



SecureVue®: Operational Security for NERC Critical Infrastructure Protection (CIP) Standards

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by the NERC CIP standards, including the scope of supported systems for each NERC CIP standard. These capabilities are in addition to specific NERC CIP reports identified in the companion document, "SecureVue: Compliance Reporting for NERC Critical Infrastructure Protection (CIP) Standards".

NERC CIP Requirement	How SecureVue Implements this Capability
Asset Identification and Approval § CIP-002 (R2, R3, R4)	<ul style="list-style-type: none"> ■ 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.
Risk Assessment § CIP-002 (R1)	<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 Policy and Protections § CIP-003 (R1, R4)	<ul style="list-style-type: none"> ■ 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.
Leadership, Scope of Responsibility, and Exceptions § CIP-003 (R2, R3)	<ul style="list-style-type: none"> ■ SecureVue implements hierarchical role-based access control, which allows organizations to assign responsibility of assets to specific users. ■ 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). ■ SecureVue's granular asset grouping capability provides the ability to isolate systems which have approved exceptions to defined policies.



NERC CIP Requirement

How SecureVue Implements this Capability

Access Controls

§ CIP-003 (R5)

- SecureVue can enumerate access controls on multiple object types, including filesystem objects (directories, files, and 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.
- Using SecureVue's optional agent software, SecureVue can identify data egressing onto removable media, including USB keys, writable CD/DVD devices, and other media.
- SecureVue provides historical reporting of compliance with policies over time.

Change Control and Configuration Management

§ CIP-003 (R6)

- 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.

Employee Awareness and Training

§ CIP-004 (R1, R2)

- 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).
- SecureVue provides alerting and notification when any user account violates an established security policy.
- SecureVue provides historical reporting of compliance with policies over time.

Access Rights Management

§ CIP-004 (R4)

- SecureVue can enumerate access controls on multiple object types, including filesystem objects (directories, files, and 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.
- 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.
- SecureVue provides alerting (with notification) when access control policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.



NERC CIP Requirement

How SecureVue Implements this Capability

Electronic Security Perimeter and Access Control

§ CIP-005 (R1, R2)

- SecureVue provides continuous capture and real-time monitoring of information in the electronic security perimeter, including: source and destination IP addresses; ports, protocols, and services; and aggregate ingress and egress bandwidth.
- 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.

Monitoring Access at the Electronic Security Perimeter

§ CIP-005 (R3)

- 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.
- 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.

Cyber Vulnerability Assessment

§ CIP-005 (R4)

§ CIP-007 (R8)

- 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 vulnerability 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.

Physical Security Plan

§ CIP-006 (R1)

- SecureVue allows assets to be categorized into user-defined groups based on physical security profile (such as assets found in a specific geographic location, data center, or room). Users can establish group membership based on data unique to assets found in the physically secure location, such as IP address/subnet or system name.

Physical Access Controls and Monitoring

§ CIP-006 (R2, R4, R6, R7)

- 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.

Port and Service Availability

§ CIP-007 (R2)

- 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 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.

Security Patch Management

§ CIP-007 (R3)

- 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.



NERC CIP Requirement

How SecureVue Implements this Capability

Malicious Software Prevention

§ CIP-007 (R4)

- 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.

Account Management

§ CIP-007 (R5)

- SecureVue can enumerate the lifecycle of user accounts, including creation date, modification date, active/inactive state, deletion date, and other properties.
- SecureVue can enumerate users across individual systems, as well as directories (Active Directory, LDAP, and RADIUS), and identify duplicate ID's.
- 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 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.

Account Management

§ CIP-007 (R5)

- 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.

Security Status Monitoring

§ CIP-007 (R6)

- SecureVue collects and correlates data from a broad range of OS's (Windows, UNIX, Linux, and others), network devices (routers, switches, VPNs, IDS/IPS, and others), applications and databases. The platform can be extended to support custom devices through SecureVue's built-in Universal Parser. The scope of data collected is not limited to logs, and includes: log and event data; asset data; system configuration data; vulnerability data; performance data; and network flow data.
- 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.



NERC CIP Requirement

How SecureVue Implements this Capability

Incident Response

§ CIP-008 (R1)

- 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.

Recovery Planning

§ CIP-009 (R1)

- 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.



eIQnetworks

31 Nagog Park

Acton, MA 01720

t. +1 978.266.9933

f. +1 978.266.0004

www.eIQnetworks.com