Security and Compliance Management. Redefined.

Technical Whitepaper

BRIDGING THE GAP
Security, Operations & Compliance

eIQnetworks, Inc.,
World Headquarters
31 Nagog Park
Acton, MA 01720
978.266.9933

www.eiqnetworks.com

TABLE OF CONTENTS

INTRODUCTION

Enterprise IT knows about continuous innovation. In a never-ending quest to adjust to accelerated business environment changes, IT has created specialized teams within 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 paradigm shift is emerging 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. Today, IT's success depends upon solutions that improve cross-team communications and collaboration.

This challenge has led to a new set of cross-functional solution requirements based on enterprise-wide collaboration. These requirements define the next-generation of Security and Operations; 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 compliance 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.

EXECUTIVE BRIEF

Over the last decade, a growing problem has emerged among the various products used to manage and understand an organization's infrastructure. Each tool deployed costs thousands to hundreds of thousands of dollars yet manages only a minute and very specific element of an organization's infrastructure. Security, Operations and Compliance personnel all use different toolsets and very few of these toolsets work together. This makes the task of understanding how the largest asset in an organization – the network – is truly operating at any given time.

Today's Defined Roles

The NOC is responsible for the network—the communications pathway within and outside the enterprise. A network failure or slowdown can have catastrophic consequences for the entire business. The NOC also makes decisions which broadly impact business operations related to data and information security, service levels and repairs, transaction integrity, and customer response times and satisfaction.

The SOC is responsible for analyzing and assessing risk as well as identifying and evaluating general security measures. After determining acceptable levels of security and risk, the SOC develops policies and procedures to manage those to acceptable levels. They must also define the actions taken when violations occur. Their enterprise role and access to nearly all corporate data and assets makes them the controlling authority for implementation, monitoring, management and reporting of these processes.

Finally, IT Audit is responsible for providing independent analysis of IT operations and assets to ensure compliance with external compliance drivers such as applicable regulations, best practices, standards, as well as internal drivers such as business partner agreements, service level agreements, and risk profiles. In addition, this group provides detailed analysis of gaps in compliance, and provides specific recommendations to address these gaps and reduce risk. To be truly effective, IT Audit must be an independent group, with a separate reporting and accountability chain of command from NOC and SOC. The problem is, there is no collaboration between these groups and the toolsets they use. The NOC and SOC (even when they have been established in a Network Operations and Security Center – NOSC) personnel use different toolsets to accomplish their roles.

Costs associated with using different toolsets are extremely high and their use is difficult to manage. These costs include hardware, software, maintenance, updates, training and sustainment. The costs also vary based on the amount of risk an organization wants to take on. Since the tools used in daily operations do not correlate data between them, Operations and Security personnel do not have a clear visible view on the security posture of the network when changes occur. These costs are real and substantial, as one famous example illustrates:

> **Computerworld** *TJX breach-related expenses: $17M and counting*, May 2007:
>
> "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."

Compelling Events

eIQnetworks SecureVue provides the visibility required to navigate, manage and report on your networks health, behavior and risk. By implementing SecureVue your organization will:

- Have a holistic view of your network
- Have consolidated reports from each operational area of the network (Security, Operations and Compliance)
- Enhance the communication and collaboration between Operations and Security personnel
- Gain a Return On Investment by replacing other tools which may not be required
- Foster standard processes and procedures for all teams
- Provide the NOSC personnel with near real-time situational awareness
- Bridge the gap between Operations, Security and Compliance tools and personnel

Here is what respected security risk assessment analysts are saying about eIQnetworks SecureVue:

> **Gartner**, *Magic Quadrant*, May 2008, "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**, *Get a holistic view of your security and compliance posture*, April 2008 "eIQnetworks takes a different approach to trying to solving the problem of disparate data; eIQnetworks has one integrated suite that does security management, change management, risk management and audit management. The idea is to use one tool and one data source to eliminate the operational islands and yield a holistic view of the network."
>
> "eIQnetworks packs a lot of punch into its SecureVue product. At the core of the product are Enterprise Security Management (ESM) capabilities, including log management, vulnerability analytics, configuration analytics, asset analytics, performance analytics, and network behavioral anomaly detection. End-to-end data is collected and correlated in one monitor and a vast dashboard with very detailed drill-down information."

