



SecureVue[®] Express





PRODUCT DESCRIPTION

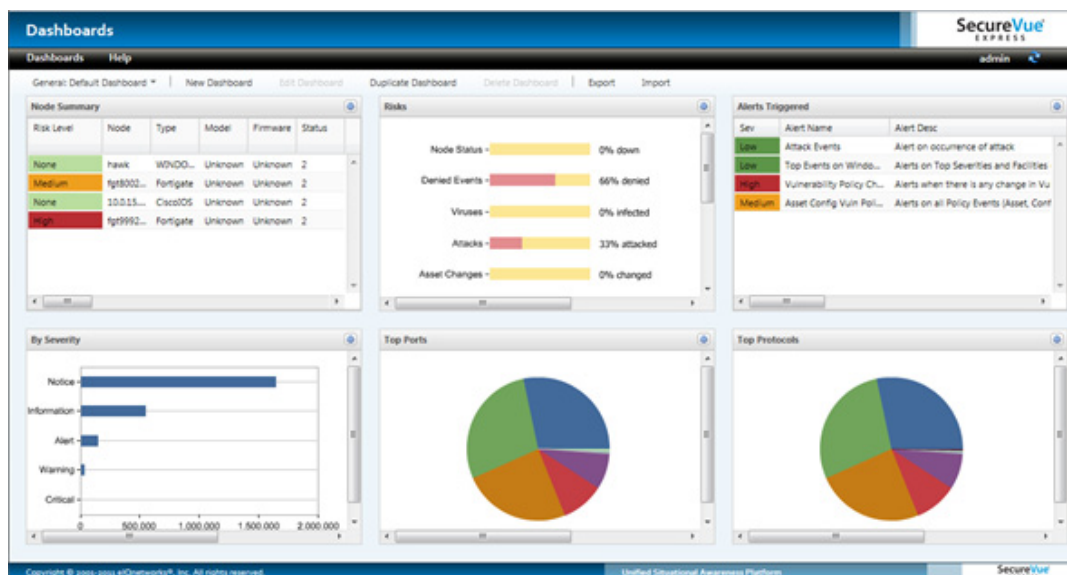
SecureVue Express® from eIQnetworks provides users with a powerful set of features derived from our industry leading situational awareness platform, SecureVue®. With SecureVue Express, eIQnetworks has given customers a risk-free way to take their first steps toward achieving a proactive and comprehensive understanding of what is taking place in their IT environments. SecureVue Express helps customers understand the benefits of overcoming the information gap inherent in “point security” products by capturing, analyzing and correlating all security and compliance-related information from network devices, hosts, operating systems and applications in a single solution.

Unlike traditional point products such as SIEM and log management that collect and analyze only event-based data such as logs, SecureVue Express delivers:

- **All Security Data.** SecureVue Express collects and analyzes all security and compliance data including logs and other event-based data, asset and configuration state, netflow data, known vulnerabilities, performance metrics, and more, all in a single platform.
- **Cross-Correlation of All Security Data.** SecureVue Express correlates all security information using a single, integrated correlation engine to identify cyber attacks such as APTs that a traditional SIEM might fail to detect.
- **Log Management and SIEM.** By automatically collecting and correlating logs and other event-based data from heterogeneous IT infrastructure components, hosts or applications, SecureVue Express can generate actionable alerts and reports that assist enterprises in meeting compliance mandates requiring log aggregation and analysis.
- **Configuration Audit.** SecureVue Express detects configuration changes across hosts, network devices and applications, and presents current and historical configuration snapshots detailing changes and trends to identify policy violations.
- **Asset Analysis.** SecureVue Express centralizes archiving, tracking and management of hardware and software, and identifies unauthorized software installations that point to potential problems such as malware outbreaks.
- **Network Flow Analysis.** SecureVue Express provides true network behavioral analysis by monitoring current and historical network performance, pinpoints issues, and alerting appropriate personnel on anomalous network traffic.
- **Forensic Analysis.** Using SecureVue express, security professionals can search across all enterprise security data in a single query and display data in time sequential fashion, mimicking the exact actions of an attacker or an incident.
- **Detailed Performance Metrics.** Using a broad range of standard protocols and services to identify system performance metrics -- from SNMP, SDEE and CPMI on network infrastructure devices, to WMI on Windows systems - SecureVue Express captures and correlates these different performance metrics into a single, seamless, comprehensive view.
- **Availability Dashboard.** SecureVue Express maintains an integrated availability dashboard, providing immediate notification when systems and components are having difficulty communicating; the straightforward “stoplight” (red, yellow and green colors) in the availability dashboard immediately notifies appropriate personnel when systems or components are unavailable for any period of time.

