



Compliance Automation Using the SecureVue® Unified Situational Awareness Platform

Solution Brief

- **SecureVue, the industry's first unified situational awareness platform, leverages all available information security data to deliver end-to-end compliance automation for all regulations, best practices, standards and other mandates**
- **Today's regulations, best practices and standards for information security compliance cannot be effectively supported with a "checklist" approach to compliance**
- **Compliance automation requires comprehensive support for compliance reporting, configuration auditing, and continuous monitoring**
- **Security point products like log management and SIEM provide only limited visibility into compliance data**

The Evolution of Information Security Compliance

For many years, organizations viewed information security compliance as a "checklist" against a law or industry policy, such as HIPAA, SOX or PCI DSS: if they implemented some specific controls, and could run a few reports to demonstrate these controls were in place when their auditor arrived, the appropriate box would be checked and the auditor would move on.

Today's organizations across both the public and private sector no longer have the luxury of a checklist mentality when it comes to information security compliance. Increasing numbers of regulations, best practices and other mandates -- whether from federal, state and international legislators, industry groups, business partner agreements, or even internal requirements - now require a focused, disciplined approach to compliance. Auditors are no longer focusing solely on information security controls, and are now laser-focused on **how effective these controls are at actually protecting information in the environment**. Information security compliance has evolved from the old checklist approach to a more comprehensive solution, based on compliance automation.

What Is Compliance Automation?

At its core, compliance automation includes three basic capabilities:

- **Compliance Reporting.** Compliance reporting maps specific information security monitoring data to specific sections of regulations, best practices and standards such as PCI, HIPAA, SOX, FISMA, GLBA, NERC CIP, and others. At first, this may seem like a simple requirement; however, all of the mandates listed above require reporting on a broad range of security data, including events, asset and configuration state, network traffic analysis, performance metrics, file integrity, and other security information. Point security products such as log management and SIEM lack the ability to collect and map all of this data, leaving significant gaps.
- **Configuration Auditing.** Organizations need to know how their critical assets are configured, from network infrastructure devices (such as firewalls and routers) to Windows/UNIX/Linux hosts, applications and databases. Configuration auditing provides comprehensive controls reporting against specific policies -- whether those policies are pre-defined standards such as CISA Benchmarks



- SecureVue from eIQnetworks provides end-to-end compliance reporting for major regulations and standards including PCI DSS, HIPAA, SOX, FISMA, GLBA, NERC CIP, and more

- SecureVue provides out-of-box configuration auditing for both network infrastructure devices and hosts, against CIS Benchmarks and DISA STIGs

- SecureVue's unified situational awareness capabilities provide a single plane of glass that simplifies continuous monitoring in the largest global enterprises

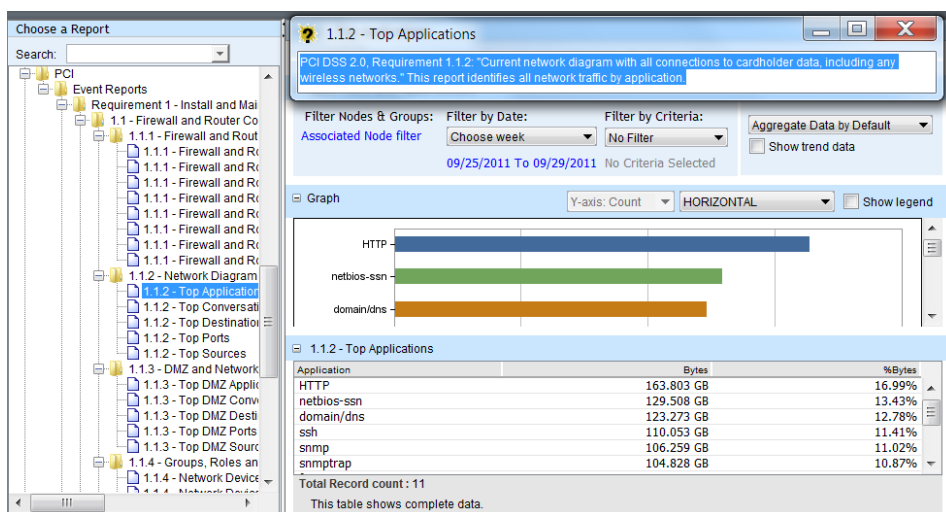
and DISA STIGs, or internally-developed minimum security requirements. Most importantly, configuration auditing needs to address both hosts and devices; only reporting on one type of infrastructure component leaves gaps in compliance visibility.

