



SecureVue®: Operational Security for the PCI Data Security Standard (DSS) 1.2

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by the PCI-DSS 1.2 standard, including the scope of supported systems for each PCI-DSS Requirement. These capabilities are in addition to specific PCI DSS reports identified in the companion document, "SecureVue: Compliance Reporting for the PCI Data Security Standard (PCI-DSS) 1.2".

PCI DSS 1.2 Requirements	How SecureVue Implements this Capability
Firewall and System Configuration Standards § 1.1 (1.1.3, 1.1.5); 1.2; 1.3 (1.3.1-1.3.8); 1.4; § 2.1; 2.2 (2.2.2-2.2.4); 2.3	<ul style="list-style-type: none"> ■ SecureVue collects configuration data from a broad range of OS's (Windows, UNIX, Linux, and others) and network devices (routers, switches, VPNs, IDS/IPS, and others). The platform can be extended to support custom devices through SecureVue's built-in Universal Parser. ■ Collected configuration data includes (but is not limited to): hardware profiles (all devices/servers); running configurations (devices), including ports/services/protocols; registry settings (Windows servers); configuration settings (devices/servers); running services/daemons (devices/servers); installed applications (servers). ■ SecureVue establishes configuration baselines for all supported OS's, devices, and databases. ■ SecureVue allows customers to establish configuration policies identifying specific user identities and credentials that should not be present on systems. ■ SecureVue provides alerting and notification when any system or device is no longer compliant with established baselines or policies. ■ SecureVue provides historical reporting of compliance with policies over time.
Periodic Review and Monitoring § 1.1.6	<ul style="list-style-type: none"> ■ SecureVue provides continuous capture and real-time monitoring of a broad range of data, including: events/logs; configuration data; asset data; vulnerability data; performance data; and network flow data. ■ SecureVue establishes monitoring policies for both individual data types, and correlated monitoring policies across multiple types of data. ■ SecureVue provides alerting (with notification) when policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.
Cardholder Data Protection Controls § 3.2 (3.2.1-3.2.3); 3.4	<ul style="list-style-type: none"> ■ SecureVue provides alerting (with notification) when cardholder data policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.
Encryption Controls § 4.1; 4.2	<ul style="list-style-type: none"> ■ SecureVue establishes configuration policies to ensure that systems are correctly configured for use of encryption technologies. ■ SecureVue provides alerting (with notification) when encryption policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.
Antivirus and Antimalware Controls § 5.1; 5.2	<ul style="list-style-type: none"> ■ SecureVue establishes configuration policies to ensure the presence of installed antivirus/antimalware applications and packages. ■ SecureVue establishes configuration policies to ensure the presence of running antivirus/antimalware services and daemons. ■ SecureVue establishes configuration policies to ensure that antivirus/antimalware data files are within appropriate aging guidelines. ■ SecureVue provides alerting (with notification) when antivirus/antimalware policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.
Patch Management Controls § 6.1	<ul style="list-style-type: none"> ■ SecureVue establishes configuration policies to ensure that operating systems, network devices, and applications are patched to appropriate levels. ■ SecureVue provides alerting (with notification) when system patchlevel policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.



PCI DSS 1.2 Requirements

How SecureVue Implements this Capability

Vulnerability Assessment

Controls

§ 6.2; 6.6
§ 11.1; 11.2; 11.3; 11.4

- SecureVue captures vulnerability data from a broad range of vulnerability assessment tools, including (but not limited to): Nessus; ISS; Qualys; Foundstone; Retina; and Harris STAT.
- SecureVue captures log data from a broad range of IDS and IPS applications and appliances. IDS/IPS data can be correlated with all other system data (configuration, asset, performance, vulnerability, and netflow) to build detailed monitoring policies.
- SecureVue establishes vulnerability baselines for all supported OS's, devices, and databases.
- SecureVue provides alerting and notification when any system or device is no longer compliant with established baselines (e.g., discovery of a new vulnerability; change in severity of an existing vulnerability).
- SecureVue provides historical reporting of compliance with policies over time.

Software Application Security

Controls

§ 6.3 (6.3.1, 6.3.5-6.3.6); 6.5
(6.5.1-6.5.10); 6.6

- In addition to capturing system-level vulnerabilities, SecureVue also captures application-level vulnerabilities identified by supported vulnerability assessment tools, including (but not limited to): input validation errors; XSS errors; injection flaws; and malicious code execution flaws.
- SecureVue allows customers to establish configuration policies identifying specific user identities and credentials that should not be present on systems.
- SecureVue provides alerting (with notification) when application security control policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

Logical Access Controls

§ 7.1 (7.1.1-7.1.2, 7.1.4); 7.2
(7.2.1-7.2.3)

