PCI Security Standards Council

APPROVED SCANNING VENDOR™

# PCI ASV SCANNING SERVICES BRIEF

*Certified Scanning. Clear Results. Confident Compliance.*

SPECIALIZED S|3 SECURITY SERVICES

# VULNERABILITY SCANNING SERVICES

***Certified PCI scanning, built for compliance without confusion.***

PCI DSS requires both external and internal vulnerability scans to validate the security of systems that store, process, or transmit cardholder data. External scans must be performed by a PCI-certified Approved Scanning Vendor (ASV) to meet compliance standards. Beginning with PCI DSS version 4.0, internal scans must be authenticated, meaning the scans must be conducted using credentialed access to identify deeper system flaws and meet compliance expectations.

S3 Security is one of only 76 certified ASVs in the US and 85 worldwide. We deliver certified results, help your team interpret findings, and guide you through remediation and rescan, so you can meet PCI requirements with clarity and confidence.

## EXPERTISE YOU CAN TRUST

With over 25 years of cybersecurity experience, S3 Security supports PCI compliance efforts across a wide range of industries and environments. As both a certified ASV and Qualified Security Assessor (QSA) company, with multiple QSAs on staff, we bring deep insight into PCI DSS requirements. Our scans are aligned to the latest PCI DSS version to deliver results that meet industry standards and are ready for submission.

## TAILORED TO YOUR BUSINESS

PCI DSS requires organizations to define the scope of internet-facing systems subject to scanning. S3 Security helps you validate that scope, coordinate access, and reduce operational complexity. Whether scanning one location or hundreds, our team ensures a smooth, certified process aligned to your unique environment.

## CERTIFIED RESULTS, READY FOR PCI

Our ASV scanning services go beyond the scan itself. We deliver PCI-ready reports, formatted for submission to acquiring banks, payment processors, or internal stakeholders. We also support your team through the full lifecycle: including guidance on scan disputes, remediation, rescans, and attestation to help you stay compliant and avoid delays.

***We simplify PCI scanning so your team can stay focused, informed, and compliant.***

# CERTIFIED EXPERTS & PROVEN TOOLS

Executives across industries rely on S3 Security for PCI scanning services that are both certified and dependable. As a PCI-certified Approved Scanning Vendor (ASV) and Qualified Security Assessor (QSA) company, we offer unmatched insight into PCI DSS requirements, helping you meet compliance obligations with confidence.

Our ASV team uses trusted tools, proven methods, and a defensible approach to deliver accurate, prioritized results that are ready for submission with clarity and confidence.

## FRAMEWORKS & METHODOLOGIES

Our ASV services align with PCI DSS scanning standards and reporting requirements. Every scan we deliver is:

- **Certified** to meet PCI DSS external vulnerability scanning requirements
- **Evidence-based**, using CVSS scoring and PCI-defined pass/fail criteria
- **Consistently formatted**, with documentation ready for assessor review or internal submission

We also support scan disputes, remediation validation, and rescans to help ensure compliance.

***Our certified ASV team delivers clear, credible results that meet PCI DSS expectations and support compliance oversight.***

# TECHNICAL CAPABILITIES

S3 Security delivers certified PCI ASV scanning services to help your organization meet compliance requirements with confidence. Our experienced team conducts both external and internal vulnerability scans—covering public-facing websites, web applications, and systems in cloud or hybrid environments—using approved tools and certified ASV engineers.

We follow the latest guidance from the PCI Security Standards Council and continuously adapt to evolving requirements, so your results are accurate, defensible, and ready for submission.

## External Vulnerability Scanning

We scan internet-facing systems for vulnerabilities such as unpatched software, open ports, insecure configurations, and weak encryption protocols. These scans are required every 90 days and after any significant change to systems in scope.

## Internal Vulnerability Scanning

Internal scanning identifies weaknesses behind the firewall, such as missing patches, legacy systems, and insecure configurations. These scans help prevent lateral movement within your network and are a key part of PCI DSS validation, especially for segmented environments.

## Cloud Vulnerability Scanning

We assess cloud-hosted environments for exposure risks, configuration weaknesses, and compliance alignment. Scans include authentication where applicable and provide insight into dynamic cloud assets that may otherwise go unnoticed in traditional scans.

