

# Bridging the Gap

---

## Achieving Situational Awareness for Information Security and Compliance in Federal Agencies

an elQnetworks White Paper



**elQnetworks**

31 Nagog Park

Acton, MA 01720

t. +1 978.266.9933

f. +1 978.266.0004

[www.elQnetworks.com](http://www.elQnetworks.com)

© 2010, elQnetworks, Inc. elQnetworks, the elQnetworks logo and SecureVue are registered trademarks of elQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.

# Contents

<b>Abstract</b>	<b>3</b>
<b>The Challenge: Overcoming the Tool and Data Gap</b>	<b>3</b>
<b>The Solution: SecureVue® from eIQnetworks</b>	<b>3</b>
<b>Introduction</b>	<b>3</b>
<b>Evolution of a Challenge</b>	<b>4</b>
<b>The Proliferation of Costly Point Products</b>	<b>4</b>
<b>Gaps Grow: Different Teams Use Different Tools that Require Different Data</b>	<b>4</b>
<b>The Challenge: Overcoming the Tool and Data Gap</b>	<b>5</b>
<b>SecureVue Bridges the Gap</b>	<b>6</b>
<b>Collaboration and Correlation</b>	<b>7</b>
Collaboration: Single Pane of Glass	7
Correlation: Intelligence & Vigilance	8
<b>Clear Return on Investment</b>	<b>8</b>
<b>Bringing All the Data Together</b>	<b>9</b>
<b>Features and Benefits</b>	<b>10</b>
Log Management	10
Vulnerability Analytics	11
Configuration Analytics	11
Asset Analytics	11
Performance Analytics	11
Network Behavioral Anomaly (NBA) Detection	11
End-to-End Data Collection & Correlation	12
ComplianceVue	12
<b>Certification and Accreditation</b>	<b>12</b>
<b>Competitive Landscape</b>	<b>12</b>
<b>Internal Organizational Initiatives</b>	<b>13</b>
<b>Summary</b>	<b>13</b>
<b>Additional Information</b>	<b>14</b>
<b>Company Information</b>	<b>14</b>
<b>Analyst and Journal Reviews</b>	<b>14</b>

## Abstract

Over the last decade, a growing challenge has emerged with the proliferation of the tools used to understand and manage an organization's infrastructure. Each tool costs thousands to hundreds of thousands of dollars to acquire and maintain, yet each manages only a small and very specific component of an organization's infrastructure. The responsibility for using these tools rests primarily with three IT teams: the Network Operations Center (NOC), the Security Operations Center (SOC) and the IT Audit function.

### *The Challenge: Overcoming the Tool and Data Gap*

While the different NOC, SOC and Audit teams use these tools, they often do not use the same tools, even when they are both members of a Network Operations and Security Center (NOSC). In addition, different tools collect and work with different types of data. The result is a tool and data gap between teams that makes it very difficult and inefficient to understand how the largest asset in an organization—the network—is operating at any given time. The result: the collaboration between these teams is inefficient at best and nonexistent at worst, and this collaboration is essential for effective security and compliance management.

### *The Solution: SecureVue® from eIQnetworks*

SecureVue from eIQnetworks bridges the growing gap between the NOC, SOC and audit teams and provides your organization with:

- **Increased operational efficiency** through automatic, real-time correlation of all important data, consolidated and customized reporting for each team, and the ability to create standard processes and procedures for all teams
- **Reduced management complexity** through the elimination of unnecessary tools and point products
- **A single window into your network infrastructure** providing a holistic view and enhanced collaboration between teams enabling faster incident identification and remediation
- **Unbeatable total cost of ownership** by reducing the need for dedicated database analysts, third party tools, custom data feeds and custom report design and generation
- **A clear return on investment** by reducing demands on backend storage and by eliminating unneeded point products

## Introduction

Enterprise IT knows about continuous innovation. In a never-ending quest to adjust to accelerated business environment changes, IT has created specialized teams—the network operations center (NOC), the security operation center (SOC) and audit groups—to manage increasingly sophisticated threats, evolving regulations and new reporting mandates. These specialized teams continually deploy point products that are complemented by best practices within each focus area. While this approach may tactically meet the requirements of each area independently, it typically creates silos of incompatible data that hinder effective cross-functional business decision making.

A new challenge has emerged as teams, whether accountable for network availability, information security, or compliance and risk management tasks, discover that day-to-day operational decisions have impact beyond any single functional area. Therefore, decision-making requires a broader perspective supported by consistent enterprise-wide data. Functional point solutions have become less efficient and effective as teams face growing complexity and interdependency, and as networks expand in size.

