Call us on 01924 284 240

Sec-1 Ltd - Approved Scanning Vendor

Expert Service for compliance with the PCI DSS

Scan your card data environment, provide a passing scan. Sounds easy. So why is it so difficult to get a passing scan?

Experience shows that a key factor is your relationship with the Approved Scanning Vendor. ASV's have become automated, distant and remote with confusing support channels.

We've worked hard at Sec-1 to provide an ASV service with a human touch.

Each report is reviewed by an ASV Engineer, false positives removed and through your Account Manager you have direct access to technical expertise for remediation advice.

By combining our leading PCI DSS scanning tool with manual hands-on management you reduce the risk of reporting false positives and inaccurate vulnerabilities.

Most importantly, the SEC-1 ASV service makes passing scans easy.

PCI DSS external vulnerability scans are conducted over the Internet by Sec-1 Ltd, as a remote service that requires scanning from a source external to your network.

Sec-1 Ltd ASV Employees take a hands-on approach to ensure that everything that can be done is done to arrive at a compliant solution in the context of your environment. From Scoping to Reporting, we work very closely with you and your team to ensure the starting point is accurate and that corrective actions are properly communicated and implemented.

ASV Scanning Process

The main phases of the scanning process are:

Scoping
Accurate scope is crucial to obtaining a compliant scan. Our guidance will help you ensure this is correct.

Scanning
Scanning quality has been validated by the PCI SSC. Further information can be found overleaf.

Reporting/Remediation
Interim reports are presented should a scan not pass first time.

Dispute Resolution
Technical understanding of our engineers will ensure that any disputes are validated.

Rescan
Unlimited rescans are included in the licensing model. Rescans will be required to arrive at a passing scan. Support services will be available to help you understand the results.

Final Reporting
A report will be sent on completion of a passing scan. This report is to confirm that the target is free from vulnerabilities rated 4 or higher on the CVSSv2 scale, and/or that compensating controls have been applied that mitigate vulnerabilities which can not be remediated.

Key Benefits...

Low cost
Competitively priced per IP address per quarter.

Qualified Personnel
Engagements are fulfilled by qualified, highly skilled, and experienced security engineers.

Maximum Quality
Our engineers use a combination of manual and automated techniques to maximise the quality of your service.

Customer Support
Assistance will be provided to scan customers to:

- Advise on the recommended scope based on current network architecture
- Prioritise the solution and mitigation of identified issues
- Apply corrective actions in line with the PCI DSS

PCI DSS v3—Requirement 11.2.2

Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).

Address Sec-1 Limited, Unit 1 Centre 27 Business Park, Bankwood Way, Birstall, West Yorkshire, WF17 9TB
Telephone 01924 284 240 • **FAX** 01924 284 241 • **Email** info@sec-1.com • **Website** www.sec-1.com

Technical Competence

Sec-1 employs a best-of-breed network infrastructure vulnerability scanning engine in tandem with our in-house developed Web Application scanner - which identifies all Web Application Vulnerabilities within the OWASP Top Ten List as required by the PCI SSC.

Discovery Scanning

Accurate & efficient component discovery (crawling) is commonly cited as one of the key challenges when performing a vulnerability scan of infrastructure and web applications.

Our web application scanner employs an innovative crawling system that automatically renders each webpage within a web browser engine allowing the scanner to identify targets in modern HTML5 web applications, something missed by many other scanners.

Vulnerability Identification

Built on decades of penetration testing experience, our Web Application scanner performs a large number of high risk vulnerability tests to identify issues including:

- SQL Injection
- XML External Entity Injection
- Command Injection
- Reflected, Stored and DOM-Based Cross Site Scripting
- Insecure Direct Object Referencing
- Unvalidated Redirects & Forwards, and more

In addition, Sec-1 regularly update the scanning engine with plugins for new vulnerabilities identified by Sec-1 penetration testers and other security researchers.

False Positive Management & Vulnerability Exploitation

To reduce false positives and to provide proof of concept evidence, our service uses safe exploitation techniques to proactively confirm discovered vulnerabilities.

Additional Services

ASV-Led Scoping

We often find organisations mistakenly identify which services are in-scope for ASV Assessment, leading to overly onerous and costly scans being performed on systems which are not required to be in scope; or alternatively, not including all relevant systems within scope potentially leaving you exposed to vulnerabilities which can affect your ongoing compliance.

Sec-1 uniquely offers an ASV-led scoping service which will help you ensure all relevant systems and web applications are included within scope.

PCI DSS Qualified Security Assessors

As well as offering ASV services Sec-1 provides complementary services for partial or complete delivery of PCI DSS Compliance.

Our services include:

- Gap Analysis
- PCI DSS Implementation and Remediation
- Telephone Consultancy
- Policy and Procedure Preparation and Review
- Penetration Testing
- Training & Staff Awareness Training
- Compliance Audit and Report On Compliance
- Validation and SAQ Completion/QSA Sign-Off
- Maintenance, Monitoring and Continual Review

PCI DSS 11.3 Penetration Testing

We offer penetration testing services to satisfy Requirement 11.3 for Internal and External, Network and Application Level Penetration Testing.

With vast experience, our CREST and CHECK Accredited Penetration Testers will assess your network, mobile, and web platforms and your Cardholder Data Environment for technical vulnerabilities. We include reporting and remediation services so that fixes are applied and validated as required by the PCI DSS.

Who should use an Approved Scanning Vendor?

Requirement 11.2.2 applies to all Merchants & Service Providers that are required to complete a Report on Compliance (RoC). It does not, however, apply to ALL merchants that are Self-Assessment Questionnaires (SAQ) eligible. The following table details where 11.2.2 applies.

SAQ	Overview
A-EP	Applies to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.
B-IP	Applies to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor.
C	Applies to merchants whose payment application system (e.g. point-of-sale systems) are connected to the internet (for example, via DSL, cable modem, etc.).
D	Applies to SAQ-eligible merchants not meeting the criteria of any other SAQ type.
D	Applies to all service providers defined by a payment brand as being SAQ-eligible.

Free Consultancy

Don't know if you need an ASV Scan?

If you are not a Level 1 Merchant or a Service Provider and are unaware of the SAQ which should be completed — and thus whether ASV scanning or Penetration Testing applies to you; you can arrange a free call with one of our Qualified Security Assessors.

Call us now on 01924 284 240 to arrange.

Address Sec-1 Limited, Unit 1 Centre 27 Business Park, Bankwood Way, Birstall, West Yorkshire, WF17 9TB
Telephone 01924 284 240 • **FAX** 01924 284 241 • **Email** info@sec-1.com • **Website** www.sec-1.com