"**What are the compelling events for evolving your Network Operations, Security and Compliance capabilities?"**

EVOLUTION OF A PROBLEM

As networks were created in an organization, it was apparent that products must be developed to keep the network operational. To manage the products which comprise a network, public and private companies created tools to view, change and report on events. This allowed organizations to understand how the network was performing. As networks evolved, more companies created differing toolsets for different problems.

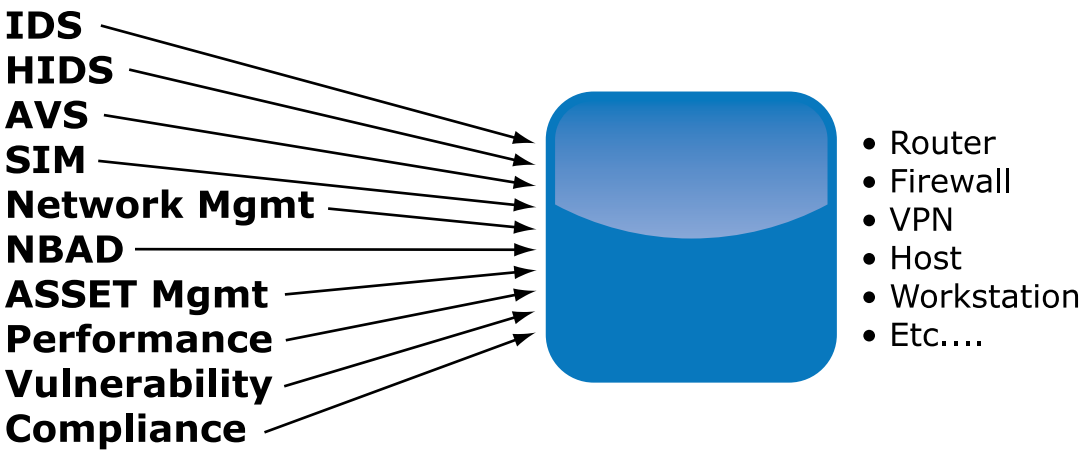
First, Operations needed specific tools to manage the data from each product or device on the network. As the mission-critical network evolved and grew, more tools were developed in efforts to understand stove-piped datasets from all of the network devices.

With the rapid growth of the Internet, many new devices, applications and systems have been introduced. With this growth, problems have become more complex and severe, leading to still more new tools being added to manage the network's security risk posture.

Now another need is at hand: compliance. Government and internal regulations are mandating that organizations meet additional requirements. This requires yet another set of tools to manage and report on these datasets.

Thus the underlying problem is that different tools are managing every network element – including routers, switches, firewalls, hosts, workstations and more.

LOTS OF TOOLS TO MANAGE ONE BOX



Further compounding the problem is that most of these tools do not have collaboration or correlation capabilities to allow the NOSC to have a single view of an event or occurrence on the network. Root cause analysis is difficult if not impossible.