- Continuous Monitoring.** Recent updates and guidance for major regulations including PCI DSS, HIPAA, and FISMA now mandate the need to continuously monitor enterprise networks. Simply collecting data is no longer enough; organizations across both the public and private sector must ensure that they are always monitoring and alerting appropriate personnel when unusual or unauthorized activity is detected. An effective compliance automation solution dramatically reduces the manual effort required to ensure continuous monitoring of systems, applications, and users.

SecureVue: The Gold Standard for Compliance Automation

SecureVue® from eIQnetworks, the industry's first unified situational awareness platform, provides unparalleled compliance automation by supporting complete compliance reporting, configuration auditing and continuous monitoring.

SecureVue's compliance reports include end-to-end controls mapping across *all* security data, including logs and events, known vulnerabilities, network traffic analysis, asset and configuration changes, performance and availability metrics, native file integrity monitoring, and more. By using the complete breadth of security data, and providing one-to-one mappings between security reports and relevant sections within regulations, best practices and standards for information security compliance, SecureVue ensures that organizations and their auditors have a one-stop repository for compliance reporting.



SecureVue maps all security data into regulations, best practices and standards -- logs and events, network traffic analysis, known vulnerabilities, performance and availability metrics, native file integrity monitoring, and more!

As importantly, SecureVue provides complete drill-down capability across all compliance reports, and can filter reports on specific controls, systems, and even across long periods of time -- and with SecureVue's proprietary, high-speed database that provides the fastest query and reporting capabilities in any security monitoring solution, you won't wait forever to get the information you and your auditors need.



Configuration auditing is another critical capability of compliance automation that SecureVue fully addresses. Unlike other solutions that focus *only* on devices or hosts, SecureVue natively collects a deep set of asset information and security configuration data from both devices and hosts -- and does so without the need for agents! SecureVue's breadth of collected configuration data is extensive, and goes far beyond the data provided by event-based tools such as log management and SIEM, or even vulnerability scanners. SecureVue captures extensive configuration data including: operating system and patch information; applications, services and daemons; system audit settings, including complete details on audit log configuration; file system access controls and (on Windows systems) system registry access controls; security settings, including those found in the Windows registry and UNIX/Linux .conf files; user rights and security policy; and network parameters, including enabled ports, protocols and policies.