PRODUCT VERSION COMPARISON

	SecureVue Express	SecureVue
Collection, Analysis and Reporting		
Number of Supported Hosts and Devices	5	Unlimited ¹
Predefined and Custom Dashboards	✓	✓
Log and Vulnerability Data	✓	✓
Netflow Data	✓	✓
Performance and Availability Data	✓	✓
Configuration and Asset Data	✓	✓
Native File Integrity Monitoring		✓
Available Pre-Defined Compliance Policies		✓
User Directory Information		✓
Advanced Capabilities		
Forensic Analysis	✓	✓
Predefined and Ad Hoc Reporting	✓	✓
Custom Reporting		✓
Predefined Alerts	50	400+
Custom Alerts	✓	✓
User-Definable Parsers		✓
Role-Based Access Control		✓
Built-In Ticketing and Workflow		✓
Integration with Enterprise Service Management Applications		✓
XML Export API		✓
CIS Benchmark Configuration Auditing		✓
DISA STIG Configuration Auditing		✓
Compliance Automation (PCI DSS, SOX, FISMA, and more)		✓
Support for Custom Applications and Platforms		✓
Distributed Architecture for Scalability		✓
Maximum Events per Second	500	1 million+
SDK for Custom Integration		✓
Support		
E-Mail	✓ ²	✓
Knowledge Base	✓	✓
Telephone		✓



SecureVue Express offers rich analysis and visualization capabilities for enterprise security data

¹ Limited only by infrastructure capacity and licenses purchased

² No SLA offered (best-effort response)

SECUREVUE EXPRESS PRODUCT SPECIFICATIONS

Supported Device List

Category	Device
Switches, Routers, VPNs, and Network Devices	CheckPoint VPN -1 CISCO IOS Cisco FWSM (Firewall Services Module) Cisco NetFlow Cisco VPN Concentrator 3xxx Juniper ISG Juniper M20, 40e, 320 Juniper Netscreen 5GT, SXT, 25, 50, 2xx, 5xx, 5xxx Juniper Netscreen SSL VPN Juniper Routers M Series
Firewalls	CheckPoint Enterprise or Standard NGX CheckPoint Express (CI) CheckPoint FW1 CheckPoint Edge W32 and WU Cisco ASA Cisco Pix Firewall Fortinet Fortigate Palo Alto Firewalls
IDS/IPS	Cisco IPS Juniper Netscreen IDP SNORT IDS Sensor SourceFire
Gateways	BlueCoat Proxy SG
Vulnerability Scanners	Nessus Rapid7 NeXpose
Servers	Windows Servers Windows Desktops
Applications	Microsoft Exchange Server

