



SecureVue®: Operational Security for NIST Special Publication 800-53

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by FISMA via the NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations", Revision 3, including the scope of supported systems for each NIST 800-53 requirement. These capabilities are in addition to specific NIST 800-53 reports identified in the companion document, "SecureVue: Compliance Reporting for NIST Special Publication 800-53".

NIST 800-53 Control Family	How SecureVue Implements this Capability
AC - Access Control	<ul style="list-style-type: none"> ■ 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 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.
AT - Awareness and Training	<ul style="list-style-type: none"> ■ SecureVue can identify when user activity, such as password management and access attempts, goes against established policies. ■ SecureVue provides alerting (with notification) when access control policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.
AU - Audit and Accountability	<ul style="list-style-type: none"> ■ SecureVue can enumerate which specific logs are enabled on systems, and ensure that these logs are configured to capture all user access. ■ 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 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. ■ SecureVue stores data in an encrypted database that has been certified for NIST FIPS-140-2 and Common Criteria EAL4+.



NIST 800-53 Control Family

How SecureVue Implements this Capability

CA - Certification, Accreditation, and Security Assessments

- SecureVue provides detailed and fully-customizable reporting of information security-related activity across all infrastructure, including network devices, security devices, operating systems, applications, and databases. SecureVue's reports provide evidence of operational capability in support of certification and accreditation activities.
- 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 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 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.
- 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.

CM - Configuration Management

- 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 provides a complete inventory of all network and host assets, including (but not limited to): CPU details; local disk/storage details; attached peripheral details; local users and groups; applications; and patches.
- 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.



NIST 800-53 Control Family

How SecureVue Implements this Capability

CP - Contingency Planning

- 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.
- SecureVue can store data on any file system, including volumes that may be located at alternate storage facilities. SecureVue easily integrates with contingency efforts by allowing users to quickly and easily restore historical data from archived data stored in alternate storage facilities.

IA - Identification and Authentication

- SecureVue captures user-based events 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 all user-based events (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 (or attempts to violate) an established access policy.
- 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.

IR - Incident 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.



NIST 800-53 Control Family

How SecureVue Implements this Capability

MA - Maintenance

- 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 provides a complete inventory of all network and host assets, including (but not limited to): CPU details; local disk/storage details; attached peripheral details; local users and groups; applications; and patches.
- SecureVue establishes configuration baselines for all supported OS's, devices, and databases, and can validate that approved maintenance changes have occurred on assets, such as increases in memory and disk storage, or installation of software and operating system patches.
- 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 maintenance efforts over time.

MP - Media Protection

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

PE - 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.

PL - Planning

- 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.
- SecureVue can correlate all collected data into real-time monitors, alerts, and reports to validate privacy impact statements.

PS - 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 can validate that terminated personnel do not have active accounts, and that no network, host, application or database activity is attributable to user after their termination.
- SecureVue provides alerting (with notification) when policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.



NIST 800-53 Control Family

How SecureVue Implements this Capability

RA - Risk Assessment

- 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.
- 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 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.

SA - System and Services Acquisition

- SecureVue captures a broad range of technology asset data in support of asset inventory.
- SecureVue can correlate individual users with specific application and process execution, in support of software usage monitoring and restrictions.
- SecureVue can identify and report on all applications and patches installed on hosts, including the user and run level of the application or patch.
- SecureVue can monitor applications and process using a combination of events, performance metrics, and flow data, to validate that these applications and processes are compliant with the organization's security engineering principles.

SC - System and Communications Protection

- SecureVue can generate detailed reports on attempted denial of service activity, including activity captured by intrusion detection and prevention (IDS/IPS) security devices.
- SecureVue can identify the prioritization of running processes on systems, and can use performance metrics to determine whether specific service(s) are utilizing inappropriate resources.
- 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 itself is certified NIST FIPS-140-2 compliant, providing assurance of transmission integrity within the SecureVue platform.
- 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.

SI - System and Information Integrity

- 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.



eIQnetworks

31 Nagog Park

Acton, MA 01720

t. +1 978.266.9933

f. +1 978.266.0004

www.eIQnetworks.com