as VISA, Mastercard and American Express, created the Payment Card Industry Data Security Standard (PCI DSS), a set of requirements for any organization—regardless of size and scope— that transmits or stores cardholder data, with the goal of mitigating risk associated with these digital transactions and the data loss incurred.

If your business stores, processes or transmits cardholder data in any way, PCI DSS applies to you. But even with the right security controls in place, businesses still struggle with how to both demonstrate and maintain PCI DSS compliance over time. To ensure your organization is on the right track for compliance, ask yourself:

1. What security measures are you taking now, and where are your compliance gaps?
2. How can you fix these vulnerabilities to protect sensitive cardholder data?
3. What evidence do you have that your controls are in place and working effectively?

If you cannot answer these compliance questions with confidence, it is time to consider a PCI solution from ZeroNorth, the security industry's first provider of risk-based vulnerability orchestration across applications and infrastructure. PCI DSS compliance is a big ask, but a necessary one.

Bolster a comprehensive cybersecurity program

Identify, prioritize and remediate vulnerabilities across the SDLC

Manage vulnerability testing requirements by identifying and remediating issues

Integrate security and DevOps tools across the SDLC to achieve accurate reporting

Consistently implement and manage project workflows across individual discovery tools

Challenge

Today, every business is in the software business, which means organizations are now tasked with building, maintaining and deploying bullet-proof software with little to no risk. And, software development and application oversight are critical components of the PCI standard, particularly in the context of two requirements:

> Requirement 6: *Develop and maintain secure systems and applications.*
> Requirement 11: *Regularly test security systems and processes.*

To earn, maintain and demonstrate PCI DSS compliance, all companies associated with card payments must adhere to a robust information security policy put in place to develop and maintain secure systems and applications. This effort to protect stored data directs organizations to ensure software is built securely, vulnerabilities in code are remediated and security systems and processes are regularly monitored and tested. This is easier said than done. Large organizations with distributed application development teams still struggle to maintain a consistent, continuous view of risk across the software development lifecycle (SDLC). Disparate workflows among security and development teams can make collaboration difficult and significantly impact an organization's ability to demonstrate PCI DSS compliance to both internal and external auditors.

Solution

To protect themselves and their customer data, while also complying with the PCI requirement, organizations today need one thing—visibility. The ZeroNorth solution addresses this need by delivering a unified platform of risk-based vulnerability orchestration across applications and infrastructure. This level of coordinated visibility enables businesses of all sizes to assess risk, prioritize critical business applications and gain the needed flexibility to rapidly onboard new testing solutions—all without slowing down the pace of business.

Because the PCI requirements have identified application security as one of its cornerstones, the ZeroNorth platform directly impacts an organization's ability to build, maintain and test the security of their systems and products. ZeroNorth ingests data from existing scanning tools, allowing businesses to leverage what they currently have, and delivers open source scan tools to close any gaps in scanning capabilities, thus providing the visibility organizations need to identify and prioritize risk.

Orchestration across the SDLC empowers businesses to create the type of strong cybersecurity program they will need to sidestep issues of siloed data and fragmented processes, without wasting time and money. Even if your business already has a clear picture of what the scope of PCI DSS compliance looks like, it is critical to identify how technology can meet your needs, in your specific environment, with a matrix of security tools—like those offered by ZeroNorth.

Learn how your organization can meet PCI DSS compliance and reduce risk.
Contact secure@zeronorth.io for more information or to request a demo.