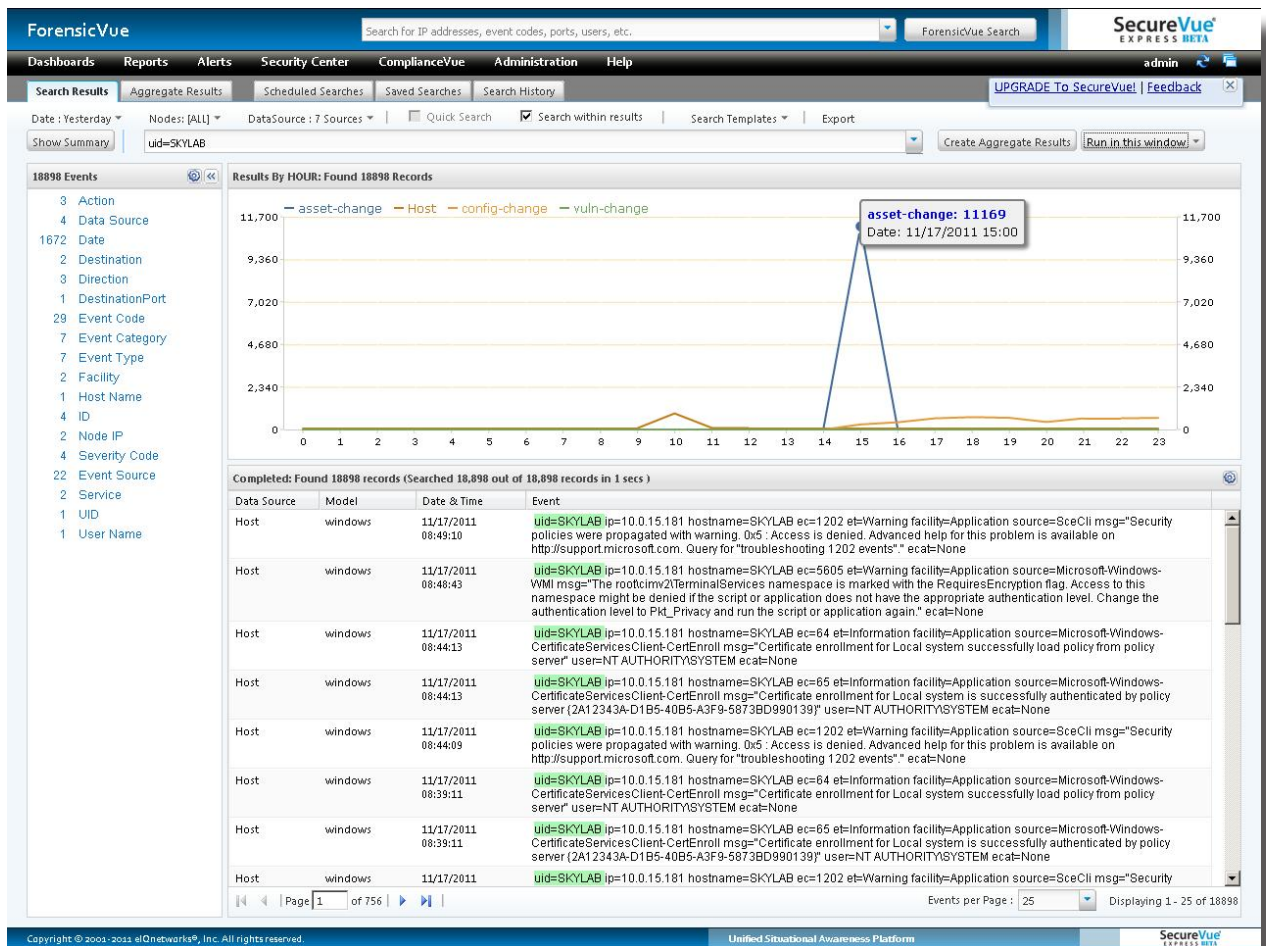
SecureVue Express Capacities and Limitations

Capacity	Description
Nodes (Hosts and Devices)	5 maximum (10 license re-allocations lifetime for SecureVue Express)
Alerts	25 simultaneously evaluated
History Archive	Limited only by available storage

SecureVue Express System Requirements

Component	Minimum Requirement
Processor	Intel x86 processor (or compatible), Dual-Core, 2.0GHz (or higher)
Memory	4 GB (or higher)
Storage	500 GB ¹ (7200 RPM SATA drives recommended)
Operating System	Microsoft Windows 7, Windows Server 2003 SP2, or Windows Server 2008
Network Card	10 Mbps ethernet (or faster)

¹ Additional storage may be required, depending on customer data retention requirements



ForensicVue, an integrated component of SecureVue Express, provides end-to-end security analysis

FOR MORE INFORMATION

To download your copy of SecureVue Express today, visit: www.eiqnetworks.com/SecureVueExpress.

To schedule a demo of SecureVue or to find out how unified situational awareness can help your enterprise, contact eIQnetworks at: sales@eiqnetworks.com



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