- SecureVue can enumerate access controls on multiple object types, including: filesystem objects (directories, files, symlinks on Windows, UNIX, and Linux hosts) and Windows registry keys.
- SecureVue can enumerate user permissions on operating systems.
- SecureVue can enumerate the default access permissions on filesystem objects.
- SecureVue establishes monitoring policies to ensure appropriate user/group access controls are assigned to filesystem objects, and users/groups have appropriate operating system permissions.
- SecureVue provides alerting (with notification) when access control policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

Authentication Controls

§ 8.1; 8.2; 8.3; 8.4

- SecureVue can enumerate users across individual systems, as well as directories (Active Directory, LDAP, and RADIUS), and identify duplicate ID's.
- SecureVue establishes configuration policies to ensure that systems are configured to support specific authentication models (e.g., passwords; two-factor) for both local authentication and remote access authentication.
- SecureVue establishes monitoring policies to ensure that password files and log files containing passwords have appropriate authentication and encryption around these files.
- SecureVue provides alerting (with notification) when authentication control policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

Authentication Standards

§ 8.5 (8.5.1; 8.5.3-8.5.6; 8.5.8-8.5.15)

- SecureVue can enumerate the lifecycle of user accounts, including creation date, modification date, active/inactive state, deletion date, and other properties.
- SecureVue establishes monitoring policies to ensure that terminated users are not associated with any system, network, or application activity.
- SecureVue can enumerate which accounts have been inactive for a defined period of time.
- SecureVue can enumerate the allowed logon periods of user accounts.
- SecureVue can enumerate password policies, including (but not limited to): mandatory password complexity; maximum password age; minimum password length; previous password use; password lockout threshold; password lockout duration; session timeout; and screensaver lockout.

Physical Access Controls

§ 9.1 (9.1.1); 9.3 (9.3.2); 9.4; 9.7; 9.9

- If physical security devices (e.g., cameras, badge readers, doorlocks, etc.) and/or visitor check-in software systems generate text-based log files that can be syslogged, SecureVue can capture these log files into its database, normalize the data, and correlate it with other events, system configuration changes, network traffic changes, hardware changes, and other unexpected behavior across the environment.
- Using SecureVue's optional agent software, SecureVue can identify data egressing onto removable media, including USB keys, writable CD/DVD devices, and other media.



PCI DSS 1.2 Requirements

How SecureVue Implements this Capability

Monitoring and File Integrity Controls

§ 10.1; 10.2 (10.2.1-10.2.7); 10.3 (10.3.1-10.3.6); 10.4; 10.5 (10.5.1-10.5.5); 10.6; 10.7 § 11.5

- SecureVue can enumerate which specific logs are enabled on systems, and ensure that these logs are configured to capture, at a minimum: all individual access to files and/or databases containing cardholder data; all actions taken by administrative users; access to the audit trails themselves; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; and creation and deletion of system-level objects.
- SecureVue captures the complete record of audit trail for every event and log entry, including (but not limited to): user ID; type of event; date and time of event; success or failure of event; origination of event; and affected object.
- SecureVue captures the current system date and time for all systems, validates that an appropriate time service (NTP) is running, and enumerates the time servers associated with each system.
- SecureVue can enumerate the access controls of audit trails.
- Because SecureVue functions as a log server that maintains pristine copies of audit trails and other logs, simply using SecureVue itself meets PCI-DSS 10.5.3, 10.5.4, and 10.5.6.
- SecureVue stores complete copies of all captured data – audit trails and other logs, configuration data, asset data, vulnerability data, performance data, and netflow data – for any user-defined period up to and exceeding one year.
- SecureVue can perform basic file integrity monitoring without agents (via file properties), and using the optional agent, can perform hash-based file integrity checking.

Incident Response Controls

§ 12.9 (12.9.5)

- SecureVue collects a broad range of security data from operating systems (Windows, UNIX, Linux, and others) and network devices (routers, switches, firewalls, VPNs, IDS/IPS, and others). The scope of data is not limited to logs, and includes: log and event data; asset data; configuration data; vulnerability data; performance metrics; and network flow data. The platform can be extended to support custom devices through SecureVue's built-in Universal Parser.
- SecureVue correlates across all collected security data types; as an example, SecureVue can correlate failed logins with other undesired activity such as unusual network traffic patterns and unauthorized system configuration changes, which may point to a broader security issue such as a large-scale attack, or insider threat.
- SecureVue provides over 150 out-of-box alerts for common security incidents, such as failed logins, host hack attempts, and data breaches. All alerts can be customized, and users can create an unlimited number of additional alerts that correlate across any and all collected security data.

Discover how SecureVue provides comprehensive compliance reporting and operational security to support the PCI Data Security Standard. Contact us at +1 877.564.7787 or email sales@eIQnetworks.com to learn more.



eIQnetworks

31 Nagog Park
Acton, MA 01720
t. +1 978.266.9933
f. +1 978.266.0004
www.eIQnetworks.com