## Evolution of a Challenge

It all started when the expansion of networks spawned the need for efficient network management tools, and companies began creating different tool sets for different network problems. First, operations staff needed specific tools to manage the data sets from each host or device on the network. As mission critical networks evolved and grew, more tools were developed to understand each of the different, siloed data sets available for the devices comprising the network. Such data sets include event log, performance, asset, configuration, vulnerability and network flow data.

### The Proliferation of Costly Point Products

With the advent of multiple different tool sets came extremely high maintenance and management costs. These costs include hardware, software, maintenance, updates, training and sustainment. The costs also vary based on the amount of risk an organization can tolerate. Since the tools used in daily operations do not correlate data between them, NOC and SOC staff do not have a clear view of the security posture of the network when changes occur. These costs are real and substantial.

Unfortunately, the high expense associated with maintaining siloed tool sets neither buys fortified security nor prevents breaches. Following the now-famous TJX breach, Computerworld reported<sup>1</sup>, "In January, the company announced that someone had broken into its payment systems and illegally accessed card data belonging to customers in the U.S., Canada, Puerto Rico, the U.K. and Ireland. In filings with the U.S. Securities and Exchange Commission in March, the company said **45.6 million credit and debit card numbers were stolen over a period of more than 18 months by an unknown number of intruders**. That number eclipsed the 40 million records compromised in a mid-2005 breach at CardSystems Solutions, Inc. and made the TJX compromise the worst ever in terms of the loss of payment card data."

Another, related development—compliance—spawned more tool sets. Government and internal regulations, standards and best practices for security emerged and created the need for organizations to be compliant. The measurement and proof of this compliance required yet another set of tools to manage and report on these data sets.

### Gaps Grow: Different Teams Use Different Tools that Require Different Data

This tool proliferation translates into many tools managing one network device, and most of these tools do not have collaboration or correlation capabilities to allow the NOC to have a single view of an incident on the network. Without effective collaboration support, these tools make root cause analysis problematic if not impossible.



Figure 1: Multiple security point solutions are required to address NOC, SOC, and Compliance needs

<sup>1</sup> "TJX breach-related expenses: \$17M and Counting", ComputerWorld, May, 2007.

Because these tools serve different purposes, they use different data. In the figure below, device A could be any product on your network such as a firewall, router, VPN, or host. There are specific data elements which help assess different properties of that device such as health, configuration, dialog, normal behavior, conversations, asset information and more. Typically, these data elements are managed by different tools used by different teams for different reasons.

For example:

- Network management tools collect MIB/Asset data
- Network behavioral tools collect flow data
- Configuration management tools collect configuration data.
- Security information/event management tools collect syslog data

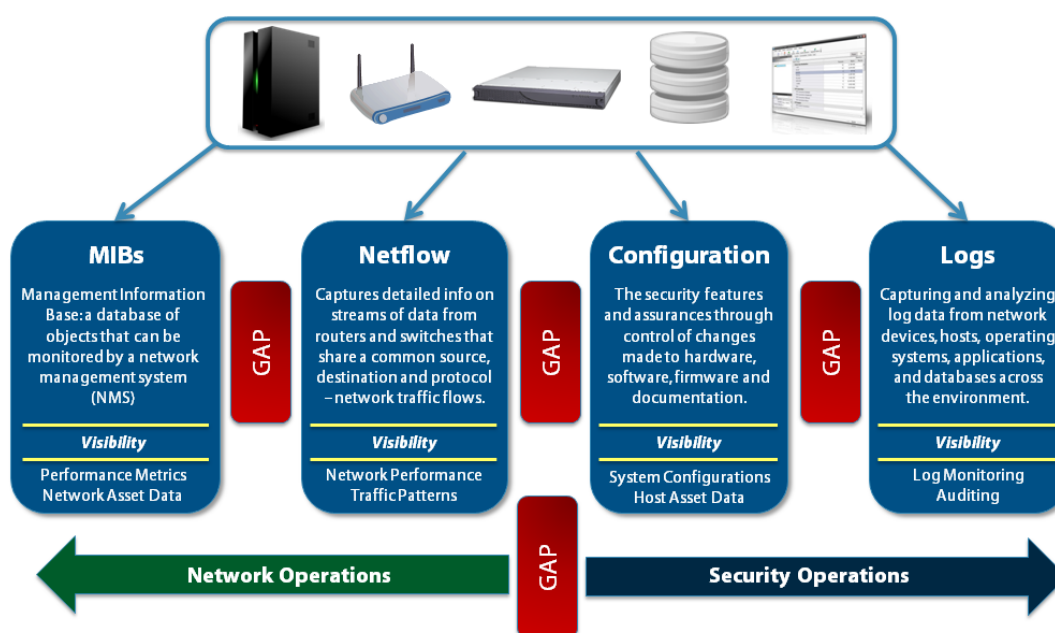


Figure 2: Multiple security point solutions leave critical information gaps

## The Challenge: Overcoming the Tool and Data Gap

The result is clear: a growing gap has emerged between tool sets, data and teams. Because of this gap, the tools are not capable of sharing, correlating or providing insight into the health and risk posture or into changes made on the network. That gap is aggravated by the difference in tool sets used by different teams. The network operations team uses its own tool set while the security team uses a different set. Thus, at least partially because of tool differences, there is an inherent gap between the two teams which is a challenge for most organizations. Specifically, organizations must address questions like:

- How do you get the teams to share and collaborate on the information that is already being collected?
- How can you bridge the gap between the different tool sets?
- How many more tools are you going to deploy to try and fix the problem?
- How much is it going to cost to correct this evolutionary problem?