THE GAP IN TODAY'S TOOLSETS

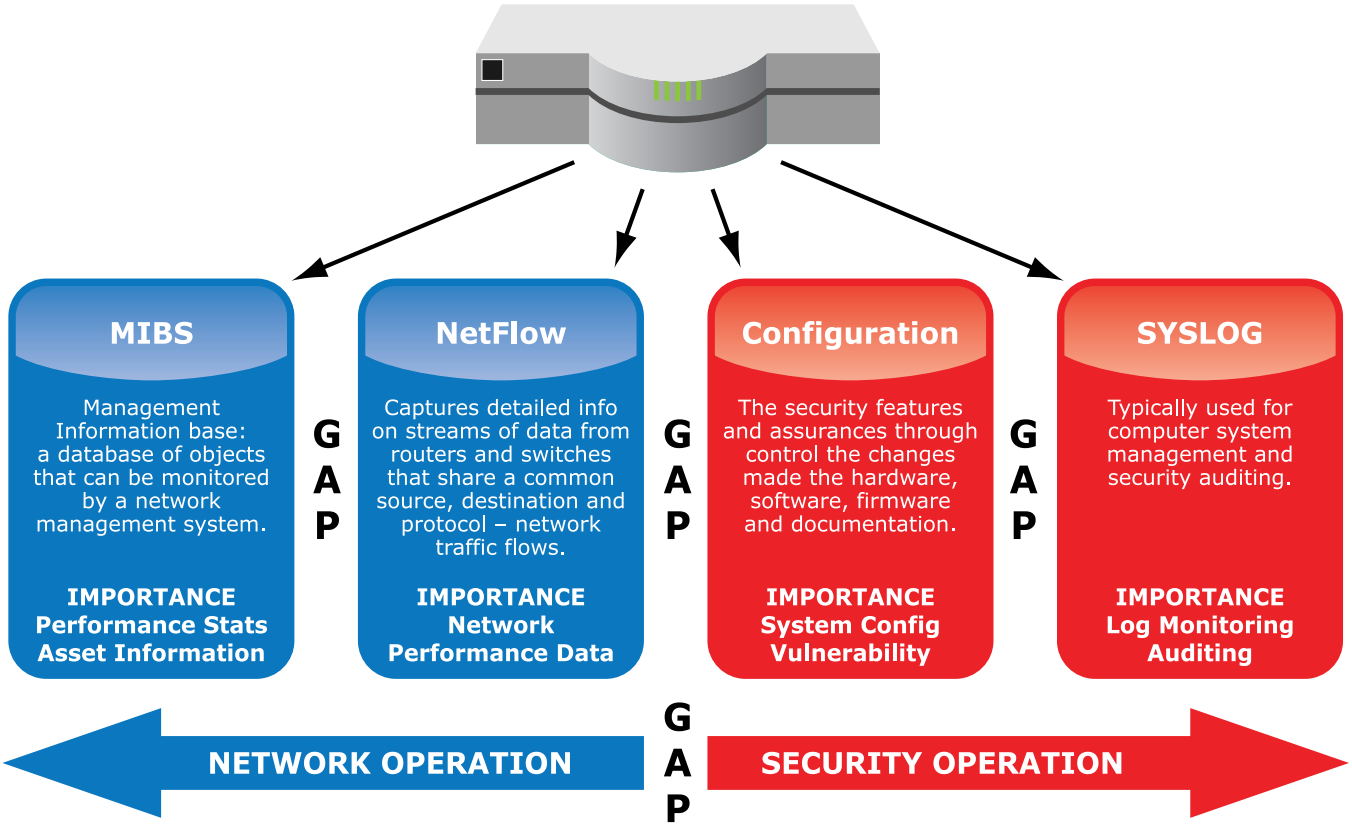
To illustrate the problem, imagine any device in your network, depicted as a generic box at the top of the diagram below. Below the box are some of the specific data elements which help assess different properties of that device (including its health, configuration, dialog, normal behavior, conversations, asset information and more). Different products used by Operations and Security personnel for specific reasons manage these data elements.

Each set of tools managing our generic box looks at a limited range of data. This leads to gaps such as these:

1. MIB/asset data is collected by network management tools
2. Flow data is collected by network behavioral tools

3. Configuration data is collected by configuration management tools
4. Syslog data is collected by Security Information/Event Management (SIEM) tools
5. Missing entirely: performance data

