RSI | Datasheet

PCI Approved

Scanning Vendor (ASV)

A PCI Approved Scanning Vendor (PCI ASV) is a company accredited by the PCI Security Standards Council (PCI SSC) to conduct vulnerability assessment scans required by PCI DSS. These scans help businesses that store, process, or transmit payment card data identify security weaknesses in their systems, applications, and network infrastructures. By simulating cyberattacks, PCI ASVs test security defenses and pinpoint vulnerabilities that could be exploited by attackers. To become certified, vendors must undergo a rigorous qualification process, ensuring their scans meet PCI SSC standards. Engaging a PCI ASV is essential for maintaining compliance, securing payment data, and preventing breaches.

PCI ASV Scanning Requirements

A PCI VA scan identifies external network vulnerabilities to help businesses meet PCI compliance requirements. This mandatory scan is essential for payment processors, banks, merchants, and service providers handling payment card data. Partnering with a compliance expert who uses the appropriate PCI DSS scanning tools for your IT environment is crucial. Failure to comply with PCI DSS ASV requirements can result in fines, restrictions, or loss of payment processing capabilities. Regular PCI ASV scans are necessary to ensure your PCI certification remains secure.

01 Regular Scanning

Scans must be conducted at least quarterly and after any significant changes to the network, such as new system components or major configuration changes.

02 Scope Definition

The scan must cover all external-facing IP addresses and domains that are involved in the processing, storage, or transmission of cardholder data.

03 ASV Compliance

Scans must be performed by an Approved Scanning Vendor (ASV) certified by the PCI Security Standards Council (PCI SSC).

04 Methodology

The scanning process should follow the PCI SSC's approved scanning procedures, ensuring a thorough and standardized approach.

05 Reporting and Remediation

A detailed report must be generated, highlighting any vulnerabilities detected. Organizations must address these vulnerabilities and perform rescans to confirm remediation.

06 Documentation

All scanning activities and results must be documented and retained for at least one year for audit purposes. This includes maintaining records of scan reports, remediation actions, and any correspondence with the ASV.

RSI Security's PCI ASV Services

Our experienced technical and account management staff will work closely with you throughout the PCI vulnerability scanning process to ensure optimal outcomes and success.

PCI VA Reports: Your Tool to Strengthening Your Cybersecurity

When RSI Security generates a PCI technical report, it serves two key purposes: confirming compliance and identifying security gaps. These reports provide critical insights to help businesses address vulnerabilities and maintain PCI DSS compliance.

Key Features of RSI Security's PCI Technical Reports:

- **Detailed Vulnerability Analysis** – Identifies security weaknesses, their risk levels, affected systems, and relevant PCI DSS requirements.
- **Prioritized Remediation Steps** – Provides clear guidance on addressing vulnerabilities based on severity to mitigate risks efficiently.
- **Supporting Evidence** – Includes screenshots, logs, or other documentation to help understand the scope of security issues.
- **Compliance Certification** – Confirms that the organization met all PCI and ASV scan requirements at the time of the assessment.
- **Ongoing Security Management** – Helps establish a baseline for continuous monitoring and proactive vulnerability remediation.

Get Started on Your PCI ASV Scanning Today

Don't let PCI compliance be a roadblock for your business. Let RSI Security guide you through the process with expert scanning, thorough reporting, and comprehensive support. Start your journey toward PCI compliance with a PCI vulnerability scan from RSI Security.

To learn more about RSI Security's PCI ASV services, get in touch today!

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com