As noted by Ptak, Noel and Associates <sup>2</sup>, these questions have led to a new set of cross-functional solution requirements based on enterprise-wide collaboration. These requirements define the next-generation of security information management—with comprehensive solutions designed to extract, correlate and analyze actionable information from a mixture of log, vulnerability, configuration, asset, performance and network behavioral anomaly data from across the enterprise. In some cases, these solutions integrate IT governance, risk and compliance (GRC) management functionality to provide a more comprehensive platform that unifies security, risk and audit management. Such platforms complement traditional point solutions by providing a common foundation for team collaboration. They present IT teams with an integrated framework for effective decision making that bridges the gap between them.

## SecureVue Bridges the Gap

As the first true example of such an integrated platform, SecureVue bridges the gap between the siloed tool approaches that have evolved over the last ten years and presents the most advanced holistic approach to security and compliance management. As shown in the figure below, SecureVue accomplishes this by collecting, correlating and reporting on all the data that is important to managing security and compliance: syslog, asset, vulnerability, performance, configuration and network flow data. No one else does this.

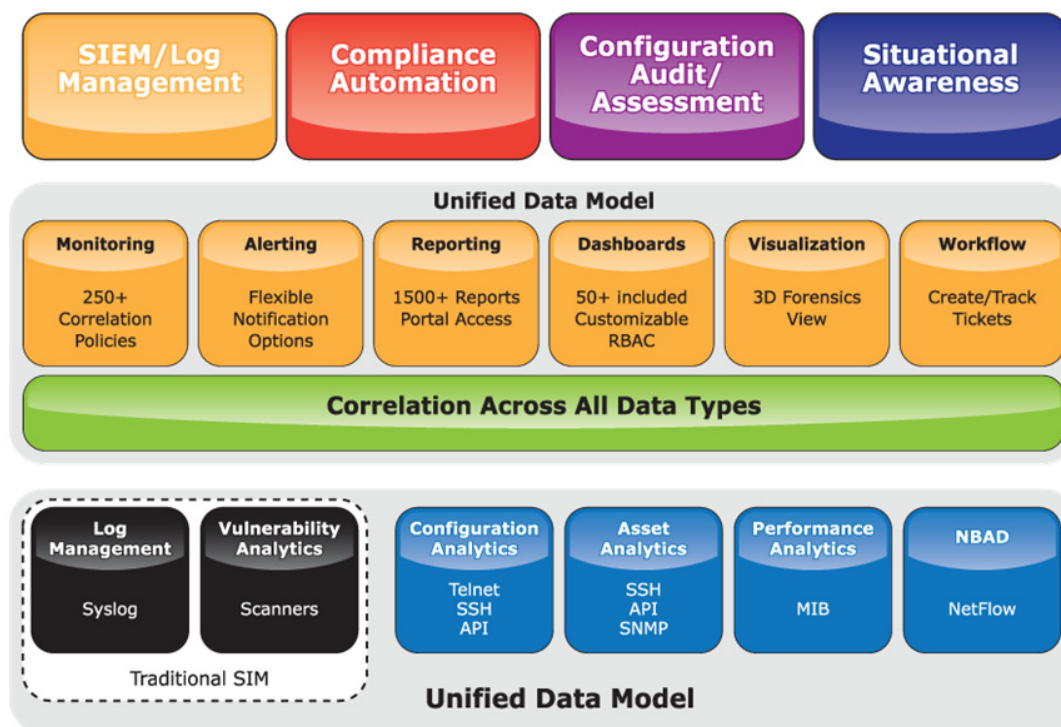


Figure 3: The SecureVue model bridges the information and tool gap left by point security products

SecureVue collects all this data from all the devices and hosts on a network and stores it in one central, easily managed database. It then executes end-to-end correlation of all this data and enables:

- **Increased operational efficiency** through automatic, real-time correlation of all important data, consolidated and customized reporting for each team, and the ability to create standard processes and procedures for all teams
- **Reduced management complexity** through the elimination of unnecessary tools and point products

<sup>2</sup> "IT Collaboration Equals Success", Ptak, Noel and Associates, January, 2008.

