

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.

The benefits of PCI ASV: A Managed Vulnerability Service add-on includes:

- ✓ 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

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.

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.

	eSentire	Typical Managed Security Service Provider (MSSP)
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	✓	✗

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.