



SecureVue®: Operational Security for the Gramm-Leach-Bliley Act (GLBA)

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by GLBA via the Federal Financial Institutions Examination Council (FFIEC) Information Security (IS) Handbook, including the scope of supported systems for each GLBA requirement. These capabilities are in addition to specific GLBA reports identified in the companion document, "SecureVue: Compliance Reporting for the Gramm-Leach-Bliley Act (GLBA)".

GLBA Requirements	How SecureVue Implements this Capability
Security Process	<ul style="list-style-type: none"> ■ SecureVue provides a unified, single-console view into all relevant information security data across the enterprise, eliminating the need to use multiple tools and avoiding the "swivel-chair approach" to security and compliance management. ■ Role-based access control ensures that information security, compliance, and IT operations personnel only have visibility into aspects of security data that are appropriate for their function. ■ SecureVue users can establish policies to monitor almost any aspect of an asset, such as hardware profiles, operating system parameters, and network device configurations. ■ SecureVue policies can be applied either universally to all assets of a similar type, or can be applied granularly to specific, targeted groups of assets. ■ SecureVue provides real-time monitors and dashboards to visualize policy compliance. ■ SecureVue provides alerting and notification when any system or device is no longer compliant with established policies. ■ SecureVue provides historical reporting of compliance with policies over time.
Information Security Risk Assessment	<ul style="list-style-type: none"> ■ SecureVue provides customizable, out-of-box risk categorizations and risk ratings for all assets. ■ Risks defined in SecureVue can be based on and combination of log and event data, system configuration changes, asset changes, and vulnerability profile changes. SecureVue provides dashboards to visualize these risks in real-time. ■ Different risk profiles can be created for individual groups of assets, allowing users to see the relative impact of threats based on asset classification.
Information Security Strategy	<ul style="list-style-type: none"> ■ SecureVue enables visualization of security strategy across all key types of security data, including: logs and events; configuration data; asset data; known vulnerabilities; performance metrics; and network flow data. ■ SecureVue collects configuration data from a broad range of system assets, including 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); and disk configurations, memory configurations, users, groups, and shared resources (servers). ■ SecureVue allows assets to be categorized into user-defined groups based on any criteria, including geographic location, business unit, risk classification, or any other criteria. ■ Individual assets can belong to more than one group, and different SecureVue policies (such as alerts, configuration baselines, risk policies, and monitoring policies) can be applied to different asset groups..



GLBA Requirements

How SecureVue Implements this Capability

Security Controls Implementation - Access Control

- 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.
- 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.

Security Controls Implementation - Physical and Environmental Protection

- 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.
- SecureVue provides alerting (with notification) when access control policies are violated.
- SecureVue maintains records of all collected data, including physical access control data, for any period of time. Retention is limited only by available storage, and user determination of when data is no longer needed.
- SecureVue provides historical reporting of compliance with policies over time.

Security Controls Implementation - Encryption

- 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.

Security Controls Implementation - Malicious Code Prevention

- 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.

Security Controls Implementation - Systems Development, Acquisition and Maintenance

- 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.
- 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 policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.



GLBA Requirements

How SecureVue Implements this Capability

Security Controls Implementation - Personnel Security

- 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 policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

Security Controls Implementation - Data Security

- 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 establishes configuration policies to ensure that systems are correctly configured for use of encryption technologies.
- SecureVue provides alerting (with notification) when policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

Security Controls Implementation - Business Continuity Considerations

- Different risk profiles, monitors, alerts, compliance requirements, and other monitoring criteria can be created for individual groups of assets, allowing users to see the relative impact of threats based on asset classification.
- SecureVue allows users to establish availability baselines for critical systems, applications, services and ports.
- SecureVue monitors the availability of critical systems, applications, services and ports, and can generate a real-time alert when system availability fails to meet a required threshold.
- SecureVue provides a real-time, out-of-box "Availability" dashboard that identifies the current state of all critical systems, applications, services and ports using a straightforward "stoplight" visualization.

Security Monitoring - Activity Monitoring

- 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 specific types of 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.
- 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.

Security Monitoring - Condition Monitoring

- 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), including identification of ports and services that are configured as open.
- SecureVue correlates configuration data regarding known ports and services with other data sources, including port/service enumeration from vulnerability scanners as well as network flow data, to ensure that all enabled ports, services, and protocols on the network are known.
- SecureVue establishes "white list" baselines of allowed ports, services and protocols, as well as "black list" baselines of ports, services and protocols that should not be allowed.
- SecureVue establishes configuration policies to ensure that operating systems, network devices, and applications are patched to appropriate levels.
- 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.



GLBA Requirements

How SecureVue Implements this Capability

Security Monitoring - Analysis and Response

- 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.



eIQnetworks

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