- **A single window into your network infrastructure** providing a holistic view and enhanced collaboration between teams enabling faster incident identification and remediation
- **Clear visualization of the risk posture of the network** and enhanced situational awareness from varying view points (network, security & compliance)
- **Dashboards, monitors and reports** that can be customized for the specific requirements of your initiatives and teams
- **The ability to enforce separation of duties** through role-based access control
- **The ability to meet enterprise compliance requirements** by built-in FISMA/SP800-53 support through Audit Center
- **Customization** to support additional mandated compliance requirements

## Collaboration and Correlation

Collaboration and correlation are the central theme of SecureVue. These two, highly sought-after benefits are realized with this tightly integrated platform.

### Collaboration: Single Pane of Glass

SecureVue provides an organization with a methodology to understand how events occur on a network. A feature, QuickVue, plays a key role in allowing SOC and NOC personnel to manage an incident collaboratively and quickly by allowing them to drill down into the assets involved. QuickVue provides all the historical changes to the configuration, asset, vulnerability scans and syslog of each network device from the time it is managed by SecureVue until the end of its production life. With this critical view of all devices, organizations can collaborate and dig deeply into how a change to a specific device allowed the incident to occur in the first place.

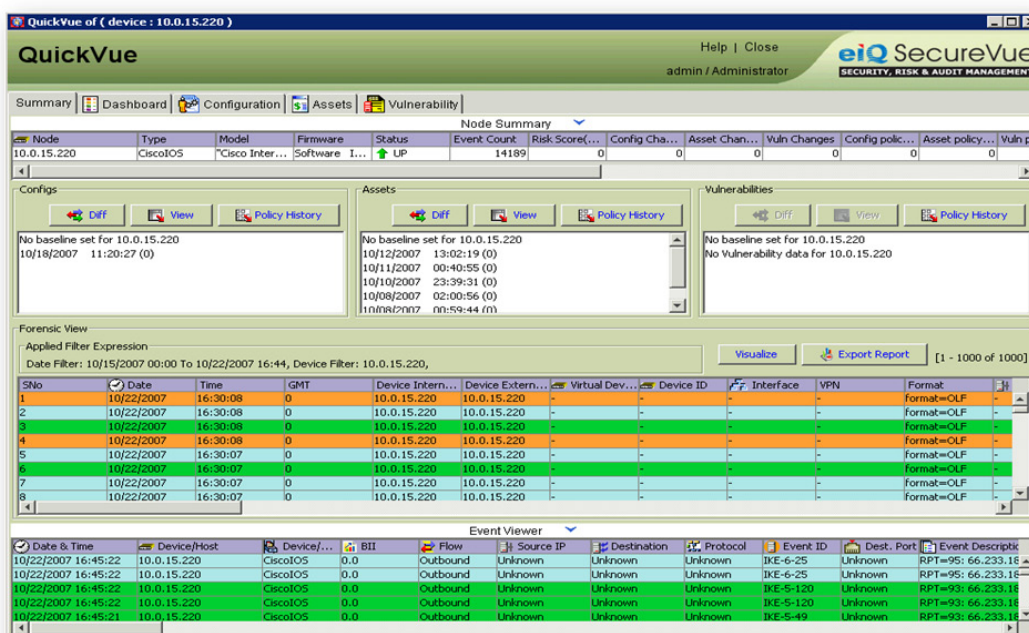


Figure 4: QuickVue provides all data - configuration, asset, vulnerability, log, and performance - in a single pane of glass

In addition, QuickVue provides baseline analysis of all assets. Should a configuration change from the baseline, an organization is notified of the change and it can quickly drill down to view the specific change that occurred through Configuration Analysis. If the change is acceptable, analysts can easily make that configuration the new baseline.

Also, when an asset change is made, the security department can launch a vulnerability scan on the device and view any new vulnerabilities created by the changes. SecureVue also keeps a historical record of each scan for each device through the operational life cycle of the asset.

### Correlation: Intelligence & Vigilance

One of the most important features of SecureVue is the ability to correlate across all data types and events that occur on a network infrastructure on a daily basis. With all the changes that occur moment by moment, SecureVue’s correlation policies keep vigilance against events throughout the infrastructure.

With tools used in IT organizations today, especially SIM tools, correlation rules look at only one data set – syslog. SIM tools are blind to network assets changes that are actually how an incident occurred in the first place. Without correlating all data sources, security and operations personnel would have to manually correlate the event with the asset changes.

With SecureVue, organizations gain an unprecedented understanding of the entire network infrastructure. By correlating events with all the important data types—configuration, syslog, asset, performance, vulnerability and network flow—the SOC and NOC form a true NOSC partnership with a single view of the network infrastructure. Collaboration is then easily accomplished between the two organizations.