The Challenge of Every Organization



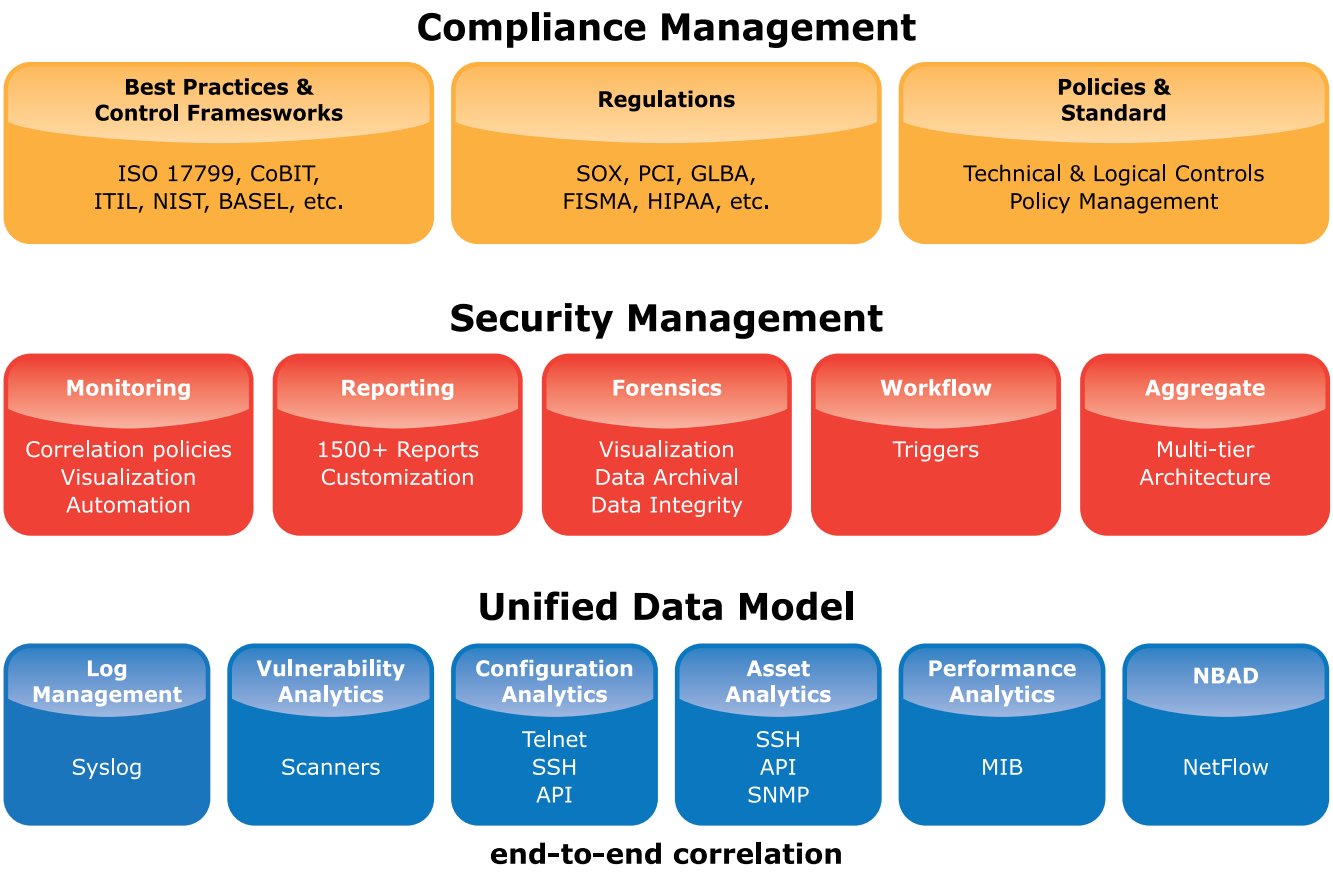
To compound the gap problem, the tools do not have the capability or capacity to share, correlate or provide insight into the health, risk posture or changes made on the network. That GAP is further widened by the fact that different teams use the different toolsets. Network Operations uses its own toolsets while the Security Team uses their own toolsets. There is an inherent gap between the two teams which is a challenge for most organizations. And that doesn't factor in the tools used by the IT Audit group to largely achieve the same goals. These disparate toolsets force network and security operations teams to ask the following questions:

- 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 toolsets in use by the various operations teams?
- How many more tools are you going to deploy in efforts to fix the problem?
- How much is it going to cost to correct this evolutionary problem?

CONVERGENCE OF TECHNOLOGIES

SecureVue bridges the gap between the stovepipe tool approaches that have evolved over the last 10 years. SecureVue collects, manages, monitors and reports:

Syslog Data | Asset Data | Scanner Data | Performance Data | Configuration Data | Network Flow Data



SecureVue collects this data from all devices and hosts on a network and brings it into one central, easily managed database. This approach equips SecureVue with the unique capability and capacity to correlate all the different data types.

This is important because:

- Role-based access control allows organizations to segregate and separate duties
- The NOSC can have a holistic view of the network and security posture
- Situational awareness can be gained from multiple viewpoints (Network, Security & Audit/Compliance)
- Dashboards, monitors and reports can be generated for the specific requirements of your initiatives
- End–to-end correlation is implemented between the different data silos
- The network risk posture can be visualized in its entirety
- Enterprise compliance requirements are met by built-in FISMA/SP800-53 compliance through Audit Center

- Additional mandated compliance requirements can be readily and easily customized for the organization
- A single pane of glass: The NOSC can drill down to identify the root cause with one tool. Both the Operations and Security teams can create workbenches and workflows to correctly identify a problem and correct it.