## URL / URI / FQDN Scanning

We assess externally accessible Fully Qualified Domain Names (FQDNs), URLs, and URIs that store, process, or transmit cardholder data to identify risks like exposed admin interfaces, outdated software, and insecure default configurations. These assessments help ensure your web infrastructure doesn't become a pathway to data exposure.

## Application-Layer Scanning

Application-layer scans evaluate how your web applications handle sessions, inputs, and access controls. We identify risks aligned with the OWASP Top 10, including injection flaws, authentication issues, and misconfigurations, and can simulate authenticated user behavior when required.

## API Scanning

We evaluate exposed APIs for vulnerabilities such as injection flaws, broken authentication, and improper access controls. Our scans align with OWASP API Security Top 10 and provide detailed findings to support remediation.

## Compliance-Ready Reporting

We deliver PCI-approved ASV reports with pass/fail status, severity rankings, remediation guidance, and executive summaries formatted for submission to assessors, acquirers, or processors. Our team also supports scan validation, rescans, and dispute resolution when needed.

***Certified PCI scanning to reduce risk, simplify compliance, and keep your organization moving forward with confidence.***

# OUR VULNERABILITY SCANNING METHODOLOGY

Certified PCI scanning demands more than automation. It requires precision, documentation, and a deep understanding of compliance requirements. Our structured ASV scanning methodology helps your team meet PCI DSS standards with minimal disruption and maximum clarity.

1

## Scope Confirmation & Planning

We begin by validating your scan scope in alignment with PCI DSS. This includes all required internal and external components, such as IP ranges, domains, and web applications. Scan timing is coordinated to reduce operational disruption.

2

## ASV Scanning

Certified ASV engineers conduct vulnerability scans in accordance with PCI DSS and ASV Program requirements. We identify high-risk vulnerabilities, outdated components, insecure configurations, and exposed services.

3

## Review & Risk Validation

We validate results using CVSS scoring and PCI-defined pass/fail status. Each finding is reviewed for accuracy and severity, and prioritized remediation guidance is provided to help your team take informed action.

4

## Initial Reporting

We deliver clear, organized reporting aligned with PCI DSS and your internal needs. Deliverables include an Executive Summary, Detailed Findings with remediation guidance, and a Scan Workbook for technical teams. All reports are formatted to support effective remediation and planning, helping your team address findings ahead of quarterly rescans and final AOSC submission.

5

## Rescanning & Attestation

Once remediation is complete, we perform a rescan to confirm that all required vulnerabilities have been addressed. If results meet PCI DSS pass criteria, we issue an Attestation of Scan Compliance (AOSC) to support your PCI compliance evidence package.

***Effective PCI compliance starts with certified scans, clear guidance, and structured execution you can trust.***

# MEASURING WHAT MATTERS

## What Does a Scan Reveal?

Certified ASV scans identify vulnerabilities, such as outdated software, exposed services, and insecure configurations, that attackers could exploit to access cardholder data. While these issues may not be actively exploited, they create clear risk pathways. Timely detection and remediation help reduce risk, protect sensitive data, and support PCI DSS compliance.

## Risk Severity Ratings

Under the PCI ASV Program, vulnerability severity determines both pass/fail status and how urgently remediation must be addressed. We follow the Common Vulnerability Scoring System (CVSS v3), assigning each vulnerability a risk level based on its score and business impact. This framework helps your team prioritize remediation efforts and streamline compliance with PCI DSS.

| Risk Level | NVD CVSS v3 | Definition |
|---|---|---|
| **High** | 7.0–10.0 | Immediate, system-wide risk with potential for full compromise and data loss. Often systemic in nature. |
| **Medium** | 4.0-6.9 | May lead to sensitive data exposure or administrative access when combined with other weaknesses. Often requires elevated privileges or chaining to exploit and may result in moderate to serious business impact. |
| **Low** | 0.0–3.9 | Minimal risk. Low impact issues or informational findings for awareness and best practices. |

***Know the impact. Prioritize what matters.***

Your ASV report clearly categorizes vulnerabilities by severity and business relevance. Each report includes actionable remediation guidance to help your team resolve failures efficiently and stay on track for timely PCI DSS submission.

# A BETTER SCANNING EXPERIENCE

At S3 Security, we understand that how your PCI ASV scans are managed has a direct impact on your compliance success. That's why we provide a dedicated engagement team to keep your scanning program organized, transparent, and on track, so your team can stay focused on operations, not paperwork.