### Clear Return on Investment

SecureVue delivers a return on investment in two different and straightforward ways:

- **Reduced procurement** of new or updated point products (and their related maintenance expenses) that could be retired with SecureVue
- **Reduced backend bandwidth** and storage requirements

By calculating the acquisition costs of any new tools for configuration, asset, network behavioral monitoring, security information management, situational awareness (correlation) or compliance, your organization could save thousands if not hundreds of thousands of dollars in the first year alone. The savings can then be multiplied out by five years for additional return. Using the chart below, you can easily forecast the return on investment by calculating the costs for each product and comparing it directly to SecureVue.

	Software	Hardware	Software Maintenance	Hardware Maintenance	Upgrades	Training	Additional Personnel Required (FTEs)	TOTAL
<b>Configuration Tool</b>	\$45,000	\$35,000	\$27,000	\$21,000	\$ -	\$7,500	0.5	\$135,500.00
<b>Asset Tool</b>	\$75,000	\$35,000	\$45,000	\$21,000	\$ -	\$7,500	0.5	\$183,500.00
<b>NBAD Tool</b>	\$15,000	\$20,000	\$9,000	\$12,000	\$ -	\$5,000	0.5	\$61,000.00
<b>SIEM/Log Management Tool</b>	\$100,000	\$45,000	\$60,000	\$27,000	\$ -	\$10,000	1.0	\$242,000.00
<b>Compliance Management Tool</b>	\$65,000	\$35,000	\$39,000	\$21,000	\$ -	\$10,000	1.5	\$170,000.00
<b>TOTAL - Security Point Solution Approach</b>								<b>\$792,000.00</b>
<b>SecureVue</b>	<b>\$125,000</b>	<b>\$45,000</b>	<b>\$75,000</b>	<b>\$27,000</b>	<b>\$ -</b>	<b>\$10,000</b>	<b>0.0</b>	<b>\$282,000.00</b>
<b>TOTAL - SecureVue</b>								<b>\$282,000.00</b>

Figure 5: SecureVue provides more capability than individual point solutions, at a significantly lower cost

The second savings results from reduced bandwidth and storage requirements. If you are currently using configuration management, asset management, a MIB tool, security information management and flow data tool sets, your organization could be creating substantial congestion on the backbone and storage components of the network. In the example below, this organization is using over 23 terabits of bandwidth and storage capacity to capture and store the information for each tool. See the red circle in the blue box below.

STORAGE & BANDWIDTH PER DEVICE							
COLUMN	1	2	3	4	5	6	7
Product	Qty	Config Data (KB)	MIB Data (KB)	Syslog Data (EPS) (KB)	Asset Data (KB)	Vulnerability Data (KB) Avg	Flow Data
Cisco PIX	1	5	15	256*N	2	6	0
Cisco IOS	1	5	10	256*N	2	6	128 * N
Cisco ASA	1	5	10	256*N	2	6	0
Windows Host	1	90	150	1024*N +tcp overhead *N	50	60	0
UNIX/Linux	1	5	40	128*N	5	60	0
Netscreen	1	4	10	256*N	2	6	0
Fortinet	1	60	900	256*N	2	6	0
Sidewinder	1	4	10	256*N	2	6	0

"N" = Events per second for average device

NOTE: Configuration, Asset, & Vulnerability Data collection for the purposes of the above metrics were setup for hourly collection.

This is RAW data to the local collector			
QTY	TIME COLUMNS 2,3,5,6 per hour	TIME COLUMNS 4,7 per hour	TOTALS
	(MB)	(MB)	(MB)
12	0.328	3.00	3.328
314	7.053	117.8	124.80
12	0.270	3.00	3.27
4000	1,367,188	1,000.0	2,367
500	53,711	125.0	179
8	0.172	2.0	2.17
3	2,836	0,750	3,59
6	0.129	1.50	1.63
<b>TOTAL/hr</b>	<b>1,432</b>	<b>1,253</b>	<b>2,685</b>
Per Day	34,360	30,072	64,432
Per Week	240,523	210,504	451,027
Per Month	1,030,814	902,160	1,932,974
Per Year	12,369,763	10,825,920	23,195,683

Actual Storage & Bandwidth with SecureVue's 15:1 compression	
From Collector to the Regional Manager and Central Server to Database	(MB)
	0.22
	8.32
	0.22
	157.8
	12
	0.145
	0.239
	0.109
	179
	4,295
	30,068
	128,865
	1,546,379

Figure 6: SecureVue's native compression provides significant reduction in bandwidth for security, operations, and compliance functions

SecureVue has a 15:1 compression ratio as the data traverses from Data Collector to Regional Server to Central Server. This capability automatically extends the bandwidth and storage capacity. Thus, the 23 terabits of data is reduced to 1.5 terabits of data. That is an enormous savings not only in the first year but also in subsequent years.

