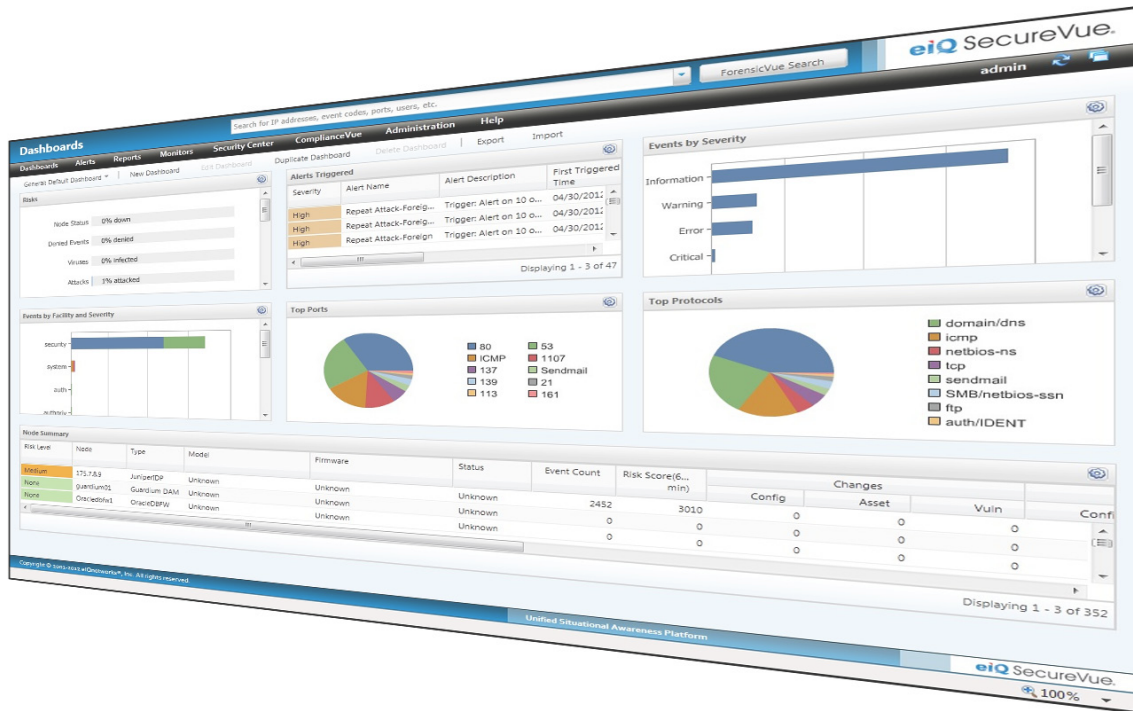




Product Data Sheet



SecureVue®

The Unified Situational Awareness PlatformSM

SecureVue unifies next-generation SIEM, security configuration auditing, compliance automation and contextual forensic analysis into a single platform, delivering situational awareness, operational efficiency and the lowest total cost of ownership (TCO) for large enterprises.

Product Description

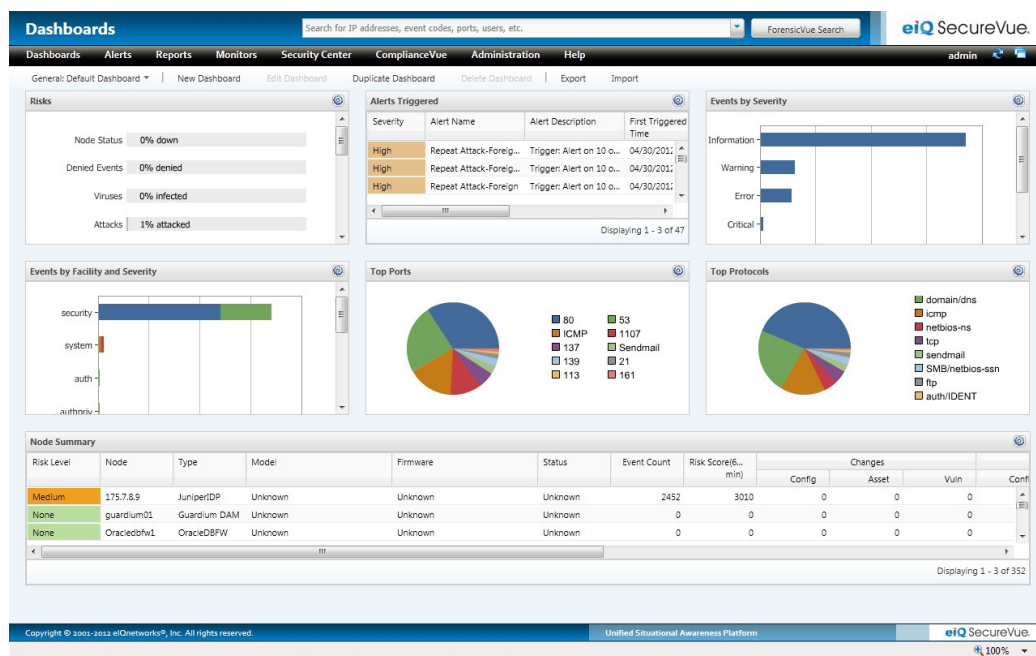
elQnetworks' SecureVue® is the first unified situational awareness platform to provide complete visibility and clarity across all enterprise data to address today's critical information security and compliance needs. SecureVue overcomes the information gap inherent in "best-of-breed" products by capturing, analyzing and correlating all security and compliance-related information from network devices, hosts and operating systems and applications in a single solution.

