LevelBlue

SOLUTION BRIEF

LEVELBLUE CONSULTING

LevelBlue Vulnerability Scanning Service (VSS)

Address Your ASV Scan Requirement for PCI DSS and Reduce Cyber Risks

Simplify and Accelerate PCI DSS Compliance

PCI DSS compliance is critical for any organization that handles credit card or other types of payment card data. Failure to comply can result in penalties and fines. Even worse, a data breach resulting from non-compliance could cost millions in settlements, legal fees, and loss of reputation.

One of the core mandates, PCI DSS 11.2, requires external vulnerability scanning by a PCI DSS Approved Scanning Vendor (ASV)—LevelBlue is an ASV.

Now, LevelBlue can help organizations of any size to meet these scanning requirements for PCI DSS:

- External quarterly vulnerability scanning, which must be performed by a PCI DSS Approved Scanning Vendor (ASV)
- Internal and external scanning as needed after significant changes in the network

Beyond Compliance

True risk reduction is something organizations of all sizes struggle with due to a variety of reasons, including:

- A lack of expertise or systematic, automated processes for vulnerability management
- Very little to no network context or up-to-date threat intelligence
- Too many vulnerabilities to address with limited resources
- Poor prioritization due to a "patch everything all the time everywhere approach" that's based only on CVSS severity ratings

These challenges are not insurmountable if you have the right people, processes, and technology.

How It Works

Meet PCI DSS Scan Requirements
Rapidly scan systems and applications to meet PCI DSS vulnerability scan requirements using the LevelBlue Vulnerability Scanning Service. Scan all internet-facing networks and systems to identify vulnerabilities and security weaknesses, with less than one percent false positive rate.

Benefits of LevelBlue Vulnerability Scanning Service

- Rapidly scans external systems and applications to quickly identify vulnerabilities and security weaknesses that put assets and data at risk
- Get expert remediation guidance from LevelBlue consultants with specific sector experience
- Better understand your organization's attack surface and help improve your organization's cybersecurity posture through ongoing risk reduction
- Be audit-ready faster by consolidating audit planning, data collection, and reporting for PCI DSS vulnerability scan requirements
- Help to stay in compliance between audits by simplifying and automating vulnerability scanning and remediation
- Validate and document vulnerability patching

Automate Quarterly ASV Network Scans
Provides for continuous compliance by automatically scheduling quarterly ASV network vulnerability scans. Scan as needed per network changes, such as new system component installations, changes in network topology, firewall rule modifications, or product upgrades.

Document Vulnerability Patching
Show that you have identified and remediated high risk vulnerabilities in a timely manner and are mitigating the ongoing risks of medium- and low-severity vulnerabilities that could be exploited in the future.

Improve Vulnerability Management
Simplify and accelerate internal policy and regulatory compliance adherence by consulting a LevelBlue industry expert who can provide guidance on meeting corporate security policies and specific cybersecurity regulations, including PCI DSS.

By pairing LevelBlue VSS and LevelBlue USM Anywhere internal scanning, we give organizations the ability to comprehensively scan their network and identify exposures and security weaknesses—including in on-prem and multi-cloud environments. Experienced LevelBlue consultants help to establish the scope and schedules for scans. They then provide customized guidance for vulnerability prioritization and remediation, based on industry best-practices. Once a clean scan is achieved, LevelBlue will provide an "attestation of compliance," for PCI DSS if it's needed. This unique combination is the secret sauce that makes it possible for organizations to help realize true risk reduction over time and to maintain ongoing continuous compliance.

Work with Security Experts
Work closely with an experienced LevelBlue consultant to establish the proper scope for objectives and PCI scan targets. During the scan and re-scan process, a LevelBlue consultant provides for alignment with scanning timeframes and target scope. Receive an "attestation of compliance" when a clean scan is achieved.

Scan Web Applications
Quickly identify critical vulnerabilities and common misconfigurations by performing extensive testing of web applications against industry best practices. Help provide that custom-built, in house, and commercial web apps are built and maintained securely.

Centralize ASV Scan Reports
Quickly view vulnerability scan results and analyze data to report on your network's security posture and plan for mitigation of risks. Easily access your ASV Scan Report Executive Summary (report follows the PCI Approved Scanning Vendor Program Guide).

Manage ASV Scan Costs
Select the solution that meets your requirements and budget. Choose from annual service options for quarterly or on-demand scanning, based on your network's size and organization's scan needs.

VULNERABILITY SCANNING SERVICE (VSS)

TYPE OF TESTS*	TECHNOLOGIES TESTED
Authentication services such as RADIUS and Kerberos Backdoors and remote access applications Backup applications Database servers DNS (Domain Name System) NetBIOS and CIFS NFS (Network File System) NTP (Network Time Protocol) P2P (peer-to-peer) and chat applications Routing protocols, including RIP (Routing Information Protocol) RPC (Remote Procedure Call) and RPC endpoint mapping SNMP (Simple Network Management Protocol) and SNMP trap Syslog TFTP (Trivial File Transfer Protocol) VPNs (Virtual Private Networks), including ISAKMP, L2TP and NAT-T Operating system type (Fingerprinting) Potential vulnerabilities Configuration Issues Obsolete software Built in accounts SSL/TLS testing (versioning, certificate validity/authenticity, matching host name) Other common UDP ports that may expose the scan customer to vulnerabilities, including ports associated with malicious activity OWASP Top 10	• Routers • Firewalls • IDS/IPS • Servers (Operating Systems) • Workstations • Laptops • IoT devices • Database Servers • Web Servers • Application Servers • Common Web Scripts • DNS Servers • Mail Servers • Web Applications • Other Application • Common Services • Wireless Access Points • Load Balancers • SSL/TLS • Remote Access Applications • Point-of-sale (POS) Software

*These are non-exhaustive lists.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.