## Bringing All the Data Together

SecureVue represents the first integrated security and compliance management platform that brings all the disparate but important data elements together in its overall architecture for end-to-end correlation. SecureVue's agent-less technology uses the native protocols of the products and tools on your network to collect configuration, asset, flow, vulnerability, network flow and syslog data sets. SecureVue can also receive information from other tools such as configuration management data bases, network monitoring, vulnerability assessment products, and so forth.

Data collection points called SecureVue Data Collectors can be located throughout the architecture, as close to the technologies as possible, to allow for our patent pending 15:1 data compression and AES encryption to decrease the amount of data being transmitted over the network. In a distributed SecureVue architecture as depicted below, Regional Servers that are placed at strategic locations for redundancy can process 25,000 events per second. Each Regional Server is a standalone system and, when you add Regional Servers to the distributed architecture, the increase in events processed per second is linear. For example, with four Regional Servers, SecureVue can process 100,000 events per second.

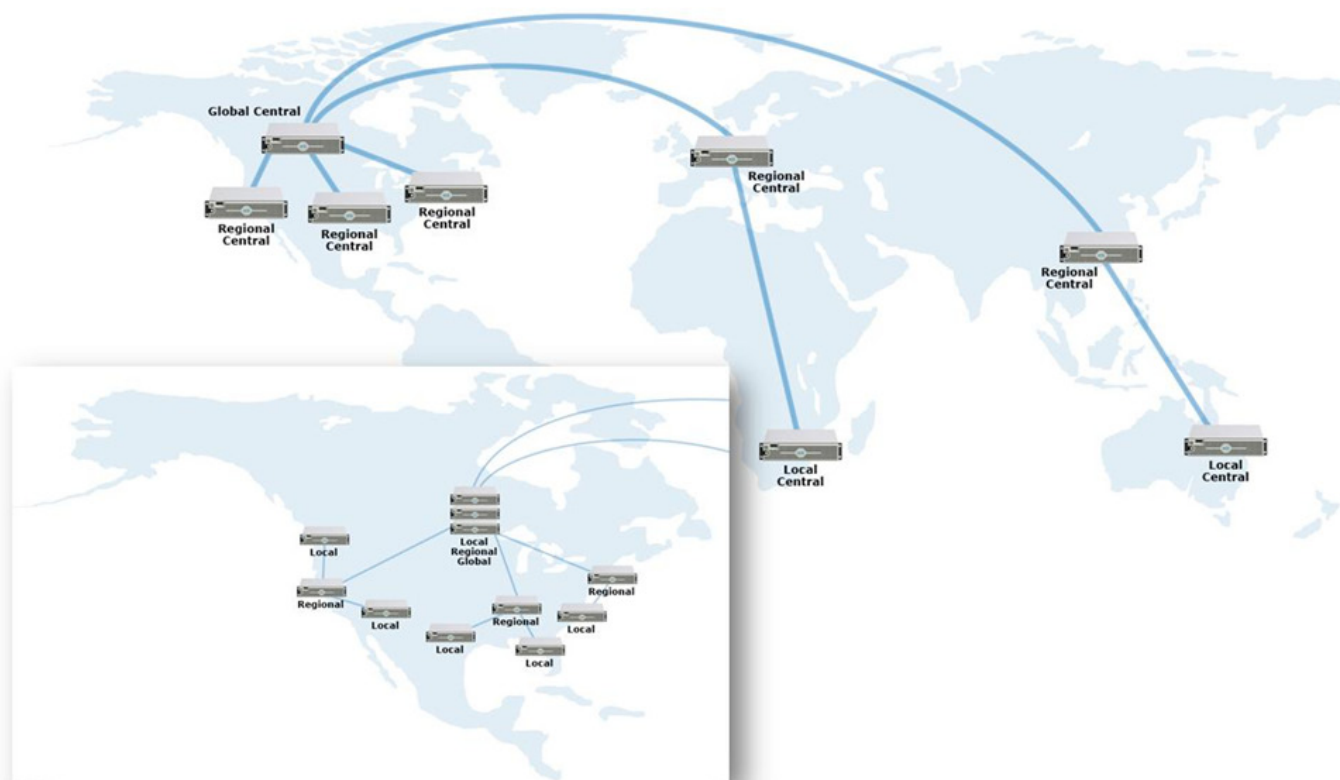


Figure 7: SecureVue scales to support the largest federal global enterprises

SecureVue’s database is a flat-file data store that allows extremely fast reporting capabilities (300,000 EPS parsing of data in the database). In a distributed architecture, data can be stored in one centralized data store—which can be fully redundant—or throughout the architecture with the Regional Servers.