**What You Can Expect:**

- A dedicated Client Administrator (CA) to oversee scheduling & coordination
- Proactive communication from kickoff through reporting
- Clear expectations & timelines for each scan
- Scope & IP address submission guidance
- Ongoing reminders to support compliance deadlines

From agenda calls to report delivery, every step is designed to ensure a smooth, transparent, and high-quality experience.

## BUILT-IN QUALITY ASSURANCE

Our QA process ensures each report meets PCI SSC expectations and supports your internal review process. Every deliverable is reviewed for accuracy, completeness, and submission readiness.

**S3 Security QA Process:**

- **Engineering QA** – Validation by certified ASV Engineer
- **VP Review** – Review for completeness and content structure
- **Executive Review** – Final approval by EVP/CTO
- **Delivery QA** – Final check by Business Operations prior to delivery

***Every ASV report we deliver is held to the highest standard: accurate, defensible, and ready for submission.***

# WHAT TO EXPECT DURING YOUR PCI ASV SCANNING ENGAGEMENT

***Consistent scanning. Clear timelines. Confident compliance.***

We manage PCI ASV scanning with a structured quarterly process designed to reduce stress and maintain compliance. From initial discovery to final reporting, our certified ASV engineers and delivery team support you with clear timelines, validated deliverables, and proactive scheduling to keep your organization on track.

## QUARTERLY ASV SCAN TIMELINE & DELIVERABLES


### Your Scan Support Team

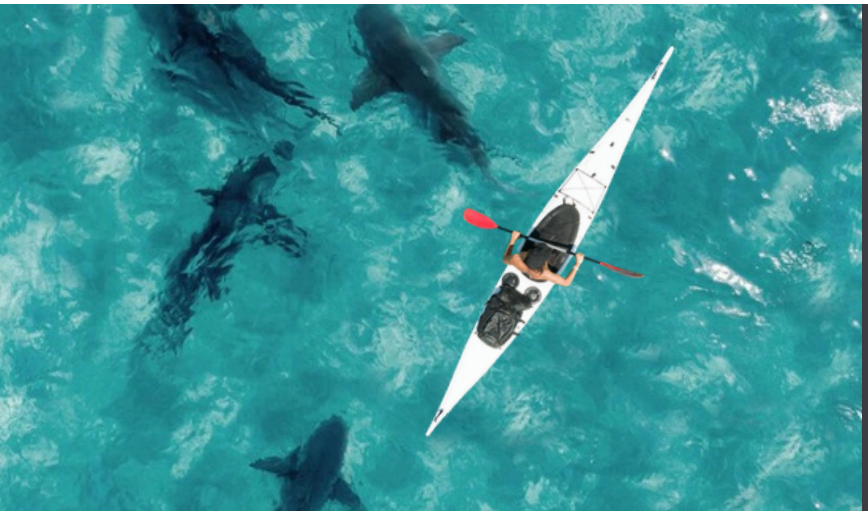
Each engagement is guided by a cross-functional team:

- **Client Administrator:** Coordinates schedules and logistics
- **ASV Engineers:** Perform certified internal and external scans
- **Delivery Team:** Finalizes deliverables including the AOSC

Every step is built to reduce disruption, increase visibility, and give you clarity on timelines, deliverables, and what happens next.

***Clear roles. Smooth execution. Strong results.***

# YOUR CYBERSECURITY PARTNER



S|3 SPECIALIZED SECURITY SERVICES

## FLOAT ON

Cybersecurity and compliance to ward off any threat.

### *Wherever You Are in Your Compliance Journey, We're With You*

Whether you're preparing for your first PCI ASV scan or looking to streamline a quarterly scanning program, S3 Security is here to help. We simplify complexity and keep your team informed, organized, and ready to report.

Our mission is to help you maintain PCI compliance without disruption, reduce risk exposure, and strengthen your readiness with scanning strategies tailored to your business.

With over 25 years of experience and certified ASV engineers and QSAs on staff, S3 Security is your trusted partner for PCI-approved scans, executive-ready reporting, and defensible results you can submit with confidence.

PCI Security Standards Council

APPROVED SCANNING VENDOR™

**CONTACT US**

972-378-5554 | info@s3security.com | www.s3security.com

4975 Preston Park Blvd. Ste. 500
Plano, TX 75093