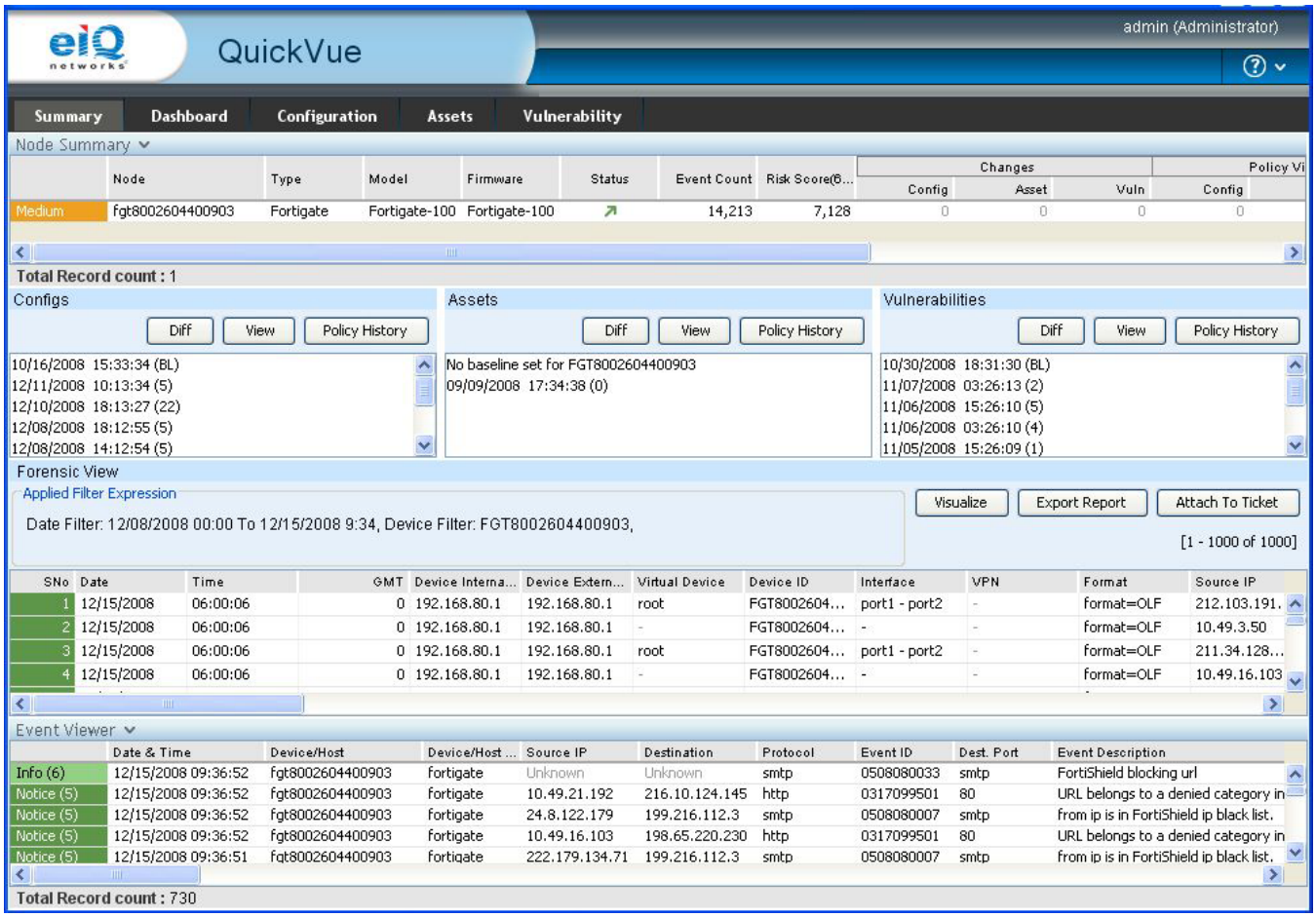
COLLABORATION & CORRELATION

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

Collaboration: SINGLE PANE OF GLASS

SecureVue provides organizations with a methodology to understand how events occur on a network. With QuickVue, security and operations personnel can manage the event by collaborating and viewing the assets that were or are involved in an incident. QuickVue provides all the historical changes to the configuration, asset, vulnerability scans and syslog records of each network device for the time it is managed by SecureVue until it is end of production life.