Unlike individual point products, SecureVue seamlessly captures the full range of enterprise security data, eliminates background noise and delivers a complete view of the enterprise to achieve true unified situational awareness. SecureVue natively collects, aggregates, analyzes, correlates and reports on all security and compliance data.

Best of all, SecureVue works with the investments already made in security and compliance technologies, allowing organizations to leverage the data from existing point products to gain a complete understanding of what's going on in enterprise environments. Using a built-in SDK (software development kit), SecureVue can easily capture data from third party tools such as CMDB, SIEM, configuration audit, and end-point security and systems management platforms.

SecureVue helps organizations solve their critical information security and compliance challenges by providing a comprehensive security and compliance platform that enables them to:

- **Combat increasing cyber attacks** and **address new compliance mandates** like never before
- **Reduce complexity** and minimize effort and operational overhead required to manage security and compliance for improved operational efficiency
- **Lower operations and management costs** for security and compliance by integrating multiple technologies into a single, unified platform and leveraging existing technologies
- **Achieve true unified situational awareness** by having complete visibility across all of the enterprise and eliminating information silos



SecureVue dashboard, displaying a broad range of security information collected from events, asset data, configuration changes, network traffic analysis, performance metrics, and more

SecureVue Key Functions

Next-Generation SIEM

SecureVue delivers all the capabilities needed for proactive security monitoring and protection including log management, SIEM (Security Information and Event Management), configuration analysis, netflow analysis, file integrity monitoring, removable media monitoring, performance monitoring and vulnerability analysis. It correlates across multiple data types from multiple data sources to proactively identify new and evolving threats such as advanced persistent threats (APTs), cyber attacks, identity and intellectual property theft and many more.

NEXT-GENERATION SIEM

- Natively collect all security and compliance-related data, including logs and other events, asset data, configuration state, network traffic analysis, performance metrics, and more
- Correlate and visualize the inter-relationships between different security data elements to detect APTs, malicious insiders and other threats
- Establish the true context of security incidents and abnormalities

COMPLIANCE AUTOMATION

- Monitor and report against regulations, best practices and standards
- Provide a single comprehensive report that includes all compliance data
- Lower TCO of compliance automation by up to 50% over a 3 year period

Compliance Automation

SecureVue provides unmatched comprehensive compliance automation to centralize monitoring and reporting against regulations, best practices and standards for information security, dramatically reducing the time required to attest the state of security controls across the enterprise to internal and external auditors. SecureVue's comprehensive compliance library includes: ISO 27001/2, FISMA/NIST 800-53, CoBIT, SOX, GLBA, HIPAA/HITECH Act, PCI-DSS, NERC CIP, CIS Benchmarks, DISA STIGs and others.

Security Configuration Auditing

SecureVue provides comprehensive configuration auditing across hosts, network and security devices, and applications to help organizations implement prescriptive configuration standards such as CIS Benchmarks, DISA STIGs and customized minimum security requirements (MSRs). This helps improve overall security and proactively identify misconfigured systems, policy violations as well as unauthorized changes across the enterprise. SecureVue provides the capability to monitor a broad spectrum of controls.

