



# SecureVue®: Operational Security for the Health Insurance Portability and Accountability Act (HIPAA)

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by HIPAA (via United States Department of Health and Human Services 45 CFR Parts 160, 162, and 164, "Health Insurance Reform: Security Standards; Final Rule") including the scope of supported systems for each HIPAA requirement. These capabilities are in addition to specific HIPAA reports identified in the companion document, "SecureVue: Compliance Reporting for the Health Insurance Portability and Accountability Act (HIPAA)".

HIPAA Requirements	How SecureVue Implements this Capability
<b>Risk Analysis</b> § 164.308(a)(1)(ii)(A)	<ul style="list-style-type: none"> <li>■ SecureVue provides customizable, out-of-box risk categorizations and risk ratings for all assets.</li> <li>■ 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.</li> <li>■ Different risk profiles can be created for individual groups of assets, allowing users to see the relative impact of threats based on asset classification.</li> </ul>
<b>Sanctions</b> § 164.308(a)(1)(ii)(C)	<ul style="list-style-type: none"> <li>■ SecureVue can enumerate users' compliance with established security policies, such as: access control (at the operating system, application, and database); allowed applications, services, and ports; and password policies (password age, previous password use, session duration, and account lockout).</li> <li>■ SecureVue provides alerting and notification when any user account violates an established security policy.</li> <li>■ SecureVue provides historical reporting of compliance with policies over time.</li> </ul>
<b>Information System Activity Review</b> § 164.308(a)(1)(ii)(D)	<ul style="list-style-type: none"> <li>■ SecureVue can enumerate which specific logs are enabled on systems, and ensure that these logs are configured to capture, at a minimum: all individual user account access; all actions taken by administrative users; access to audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; and creation and deletion of system-level objects.</li> <li>■ 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.</li> <li>■ 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.</li> </ul>
<b>Assigned Security Responsibility</b> § 164.308(a)(2)	<ul style="list-style-type: none"> <li>■ SecureVue implements hierarchical role-based access control, which allows organizations to assign responsibility of assets to specific users.</li> <li>■ SecureVue's role-based access control allows security leadership to limit the scope of visibility into specific assets to only authorized users, while maintaining top-level, command-and-control visibility across the enterprise for senior management teams (e.g., CISO, CIO).</li> </ul>
<b>Workforce Security</b> § 164.308(a)(3)(i)	<ul style="list-style-type: none"> <li>■ 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.</li> <li>■ SecureVue can enumerate user permissions on operating systems.</li> <li>■ SecureVue can enumerate the default access permissions on filesystem objects.</li> <li>■ SecureVue establishes monitoring policies to ensure appropriate user/group access controls are assigned to filesystem objects, and users/groups have appropriate operating system permissions.</li> <li>■ SecureVue provides alerting (with notification) when access control policies are violated.</li> <li>■ SecureVue provides historical reporting of compliance with policies over time.</li> </ul>
<b>Isolate Healthcare Clearinghouse Functions</b> § 164.308(a)(4)(ii)(A)	<ul style="list-style-type: none"> <li>■ SecureVue allows assets to be categorized into user-defined groups based on any criteria, including geographic location, business function, whether the asset contains or processes healthcare data, or any other criteria.</li> <li>■ 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.</li> <li>■ SecureVue users can establish policies to monitor almost any aspect of designated healthcare clearinghouse systems, such as system access, hardware profiles, operating system parameters, and network device configurations.</li> <li>■ SecureVue provides alerting and notification when any designated clearinghouse system is accessed or attempted to be accessed by unapproved or unauthorized users, applications, ports, protocols, and services.</li> </ul>



## HIPAA Requirements

## How SecureVue Implements this Capability

### Access Authorization, Establishment and Modification

§ 164.308(a)(4)(ii)(B)-(C)

- 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.

### Protection from Malicious Software

§ 164.308(a)(5)(ii)(B)

- 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.

### Login Monitoring

§ 164.308(a)(5)(ii)(C)

- SecureVue captures events - including login attempts - across a broad range of operating systems (Windows, Linux, UNIX, and others), network infrastructure devices (routers, switches, firewalls, IDS/IPS, and others), applications, and databases.
- SecureVue captures the complete record of login attempts (both successful and failed), including (but not limited to): user ID; date and time of login attempt; success or failure of login attempt; originating system/IP address of login attempt.
- SecureVue provides alerting and notification when any account violates an established login policy, such as maximum failed login attempts.
- SecureVue provides historical reporting of compliance with policies over time.

### Password Management

§ 164.308(a)(5)(ii)(D)

- 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 can enumerate password policies and user's compliance with these 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 provides alerting and notification when any user account violates an established password policy.
- SecureVue provides historical reporting of compliance with policies over time.

### Security Incident Response and Reporting

§ 164.308(a)(6)(ii)

- 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.



## HIPAA Requirements

## How SecureVue Implements this Capability

### Criticality Analysis and Contingency Operations

§ 164.308(a)(7)(ii)(E)  
§ 164.310(a)(2)(i)

- 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.

### Physical Access Control and Validation Procedures

§ 164.310(a)(2)(iii)

- 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.

### Device and Media Controls

§ 164.310(d)(1)

- Using SecureVue's optional agent software, SecureVue can identify data egressing onto removable media, including USB keys, writable CD/DVD devices, and other media.

### Unique User Identification

§ 164.312(a)(2)(i)

- SecureVue can enumerate users across individual systems, as well as directories (Active Directory, LDAP, and RADIUS), and identify duplicate ID's.
- SecureVue can enumerate the lifecycle of user accounts, including creation date, modification date, active/inactive state, deletion date, and other properties.
- SecureVue can enumerate which accounts have been inactive for a defined period of time.
- SecureVue can enumerate the allowed logon periods of user accounts.

### Automatic Logoff

§ 164.312(a)(2)(iii)

- SecureVue can enumerate session timeout and allowed logon window values on servers and workstations, and capture all events related to user logoff (including forced logoff due to session timeout or expired logon window).

### Encryption and Decryption

§ 164.312(a)(2)(iv)

- 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.

### Audit Controls

§ 164.312(b)

- SecureVue can enumerate which specific logs are enabled on systems, and ensure that these logs are configured to capture all user access at the electronic security perimeter.
- 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.
- Within SecureVue, users can establish "what is normal" for traffic crossing into or out of the electronic security perimeter by either manually defining allowed sources/destinations, ports, protocols, and services, or by allowing SecureVue to monitor the perimeter and automatically establish a baseline of "normal" traffic patterns.
- SecureVue establishes monitoring policies to determine whether unusual network traffic is identified across the boundary of the electronic security perimeter.
- SecureVue provides alerting (with notification) when policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.
- 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.



### eIQnetworks

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