With this critical view of all devices, organizations can collaborate and dig deep into the data to identify HOW a change to a specific device allowed the event to occur in the first place.



In addition, QuickVue provides a baseline analysis of all assets. Should a configuration change from the baseline (and thus deviate from the policy), an organization is notified of the change and can quickly drill down to view the specific change that occurred through Configuration auditing capability of SecureVue. If the change is acceptable, analysts can easily make that configuration the new baseline.

This level of collaboration is critical in building a better security process. For example, 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. This ensures no new issues are introduced by the constant changes to devices on the network. SecureVue also keeps a historical record of each scan for each device through the operational life cycle of the asset to enable forensic analysis in the event of an incident.

Correlation: Intelligence & Vigilance

By gathering more data types than other solutions, SecureVue can 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 ensure constant vigilance against security attacks throughout the infrastructure.

With many of the tools used in IT organizations today, especially SIM offerings, the correlation rules look at only one dataset – log data. SIM tools are blind to the configuration changes that actually create exposures in the first place. Without correlating all data sources, security and operations personnel would have to manually assemble the information to isolate and pinpoint the cause of an incident.

With SecureVue, organizations gain an unprecedented understanding of their entire network infrastructure. By learning of configuration changes, asset changes, vulnerability changes, performance changes and abnormal network flows – and then seeing all of these data types correlated to look for potential issues – the Security Operations Center and Network Operation Center form a true NOSC partnership. With a single view of the network infrastructure, collaboration is easily accomplished between the two organizations.

INTERNAL ORGANIZATIONAL INITIATIVES

Take a moment to examine some or all of the information being requested by the C-Level personnel in your organization. Think of the number of costs (software, hardware, maintenance, and training) that will be required to deliver on their requests. Over the past two years, some of the information and value eIQnetworks has delivered to customers includes:

- Enterprise security posture awareness
- Dashboards for the C-Level executive
- Monitors and reports for all 17 controls of FISMA/SP800-53 compliance to assist in the OMB initiatives
- Reports for the 12 requirements of PCI-DSS (Payment Card Industry – Data Security Standard)
- Role-based access capabilities

- Situational awareness
- "Solution spaces" for Security and Operations to work effectively
- Reduce Total Cost of Ownership (TCO)
- Enterprise-focused solution platform
- Efficient standardized security and compliance processes & procedures
- Best practices for compliance
- Better defense of the network and technology assets

COMPETITIVE LANDSCAPE

Regardless of the products and tools that will be tested in a proof of concept, none of them offer the depth and breadth of SecureVue's integrated capabilities.

Some tools have specific capabilities that require agents on all the hosts and workstations while some other tools require extensive and exhaustive customization to provide any semblance of information.

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

NIST SP 800-53 Control Families	SIM	Asset	Config	Performance	NBAD	SecureVue
Risk assessment	◐	○	○	○	◐	●
Planning	○	◐	◐	◐	○	●
System & service aquisition	○	◐	◐	◐	○	●
Certification, Accreditation & sec assessment	○	○	○	○	○	●
Personnel security	○	○	○	○	○	●
Physical & environmental protection	○	○	○	○	○	●
Contingency planning	○	◐	◐	◐	◐	●
Configuration management	◐	◐	◐	○	○	●
Maintenance	○	◐	◐	○	○	●
System & information integrity	◐	◐	◐	○	○	●
Media protection	◐	◐	◐	○	○	●
Incident response	●	◐	◐	◐	●	●
Awareness & training	○	○	○	○	○	●
Identification & authentication	◐	○	○	○	◐	●
Access control	◐	○	○	○	◐	●
Audit & accountability	◐	○	○	○	◐	●
System & communications protection	●	◐	◐	○	◐	●

● Supported ◐ Partial Support ○ Not Supported

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

RETURN OF INVESTMENT

There are two areas which SecureVue provides a very compelling Return-On-Investment:

1. Decrease the amount of money for the procurement of new products. Maintenance dollars needed for existing point product technologies could be eliminated with SecureVue.
2. Reduction in back end bandwidth and storage requirements to support the security and compliance management platform.