Role-based access ensures that personnel will not have the ability to inappropriately access other Regional Servers or go upstream to the Central Server.

## Features and Benefits

This is a high-level list of key benefits and features of SecureVue. If you need a further detailed list, please contact your sales representative.

### Log Management

Automatically collects, correlates and alerts on event data from virtually any device, host and application:

- **Centralized Archival.** Compresses, encrypts and archives data on DAS, SAN and NAS storage systems
- **Data Integrity.** Provides a clean record of all logs to ensure integrity
- **Forensic Investigations.** Provides an easy-to-use search engine to quickly identify anomalies by accessing volumes of data
- **Universal Parser.** Provides a mechanism to collect data from unsupported nodes and applications

## Vulnerability Analytics

Collects and correlates data from leading vulnerability scanners:

- **Scan.** Scans assets on demand to identify, track, report and alert on system vulnerabilities
- **Identify.** Quickly detects vulnerabilities that require remediation
- **Track.** Provides historical analysis and trending to verify vulnerability mitigation
- **Integration.** Complete integration with Nessus and Qualys

## Configuration Analytics

Collects, alerts, correlates, compares configuration changes:

- **Asset Baseline.** Sets baselines to establish security configuration standards
- **Policy Wizard.** Enables the creation of policies based on configuration standards
- **Manage Change.** Monitors assets to identify, alert and reconcile changes
- **Compare.** Presents current and historical configuration snapshots that detail changes and trends

## Asset Analytics

Centralizes, tracking and management of hardware and software:

- **Identify.** Discovers and classifies all assets within the enterprise
- **Manage.** Captures asset inventory to enable the creation of policies
- **Monitor.** Monitors and alerts on changes to applications and processes
- **Trend.** Tracks assets to facilitate intelligent decisions regarding upgrades and patches

## Performance Analytics

Monitors, collects and analyzes performance data:

- **Monitor.** Measures metrics such as CPU, memory, disk and bandwidth to provide and alert on key performance indicators
- **Prioritize.** Allows for quick detection and remediation of deficiencies across the enterprise
- **Trend.** Tracks performance to provide support for operational improvements

## Network Behavioral Anomaly (NBA) Detection

Profiles all NetFlow, C-Flow, S-Flow, J-Flow and host data to identify and alert on anomalies based on resource utilization, application usage and behavioral patterns:

- **Profile.** Profiles interactions between users, applications and systems to identify typical usage patterns
- **Monitor.** Proactively baselines behavior and alerts on anomalies
- **Resolve.** Minimizes business impact by providing context to reduce MTTR

## End-to-End Data Collection & Correlation

By correlating log, vulnerability, configuration, asset, performance and NBA data across the enterprise, SecureVue transforms volumes of security and compliance information collected across the enterprise into actionable intelligence. The fusion of traditionally disparate data silos enables you to automate incident identification to drive efficiency and reduce management complexity.

## ComplianceVue

SecureVue's compliance library—containing more than 5,000 technical and functional controls—maps directly to audit requirements for:

- **Regulations.** FISMA, DIACAP, GLBA, HIPAA, NERC, SOX, PCI DSS and more
- **Best Practices & Frameworks.** CIS, COBIT, ISO 17799 /27001, NIST 800-53, PCI DSS and more
- **Security Configuration Standards.** DISA STIGs, CIS benchmarks and more
- **Wizard-Based Policy Mapping.** SecureVue's wizard-based policy mapping empowers you to add and modify regulations and best practices to address a broad range of unique business drivers, including internal practices, service level agreements and business partner requirements
- **At-A-Glance Dashboards with Role-Based Access.** SecureVue presents comprehensive real-time views into current and historical regulatory, best practice and policy compliance trends to achieve the goals of different constituents across the organization
- **Advanced Metrics-Based Reporting.** SecureVue provides realigned, audit-friendly reports that map compliance drivers to specific IT controls

## Certification and Accreditation

- **SecureVue 3.x FIPS-140 Level 2 Certification** - CERTIFIED APRIL 2010
- **NIAP EAL4 + (2 Augmentations)** - ENTERED MARCH 2009
- **U.S.-based company;** World Headquarters: Acton, MA

## Competitive Landscape

Regardless of the products or tools that will be tested in a proof of concept against SecureVue, none of them offer the integrated capabilities of the eIQ platform. Some tools have specific capabilities that require agents on all the hosts and workstations while others require extensive and exhaustive customization to provide useful information.

For example, SecureVue provides all 17 controls of the government-mandated FISMA with SP800-53. As depicted in the table below, no other tool delivers each area of the SP800-53 requirements. To accomplish this without SecureVue, your organization would need to procure a tool for each area and then piece together a reporting structure. It is not impossible, but it is extremely difficult. In fact, once the report is complete, it will probably be out of date. With SecureVue, the monitors and reports are near real-time, 7x24, 365 days a year.