SECURITY CONFIGURATION AUDITING

- Implement and continuously monitor prescriptive configuration standards including CIS and DISA STIGs
- Identify misconfigured systems, policy violations and unauthorized changes
- Improve cyber security posture with secure system configurations up to 50% over a 3 year period

FORENSIC ANALYSIS

- Reduce root cause discovery times by up to 60%
- Investigate complex security incidents in minutes or seconds
- Deliver full contextual forensic analysis across multiple data types

Forensic Analysis

SecureVue allows organizations to perform detailed forensic analysis across all data by searching, reporting and analyzing all data from a single unified console. Security professionals can troubleshoot application problems, policy violations and misconfigured systems, and investigate security incidents in minutes or seconds as well as correlate and analyze complex events that span thousands of systems. Security professionals can also meet compliance mandates at a much lower cost, and reduce the time to root cause discovery by up to 60%.

SecureVue Data Collection Capabilities

Native, Out-of-Box Collection

SecureVue intelligently collects and correlates all relevant security and compliance data including events, configurations, asset, vulnerability, performance, netflow and security controls to proactively detect cyber attacks and policy violations. SecureVue supports the collection of a variety of data from hundreds of devices and vendors including:

- **Events** - collect logs and other event data from any network devices, security devices, servers, desktops, databases and applications; all data is compressed and stored in both normalized and raw formats
- **Configuration Data** - agentless collection of configuration data from network devices, security devices, servers and desktops, including the ability to import SCAP-compliant policies for DISA STIGs, CIS Benchmarks and other content
- **Asset Data** - agentless collection of asset data from network devices, security devices, servers and desktops
- **Performance and Availability Data** - collect all performance and availability data from any node across the enterprise using SNMP MIBs and traps, WMI, and other protocols
- **Vulnerability Data** - collect data from all leading vulnerability scanners and use built-in integration with leading vulnerability scanners to schedule scans from within the SecureVue console
- **Netflow Data** - collect a broad range of flow data for traffic analysis, including C-Flow, J-Flow, S-Flow and others
- **File Integrity Data** - collect file integrity data in real-time without the need to enable file auditing on Windows servers
- **Removable Media Data** - collect removable media (USB) data in real-time, including device insertion and removal, file transfers and full user context
- **User Activity Data** - associate individual user identities with one or more accounts across different systems, and track all activity based on the actual identity of the user
- **Universal Parser** - supports any non-standard logs via a simple GUI interface

Software Development Kit (SDK)

SecureVue's SDK enables application developers to retrieve and insert information from and into SecureVue quickly and securely. To meet the various needs of customers and partners, SecureVue's SDK provides a comprehensive, simple-to-use set of XML-based tools for application developers. The SDK allows organizations to tailor SecureVue to particular needs, streamline and automate processes and integrate external applications. Built on a standards-based and extensible platform, the SDK lets organizations leverage development team's existing skills and quickly build solutions that bring tangible value to customers.

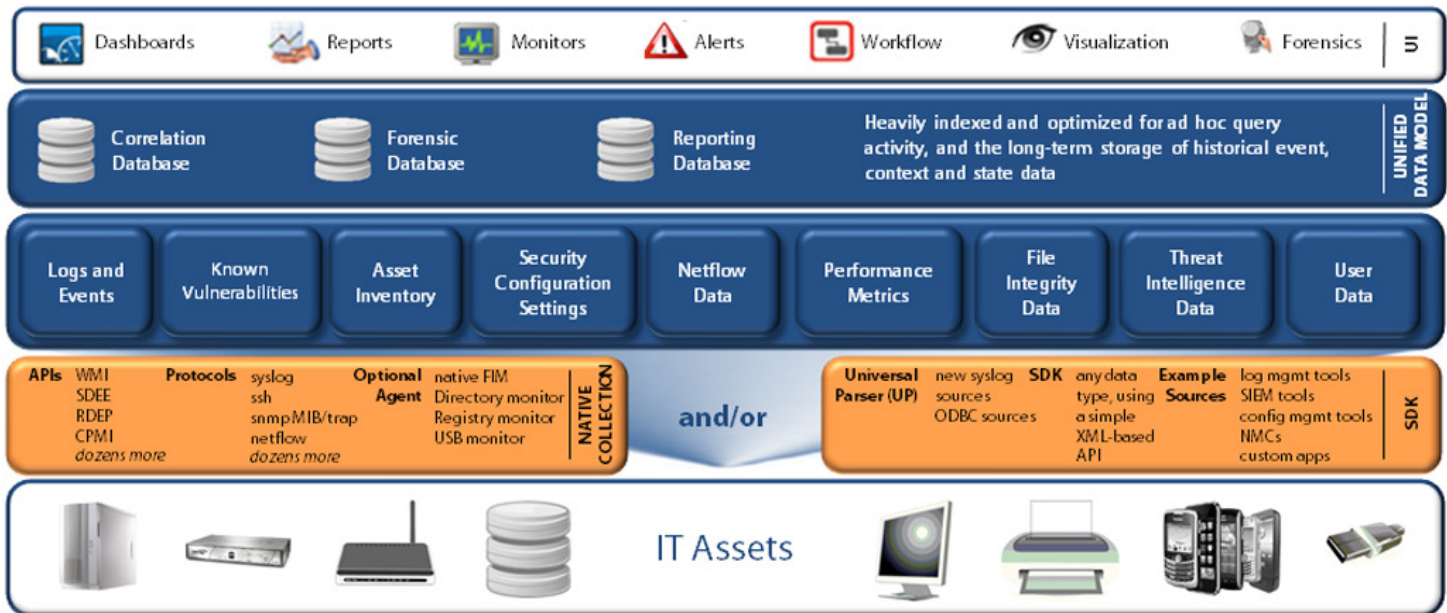
Key features of the SecureVue SDK include:

