

SecureVue[®]

Evaluation Guide

Unified Threat and Compliance

Contents

SOLUTION OVERVIEW	4
INTENDED AUDIENCE	6
PRE-INSTALLATION CHECKLIST	7
STARTING SECUREVUE	8
CONNECTING DATA SOURCES	8
CONFIGURING ADDITIONAL DATA COLLECTION	11
USING SECUREVUE	13
ADMINISTRATIVE INTERFACE	13
Dashboards	13
Drilldown Topology	15
QuickVue	16
Correlation Policies and Alerts	18
Workflow	19
Profiles	20
SECURITY CENTER	21
Using Log Management	22
Vulnerability Analytics	23
Configuration Analytics	24
Assets Analytics	25
Performance Analytics	26
NBA Analytics and Flow Profiler	27
Availability	28
Quarantine	29
SNMP Traps	30
Comprehensive Reporting	31
Forensics Analysis	32
3-D Visualization	33
ComplianceVue	35
TROUBLESHOOTING	37
ABOUT EIQNETWORKS	38

Copyrights

COPYRIGHT, RESTRICTED RIGHTS AND TRADEMARK NOTICES

Copyright © 2001-2010 eIQnetworks, Inc. All rights reserved. Any redistribution or reproduction of any materials herein is strictly prohibited without obtaining the prior written permission of eIQnetworks, Inc..

This notice does not imply unrestricted or public access to these materials which are a trade secret of eIQnetworks, Inc. ("eIQ") and which may not be reproduced, used, sold or transferred to any third party without the prior written consent of eIQ. eIQ's software uses certain third-party libraries/software. The conditions and restrictions required of software users by the owners of such Third Party Software are referenced in "THIRDPARTYLICENSEREADME.txt" under the application install path.

eIQnetworks® and SecureVue® are registered trademarks of eIQnetworks, Inc. All rights reserved.

ComplianceVue™ and QuickVue™ are trademarks of eIQnetworks, Inc. All rights reserved.

All other trademarks or registered trademarks are the property of their respective companies.