Though SecureVue is much more than a SIM/SEM tool, Gartner labeled it as such to fit it into one of their Magic Quadrant guides. Here are some of the excerpts from Gartner on eIQnetworks SecureVue competition:

- **eIQnetworks SecureVue:** "SecureVue provides a broad function set that includes SIEM, performance, security asset and configuration policy compliance capabilities."

- **Arcsight:** "ArcSight ESM software requires substantial end-user expertise in areas such as database tuning, and customers typically comment on the investment in server-side resources needed to support the deployment."
- **NetForensics:** "Needs to execute on its plans to simplify deployment and support requirements for the nFX Open Security Platform."
- **Cisco MARS:** "Although MARS supports basic compliance monitoring for servers, it is not optimal for SIM deployments that require highly customized audit/reporting function. Larger enterprises with heterogeneous network device data source requirements, and those that require consolidated correlation or reporting across multiple appliances will find MARS insufficient for their specific needs."
- **Q1 Labs:** "Other appliance-based solutions are more appropriate when only log management and/or basic event management is required."
- **LogLogic:** "Limited SEM capabilities usually preclude the use of LogLogic appliances as the sole technology when SIM and SEM functions are needed."

## Internal Organizational Initiatives

Take a moment to examine some or all of the initiatives that are being requested by C-Level management in your organization. Identify those initiatives and then consider the number of tools (software, hardware, maintenance, training and sustainment) required to accomplish what is being requested. Over the past two years, these are some of the initiatives eIQnetworks has responded to:

- Enterprise Security Posturing
- Dashboards for C-level users
- Monitors and reports for all 17 controls of FISMA/SP800-53 compliance to assist in the OMB initiatives
- Role-based access capabilities
- Situational Awareness
- No siloed technologies
- Gapless capabilities
- Solution spaces for security and operations to work effectively
- Reduced total cost of ownership
- Enterprise-focused solution platform
- Efficient standardized processes and procedures
- Best Practices for compliance
- Better defense of the network
- Holistic approach
- "Tell me what is normal!"

## Summary

If your organization has specific initiatives for the Network Operations and Security Center and/or is executing on a compliance strategy, testing SecureVue against any other tool should be a top priority for you. eIQnetworks has a Proof of Concept Guide with very detailed and specific checklists to help guide your organization to all the key benefits, value and cost savings of SecureVue. eIQnetworks believes that SecureVue delivers the most cost effective and comprehensive technical solution on the market today.

Customers say they have never seen anything like SecureVue. They say it is hard to believe that there is a platform on the market that will consolidate, monitor and report on every critical system, device or component in one single view. We look forward to turning you into a believer by showing you how SecureVue will perform in your environment.

## Additional Information

### Company Information

eIQnetworks®, Inc., a leader in integrated security, risk and audit management, enables enterprise, government and MSSP customers to effectively meet security and compliance challenges through a unified framework. More than 2,700 organizations worldwide rely on the power of eIQ's enterprise security management and IT governance, risk and compliance solutions to proactively detect security breaches, speed incident remediation and support evolving best practices and compliance regulations across the enterprise. For additional information, please visit [www.eIQnetworks.com](http://www.eIQnetworks.com) or call +1 978.266.9933.

### Analyst and Journal Reviews

- **Red Herring North American Top 100 Company (5/08)**

[http://www.redherring.com/blog/jdreyfuss\\_redherring?bid=24253](http://www.redherring.com/blog/jdreyfuss_redherring?bid=24253)

Red Herring North America 100 Award - For 10 years, Red Herring's editorial team has diligently surveyed entrepreneurship around the globe. Technology industry executives, investors, and observers have regarded the Red Herring 100 lists as an invaluable instrument to discover and advocate the promising startups like eIQnetworks that will lead the next wave of disruption and innovation.

- **Gartner Report (5/08)**

[http://www.eiqnetworks.com/news/eIQ\\_GartnerVisionary.shtml](http://www.eiqnetworks.com/news/eIQ_GartnerVisionary.shtml)

eIQnetworks has been positioned by Gartner, Inc. in the Visionaries Quadrant of its newly published Magic Quadrant for Security Information and Event Management. Gartner states: "eIQnetworks' SecureVue offering is unique in that it provides broad capabilities that include SEM, SIM, security configuration policy compliance, operational performance functions and some NBA capabilities in a single product."

- **Network World (4/08)**

<http://www.networkworld.com/newsletters/techexec/2008/041408techexec1.html?page=1>

"This product does so much that I can't possibly begin to tell you about the features and functions here. In the past year and a half, my company has studied dozens of solutions meant to improve an enterprise's security and compliance posture. We can honestly say that eIQnetworks has the broadest range of capabilities we've seen in one integrated product."