edgescan™

DATASHEET

PCI Approved

Firms that authorize online transactions have certain information-security obligations under the law. Edgescan will partner with your team to strengthen your security posture beyond full regulatory compliance, building a cutting-edge defense for your web-facing assets.

The Baseline

The Payment Card Industry Security Standards Council (PCI SSC) has established a number of requirements for firms that process financial transactions via web-facing applications. Organizations are obligated by law to establish a robust security posture in order to defend against cyber threats and safeguard customers' personal information, including credit card details and cardholder data.

The longtime core requirement is 11.2.2: firms must undergo Quarterly Vulnerability Scanning by a PCI SSC Approved Scanning Vendor (ASV). If significant issues are identified, continual rescanning is necessary until no vulnerabilities rated 4.0 or higher by the CVSS are present.

Evolving Demands

The PCI SSC has updated the regulatory framework for firms processing payments online to keep pace with the evolving threat environment and advancements in information-security tools. From March 31, 2024, the requirements have grown to include:

- 11.4.2 and 11.4.3, which mandate an **Annual Penetration Test** on both internal and external Cardholder Data Environments (CDEs), as well as additional pen tests following significant changes to infrastructure or applications.
- 11.4.4, which holds that organizations must achieve **Verification of Remediation** by conducting repeat testing to certify the effectiveness of corrective actions.
- The regulations also advocate for a **Risk-Based Approach** to prioritizing remediation efforts.

Scan Compliance

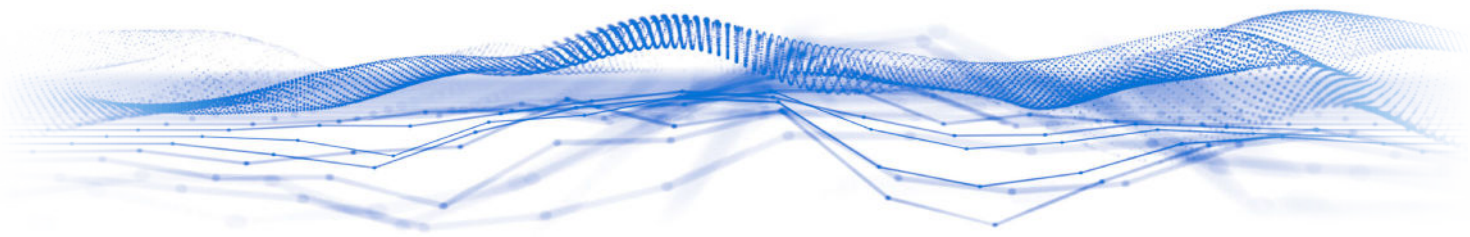
Edgescan is recognized as a PCI SSC Approved Scanning Vendor (ASV), which designates a firm that conducts external vulnerability scanning services and validates a payment processor's adherence to the scanning requirements of PCI DSS. The Edgescan solution has been fully approved for PCI ASV scanning across all geographies, and Edgescan is ISO27001-certified to handle you and your customers' information with the utmost care.

Continuous Compliance

Edgescan will probe your web-facing applications, network, and more to ensure your PCI compliance requirements are met and that you pass your quarterly scan, but many of our clients require the flexibility of conducting ASV scans themselves. Instead of once per quarter, they may choose to run them daily, weekly, or on a more ad-hoc basis.

The award-winning Edgescan dashboard allows clients to initiate scans on-demand, and the results are consolidated in a single interface to allow for a more efficient and holistic approach to maintaining PCI compliance. Once the report on a system's vulnerabilities is compiled, our expert penetration team is available to advise you on what course of action is required to pass your quarterly assessments.

The platform also incorporates a guided remediation process with a variety of risk-rating tools to assist your internal security team in prioritizing the most critical threats for immediate remediation, per PCI guidance. When a vulnerability is marked as resolved in the Edgescan dashboard, a team of CREST- and OSCP-certified experts is on hand to probe that asset and verify the remediation, thereby satisfying Requirement 11.4.4.



Seamless Service

The Edgescan solution is tailored to snap into and enhance your existing security model. With that in mind, it involves:

No Agents or Software Installations: Edgescan ASV does not use agents or require you to install software to perform our scanning service.

No Disruptions: When conducting a scan, Edgescan ASV does not interfere with the cardholder data system.

Production-Safe Testing: Edgescan will deliver precautionary assessments of planned activities to help ensure we do not cause outages.

Flexible Schedules: Edgescan offers automatic scheduling for required quarterly scans, or you can scan as often as you'd like to identify and remediate vulnerabilities on a rolling basis.

24/7 Support: Leverage round-the-clock chat, email, or telephone support to understand and address issues. Maintain your coverage across all web-facing assets, be it on-site or via public, private, or hybrid cloud infrastructure.

Dev Support: Scan your web applications during and after development to ensure they're securely built and securely maintained.

Beyond Compliance

But the standout factor is that Edgescan ASV reports do not just satisfy PCI-ASV standards, they clear the bar with plenty of room to spare.

The Edgescan ASV solution is powered with the same logic as the award-winning Edgescan continuous security testing and exposure management SaaS platform, which is used by some of the world's largest and best-known enterprises. Clients who operate a continuous compliance model use the full Edgescan service, as it has the added flexibility of running unlimited scans for the same fixed annual cost.

The regulatory framework surrounding online payment processing will continue to evolve, but regular penetration testing is now the industry standard for high-risk web-facing assets and those of critical organizational importance, as are risk prioritization tools that help security teams to govern the remediation process. Verification of remediation is also essential for any internal security team seeking full confirmation that they've addressed a system vulnerability.

The Edgescan platform provides all these elements of PCI compliance as a baseline, then offers another level of insight into your attack surface—from the network level to web-facing applications to APIs and more—to help you build a cutting-edge security framework that represents the industry standard of tomorrow.

For more information on how Edgescan can help secure your business, contact: *sales@edgescan.com*