By calculating the costs of avoiding having to procure new tools for configuration, asset, network behavioral monitoring, security information management, situational awareness (correlation) or compliance – organizations can save thousands if not hundreds of thousands of dollars in the first year – which can then be multiplied out by five years for additional savings.

The second area of savings is the reduced bandwidth and storage requirements of SecureVue compared to the backend demands of supporting and operating multiple point products.

Currently, organizations that are using configuration management, asset management, network management tools, security information management and flow data toolsets could be creating substantial congestion on the network backbone and storage environment. 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. Note the red circle in the blue box below.

STORAGE & BANDWIDTH PER DEVICE

COLUNM	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	Actual Storage & Bandwidth with SecureVue's 15:1 compression
	(MB)	(MB)	(MB)	From Collector to the Regional Manager and Central Server to Database (MB)
12	0.328	3.00	3.328	0.22
314	7.053	117.8	124.80	8.32
12	0.270	3.00	3.27	0.22
4000	1,367.188	1,000.0	2,367	157.8
500	53.711	125.0	[illegible]	[illegible]
8	0.172	2.0	2.17	0.145
3	2.836	0.750	3.59	0.239
6	0.129	1.50	1.63	0.109
TOTAL/hr	1,432	1,253	2,685	179
Per Day	34,360	30,072	64,432	4,295
Per Week	240,523	210,504	451,027	30,068
Per Month	1,030,814	902,160	1,932,974	128,865
Per Year	12,369,763	10,825,920	23,195,683	1,546,379

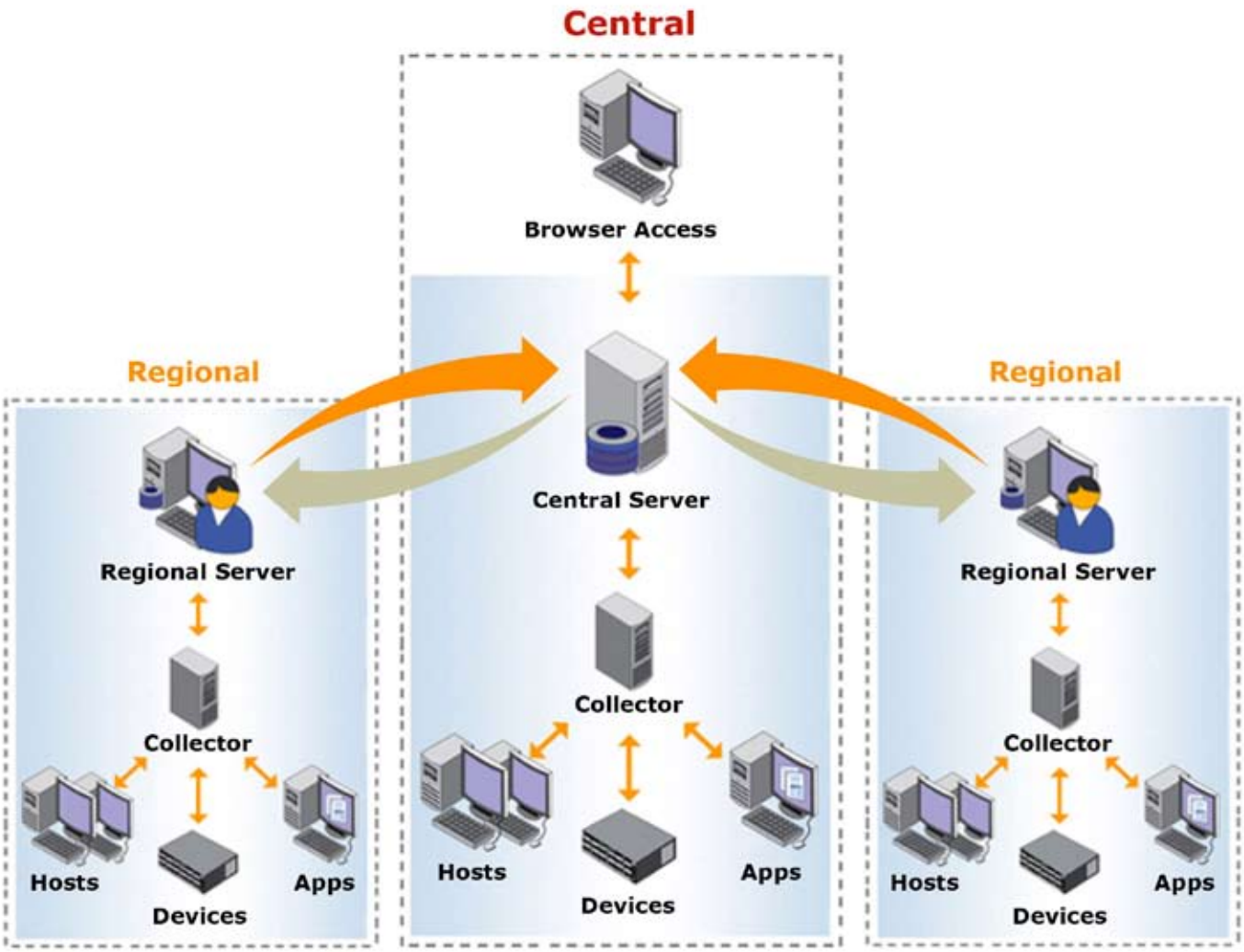
To ensure the most effective use of storage resources, SecureVue has a 15:1 compression ratio as the data travels from the collector to the central server. This capability automatically extends bandwidth and storage capacities. Thus the 23 terabits of data is reduced to only 1.5 terabits. This is an enormous savings not only in year 1, but also in subsequent years.