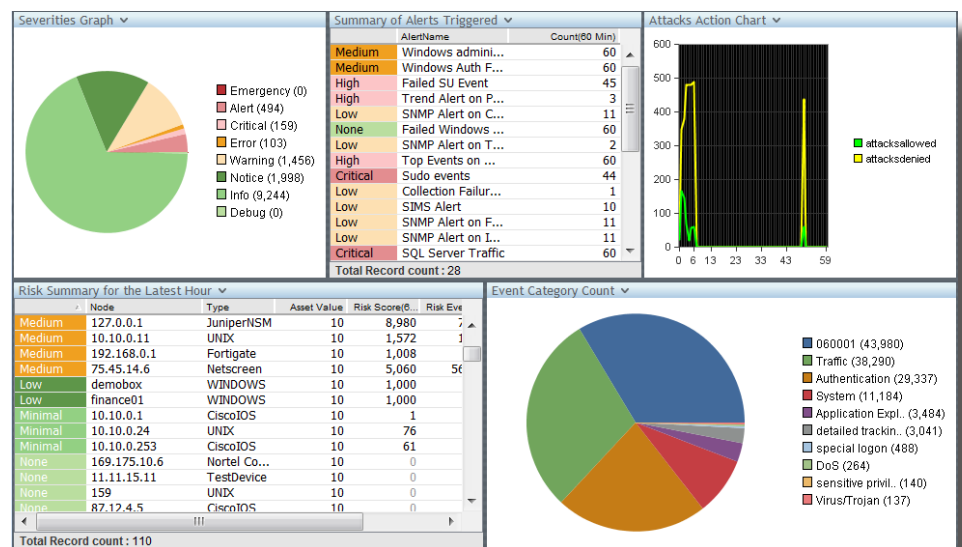
Section	Control	Rule	Status
1 Service Packs and Hotfixes	1.1.1 Cu...	1.1.1 Current Service Pack installed	VIOLATION
	1.2.1 All ...	1.2.1 All Critical and Important Hotfixes available to date have been installed.	OK
2.1 Major Auditing and Account Policies Requirements	2.1.1 Mi...	2.1.1 Minimum Password Length	OK
	2.1.2 Ma...	2.1.2 Maximum Password Age	VIOLATION
2.2.1 Audit Policy (minimums)	2.2.1.1 A...	2.2.1.1 Audit account logon events	OK
	2.2.1.2 A...	2.2.1.2 Audit account management	VIOLATION
	2.2.1.3 A...	2.2.1.3 Audit directory service access	OK
	2.2.1.4 A...	2.2.1.4 Audit logon events	OK
	2.2.1.5 A...	2.2.1.5 Audit object access	VIOLATION

Applied Filter Expression
Policy Name : CISwin2003DC
Node : demobox

Compliance Evaluation Time : 09/29/2011 05:06:29
Configuration Collection Time : 09/29/2011 03:50:45
Vulnerabilities Collection Time : No Vulnerabilities Collection

SecureVue provides one-to-one mapping of configuration data to each and every control within prescriptive security standards such as CIS benchmarks and DISA STIGs, including a straightforward "stoplight" dashboard to quickly identify individual systems and controls that are not in compliance

eIQNetworks provides a comprehensive configuration auditing compliance library, that includes a broad range of prescriptive security control standards including CIS Benchmarks and DISA STIGs. In addition, users can create their own configuration standards based on internal security policies and requirements.



SecureVue provides one-to-one mapping of configuration data to each and every control within prescriptive security standards such as CIS benchmarks and DISA STIGs, including a straightforward "stoplight" dashboard to quickly identify individual systems and controls that are not in compliance

Compliance has evolved from a discipline of periodic evaluation to one of constant evaluation. This can easily be seen in recent updates and guidance for major regulations which have a new emphasis on continuous monitoring -- perpetually evaluating the environment in real-time for potential problems. SecureVue's flexible, fully customizable platform provides a complete capability for visualizing enterprise security posture, and because SecureVue natively collects *all* security data -- logs and events, asset and system configuration state, network traffic analysis, known vulnerabilities, performance and availability metrics, file integrity data, and more - the ability to gain true situational awareness across the enterprise has never been easier or more complete.

SecureVue: Comprehensive Results, Low TCO and Massive ROI

Because SecureVue from eIQnetworks provides so many compliance automation capabilities within a single solution -- including comprehensive compliance reporting, configuration auditing, and continuous monitoring - the need to buy expensive, overlapping technologies is obsolete. As importantly, ***SecureVue leverages your existing technologies***, including point products such as log management, SIEM, IDS/IPS, vulnerability scanners, identity management tools, directory services and more, ensuring that your existing investment in security and infrastructure technologies is never wasted. The freedom to combine existing technologies with SecureVue's native data collection capabilities ensures a low total cost of ownership (TCO), while delivering a huge return on investment (ROI) through immediate results and a single pane of glass into enterprise compliance.

Discover how SecureVue provides comprehensive compliance automation for PCI, HIPAA, FISMA, SOX, GLBA, NERC CIP, CIS Benchmarks, DISA STIGs, and more. 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