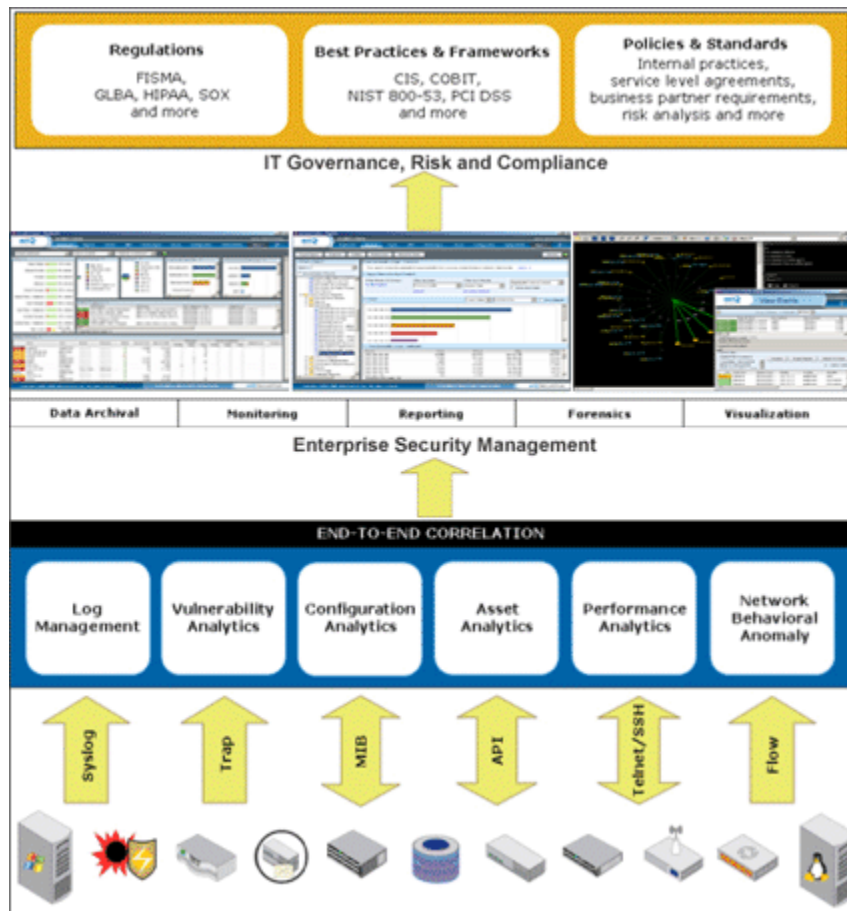
U.S. GOVERNMENT AGENCIES ONLY

The software described in this Documentation, and this Documentation itself, were developed at private expense and the software is 'commercial computer software' provided with RESTRICTED RIGHTS. Use, duplication and disclosure by civilian agencies shall be in accordance with FAR 52-227-19(c) or other agency data rights provisions, as may be applicable. Use, duplication and disclosure by DOD agencies are subject solely to the terms of a Contractor/Licensor System Sale, Evaluation and License Agreement as stated in DFARS 227-7202. Unpublished - All rights reserved under the Copyright Laws of the United States. Contractor/Licensor: eIQnetworks, Inc., 31 Nagog Park, Acton, MA 01720-3424.

1. Solution Overview

As information technology becomes the nerve center of today's enterprise, organizations are under increasing pressure to meet security, risk and compliance challenges. Financial fraud and identity theft are on the rise. Security threats and targeted attacks are becoming more sophisticated and regulations in the private and public sectors continue to evolve. Growing concerns like these require stronger security policies, processes and controls. Tactical deployments of point solutions aimed at meeting single requirements are no longer enough. Forward-looking organizations are taking a more strategic approach and adopting security standards, best practices and integrated frameworks to mitigate long-term risk.

SecureVue from eIQnetworks is a leading IT security, risk and audit management platform that combines next-generation security information management (SIM) with governance, risk and compliance (GRC) to improve operational efficiency and reduce management complexity. Using an integrated model, SecureVue goes beyond traditional log-based SIM solutions to collect, correlate, archive, analyze and report on all critical security and compliance data. Through end-to-end correlation, SecureVue transforms volumes of log, vulnerability, configuration, asset, performance and flow data into actionable intelligence. Built-in network behavioral anomaly detection (NBA) automatically profiles flow data to identify anomalies.



Providing insight into the infrastructure's overall security, risk and compliance posture, SecureVue helps organizations make business decisions that improve the bottom line by:

- Consolidating and unifying disparate data silos
- Correlating IT security, risk and audit information
- Complying with numerous government and industry regulations
- Implementing security best practices and processes
- Collaborating between NOC, SOC and compliance groups
- Automating processes to increase operational efficiency
- Reducing time to identify and fix security incidents

2. Intended Audience

This document was developed to assist evaluators who are planning to deploy SecureVue.

3. Pre-Installation Checklist

The checklist below has been created for standalone installations where both the data collector and SecureVue software are on the same system. For a distributed installation, please refer to the *SecureVue Deployment Guide*. Before starting the installation and evaluation please confirm:

- The evaluator has administrative access to the device, systems and applications to be managed
- Devices to be managed are configured to direct syslogs the SecureVue system
- Telnet, SSH, SNMP and WMI have been enabled to collect configuration, asset and performance data

4. Starting SecureVue

Once the software has been successfully installed, you can start SecureVue by double clicking on the SecureVue icon that is placed on your desktop.

When asked for a username and password, enter the default "admin" username and password that was created during the SecureVue installation.

