DATA SHEET

PCI ASV: A Managed Vulnerability Service Add-On

Simplify your quarterly PCI vulnerability scanning.

Your organization needs to be able to process credit card data to achieve revenue objectives, which means adherence to the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS includes a requirement to pass a quarterly external assessment from an Approved Scanning Vendor (ASV). Already challenged with tracking and remediating vulnerabilities in an increasingly complex threat landscape, compliance with PCI DSS is an added layer your team must address. Integrate and simplify your PCI compliance process with PCI ASV, a Managed Vulnerability Service add-on.

STREAMLINED SCANNING

Pre-configured, quarterly PCI scanning templates of externally facing PCI assets facilitate easy execution.

EFFICIENT REMEDIATION

The ASV dispute resolution and remediation process runs in compliance with PCI DSS 11.2.2.

DEDICATED EXPERTISE

Dedicated Managed Vulnerability Service experts act as an extension of your team, lessening the stress on internal resources.

67% of respondents said non-compliance with PCI DSS Requirement 11 was a contributing factor in breaches[1]

73% of breached organizations did not have PCI DSS requirement 11 implemented at the time of breach[1]

FEATURES

Management of the Approved Scanning Vendor (ASV) process
Dedicated security experts manage the majority of the PCI ASV process on your behalf.

Attestation and reporting preparation
Final attestation and reporting for quarterly external vulnerability scans are prepared by eSentire's dedicated Managed Vulnerability Service team.

Ongoing visibility of ASV disputes
Gain visibility into results and disputes organized as unassessed, assessed, passed or failed, as well as additional information needed.

Unification of vulnerability management and PCI DSS 11.2.2 compliance
Manage IT asset vulnerabilities and PCI attestations on a single platform.

[1] *2018 PCI DSS Data Breach Trends – Security Metrics*

BENEFITS

- Meet PCI compliance requirements
- Minimize the vulnerability associated with the discovery-to-remediation timeframe
- Improve scanning consistency, timeliness and confidence
- Alleviate demand on internal security and compliance resources
- Reduce technology solution sprawl
- Create operational efficiencies

Approved Scanning Vendor Process Responsibility Checklist

The PCI Security Standards Council divides the ASV process into phases that are featured in the chart below. eSentire's dedicated Managed Vulnerability Service team manages the majority of the ASV workflow on your behalf.

	Typical Managed Security Service Provider (MSSP)	eSentire
Scoping		
Identification of assets within network	✗	✓
Configuration and setup for scanning	✓	✓
Scanning		
Perform scans on behalf of the client	✓	✓
Initial Reporting/ Remediation		
Interpretation of scan results	✗	✓
Patching/remediation	✗	✗
Dispute Resolution	✗	✓
Rescan (as needed)	✗	✓
Final Reporting		
Prepared PCI compliance attestation	✗	✓
Prepared ASV scan report summary	✗	✓
Prepared ASV scan vulnerability details	✗	✓

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**