- Ability to integrate any applications that use ODBC compliant SQL databases and/or output data in SecureVue's fully-documented XML schema
- Provision bi-directional APIs for reliably and securely retrieving and inserting data from and into SecureVue
- Comprehensive package including the SDK tool, documentation and sample code for development and debugging assistance

SecureVue Product Architecture

eIQnetworks has pioneered a new and efficient solution to address the challenges of information security professionals. SecureVue provides a high-performance, massively scalable platform that ensures the security and confidentiality of both internal information and critical customer data. SecureVue is scalable to the largest and most demanding global enterprises. eIQ's unified situational awareness platform provides organizations with a robust architecture to to:

- Assess the effectiveness of various security technologies
- Leverage existing infrastructure investments including CMDB, end point protection tools, SIEM and log management products, and others
- Access, correlate and analyze all information without "blind spots" due to lack of visibility, all with a single console
- Understand how information relates including identifying anomalies and violations, eliminating false positives and establishing clarity to make sense of all data



Supporting standalone and distributed architectures, SecureVue scales to collect all data from network devices, systems and applications. With the capacity to process over one million events per second across thousands of nodes in a distributed architecture, SecureVue delivers optimal performance to meet the requirements of even the most demanding commercial enterprise, government and managed security service provider (MSSP) customers.

CERTIFICATION AND ACCREDITATION

SecureVue has achieved certification and validation for a broad range of federal and commercial standards:

- NIAP Common Criteria, EAL 2+
- NIST FIPS 140-2, Level 2
- NIST SCAP
- Certificate of Worthiness (CON), United States Army
- DISA Unified Capability Approved Product List (UC-APL)

SecureVue Features and Benefits

Feature	Benefit
Gain Situational Awareness	eIQ's SecureVue lets you see exactly what is happening within your infrastructure and adjust on-demand, allowing immediate focus on any anomalies. Situational awareness improves threat detection capability while reducing response and root cause discovery times.
Expandable, Open Platform	SecureVue's open, extensible architecture creates a flexible deployment environment that allows new plug and play applications as needed. Tie IT systems and change management tools into SecureVue and automate tasks, policies and workflows across SecureVue and third-party products.
Integrated Architecture to Collect and Aggregate All Data	SecureVue collects, correlates, archives, analyzes and reports on all security data, including log/event data, configuration data, asset data, performance and availability data, vulnerability data, netflow data, file integrity data, removable media data and security controls data across the enterprise.
Cross-Correlation to Detect Cyber Attacks and Policy Violations	SecureVue ships with over 500 correlation policy templates that are designed to detect anomalies and policy violations in real-time. By automatically cross-correlating multiple data types, SecureVue uniquely provides the capability to discover hard-to-detect attacks early, ensuring that organizations can minimize data loss or system-wide failure.
Scalable to Largest and Most Demanding Global Enterprise Infrastructures	SecureVue's advanced architecture supports massive hierarchical deployments ranging from one to six tiers of data collection - all from a single code base. With the capacity to process over 15,000 events per second in a standalone deployment, and over 1,000,000 events per second (EPS), >1,000,000 flows per second (FPS) across >1,000,000 nodes in a distributed implementation, SecureVue delivers optimal performance to meet the requirements of even the most demanding commercial enterprise, government and managed security service provider (MSSP) customers.
Detailed Compliance Reporting	Providing over 1,500 security and compliance metrics-based reports, SecureVue gives visibility into infrastructure activity across lines of business, locations and applications. Reports provide extensive drill-down capabilities that allow users to quickly go from big-picture summary data to specific security, risk and audit management details.