SecureVue OVERVIEW

Architecture

SecureVue brings together the disparate data elements, which comprise a network architecture. SecureVue's agent-less technology uses the native protocols of the products and tools on the network to collect configuration, asset, flow, and vulnerability and log datasets. SecureVue can also receive information from other tools such as configuration management databases (CMDB), network monitoring, vulnerability assessment products and more.

Data collection points (SecureVue Collectors) can be located throughout the architecture, as close to the collection points as possible, to allow for our patent pending 15:1 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 can process tens of thousands of events per second and should be placed at strategic locations for redundancy. Since each Regional Server is a stand-alone system, placing additional Regional Servers in the architecture enables linear scaling of the system.



SecureVue's database is a proprietary data store that was built specific for high speed insertion of data and extremely fast reporting capabilities. In a distributed architecture, data can be stored in one centralized data store (which can be fully redundant) or throughout the network where Regional Servers are implemented. The security and integrity of the collected data in this distributed architecture is ensured through role-based access.

SecureVue offers the following features and benefits:

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
- Investigate: 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
- Integrate: complete integration with Nessus and Qualys

Configuration Analytics: collects, alerts, correlates, and compares configuration changes

- Asset Baseline: sets baselines to establish security configuration standards
- Policy Wizard: enables policies to be created 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 policies to be created
- 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 for elements including 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 organizations to automate incident identification to drive efficiency and reduce management complexity.

Compliance:

CERTIFICATIONS & ACREDITATIONS

SecureVue 3.x FIPS 140 Level 2	JUNE 2008
NIAP EAL2	SEPT 2008
Army DIACAP	AUG 2008
U.S.-based company	World HQ Acton, MA

SUMMARY

Organizations that have specific initiatives for their Network Operations and Security Centers or are developing and updating their compliance strategies should test SecureVue against other tools being considered. The eIQnetworks Proof of Concept Guide provides very detailed and specific checklists to help guide organizations to evaluate all the key benefits, value and cost savings of SecureVue. We believe SecureVue delivers the most cost effective and comprehensive technical solution that is on the market today and welcome opportunities to prove it.

Many customers tell us that 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 enjoy demonstrating exactly that in each customer environment, matched to the specific initiatives, requirements and projects of each organization.

ADDITIONAL INFORMATION

About eIQnetworks

eIQnetworks, Inc., is redefining security and compliance management by fostering collaboration across security, network, data center and audit teams to more quickly isolate the root cause of security issues and ensure compliance mandates are being enforced. Global financial, media, healthcare, manufacturing, and government enterprises rely on eIQnetworks to make sense of formerly disparate data sources to react faster to emerging threats, automate their compliance efforts, and more effectively monitor security policies. Headquartered in Acton, Mass., eIQnetworks is located online at www.eIQnetworks.com and can be reached at +1 877.564.7787.

World Headquarters
31 Nagog Park
Acton, MA 01720
(978) 266-9933