Feature	Benefit
Single Unified Console Delivers Operational Efficiency and Cost Savings	SecureVue provides an enterprise-wide view of security and compliance status from a single unified console. Data from multiple point products can be aggregated and correlated using SecureVue SDK, enabling users to speed incident identification and provide root cause analysis, fostering collaboration between NOC, SOC and compliance teams, resulting in reduced compliance costs and efficient operations.
Full Contextual Forensics Analysis Reduces Root Cause Analysis Time	SecureVue's flat-file data storage, coupled with the industry's first multi-data single search forensics engine, delivers a fast, optimal method to investigate any incident and obtain all relevant data to understand the root cause of an incident in a manner of minutes and hours, instead of days and months. eIQ's ForensicVue, an integrated component of the SecureVue platform, can eliminate "conference room syndrome" and reduce the investigative analysis time by up to 60% versus alternative options.
Comprehensive, Real-Time and Interactive Dashboards	With over 50 built-in and customizable dashboards, SecureVue provides executives with high-level summary reports while allowing IT professionals to easily drill-down into the more complex details of monitoring, alerting, reporting and forensics.
Role-based Access Control Allows for Segregation of Duty	With integrated LDAP and Active Directory support as well as data segregation, SecureVue allows multiple users to obtain their own view of the system based on their role and permissions. Service providers and MSSPs can segregate each customer's data, making SecureVue the best solution for multi-tenant environments. This role-based approach to security ensures that SecureVue provides the appropriate separation of duties mandated by many regulations, best practices and information security standards.
Encrypted and Compressed Data Archive	SecureVue collects and aggregates on a SAN, NAS, DAS or WORM storage in encrypted and compressed (18:1 compression ratio) format to meet data retention and data integrity requirements.
Automated Auditing of Security Controls Helps Respond to Problems	SecureVue helps implement, monitor and report on security controls to help organizations automate compliance programs to meet current and new compliance requirements, including prescriptive security controls. By leveraging a single platform and consolidated compliance reports and controls, organizations can reduce their compliance costs and reduce organizational risk.

SecureVue Product Specifications

SecureVue is distributed either as user-installable software, or on security-hardened Intel®-based appliances. The following tables identify the specific hardware included with SecureVue appliances, and also represent the minimum recommended hardware specifications for SecureVue when installed on customer premise equipment.

SecureVue Server

Component	Description
Processor	Dual Intel® Xeon® Quad Core 2.8 GHz
Memory	16GB DDR3 SDRAM
Storage	3 TB 15K RPM SATA-3 Drives (RAID 5)
Operating System	Windows Server 2008 Standard 64-bit
Network Interface Card	(2) Dual-Redundant 10/100/100GB Ethernet (4 interfaces total)
Integrated Lights-Out (ILO) Card	Yes
Form Factor	2U, EIA/TIA rack mountable

SecureVue Data Collector

Component	Description
Processor	Single Intel® Xeon® Quad Core 2.8 GHz
Memory	4GB DDR3 SDRAM
Storage	1 TB 7200 RPM SATA-3 Drives (RAID 5)
Operating System	Windows Server 2008 Standard 64-bit
Network Interface Card	(2) Dual-Redundant 10/100/100GB Ethernet (4 interfaces total)
Integrated Lights-Out (ILO) Card	Yes
Form Factor	1U, EIA/TIA rack mountable

About eIQnetworks

eIQnetworks delivers unified situational awareness solutions for the largest enterprises around the world, including government, financial, telecommunications, retail and healthcare. The company's flagship solution, SecureVue®, is the only platform to provide a more accurate, in-depth view of an organization's security and compliance position via a single console through comprehensive, real-time security monitoring, compliance automation, configuration auditing and forensic analysis. Vital to the protection of an organization's infrastructure, the company's solutions proactively protect against cyber attacks, detect breaches and policy violations and respond to incidents and security controls, dramatically reducing total cost of ownership. eIQnetworks is a privately held company headquartered in Acton, Mass. For more information, visit <http://www.eiqnetworks.com>, e-mail us at sales@eqnetworks.com, or call us at +1.877.564.7787.



eIQnetworks
31 Nagog Park
Acton, MA 01720
t. +1 978.266.9933
f. +1 978.266.0004
www.eiqnetworks.com



© 2012, eIQnetworks, Inc. eIQnetworks, the eIQnetworks logo and SecureVue are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.