Connecting Data Sources

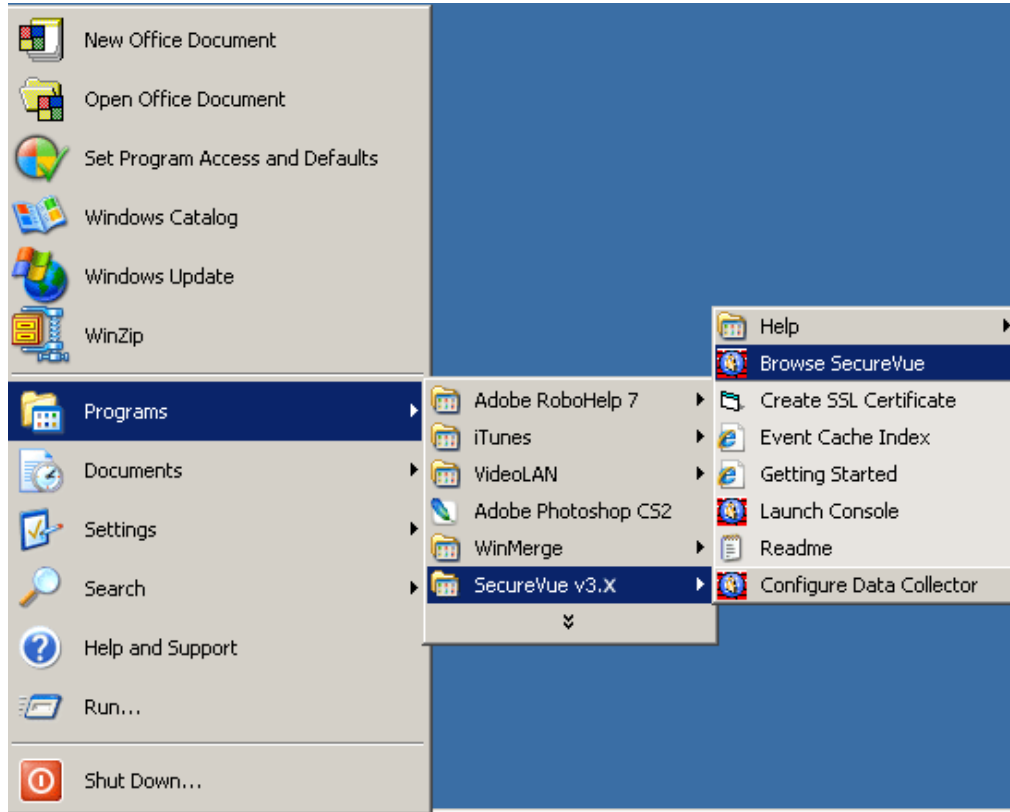
To get a comprehensive look at SecureVue, it is important to connect multiple data sources. Refer to the *eIQ Supported Device List* for a complete list of devices supported.

An important installation step during setting up an evaluation of SecureVue is making sure that the devices to be managed are known to the SecureVue application ("discovered"). A device can be discovered by SecureVue using any of the following methods:

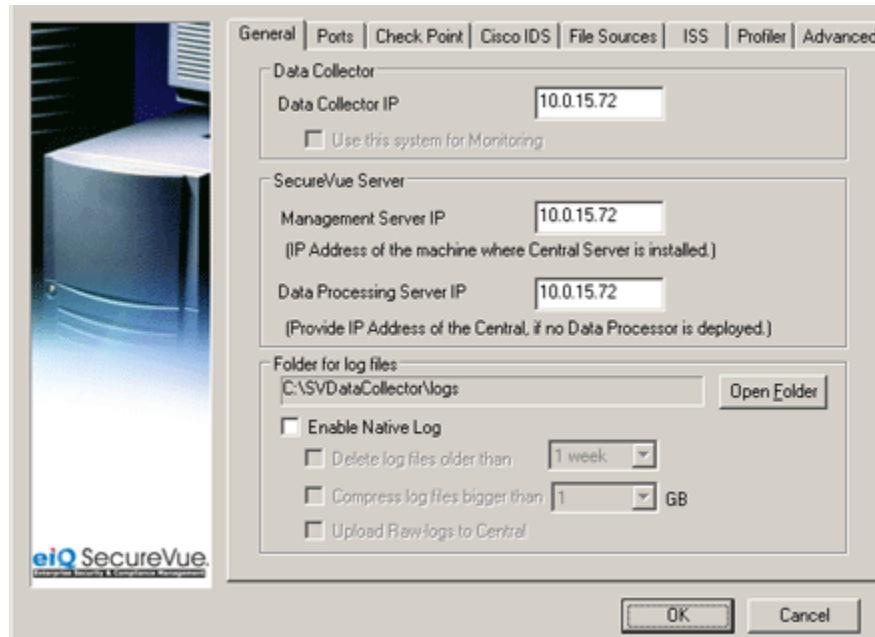
1. Directing syslog data to the system where SecureVue data collector is installed (systems that generate syslog)
2. Manually adding the device using the data collector interface (all devices that do not stream syslog) or SecureVue user interface (Bluecoat only)
3. Once discovered hosts must be added via the Host Manager interface with the exception of Novell servers, which need to be added at the data collector interface

Devices that do not generate syslog and must be added manually using the data collector interface include: Checkpoint Firewalls (utilizes LEA), Cisco IDS (utilizes RDEP and SDEE) and ISS SiteProtector

When manually adding devices, the data collector user interface can be launched from the Windows Start Menu:



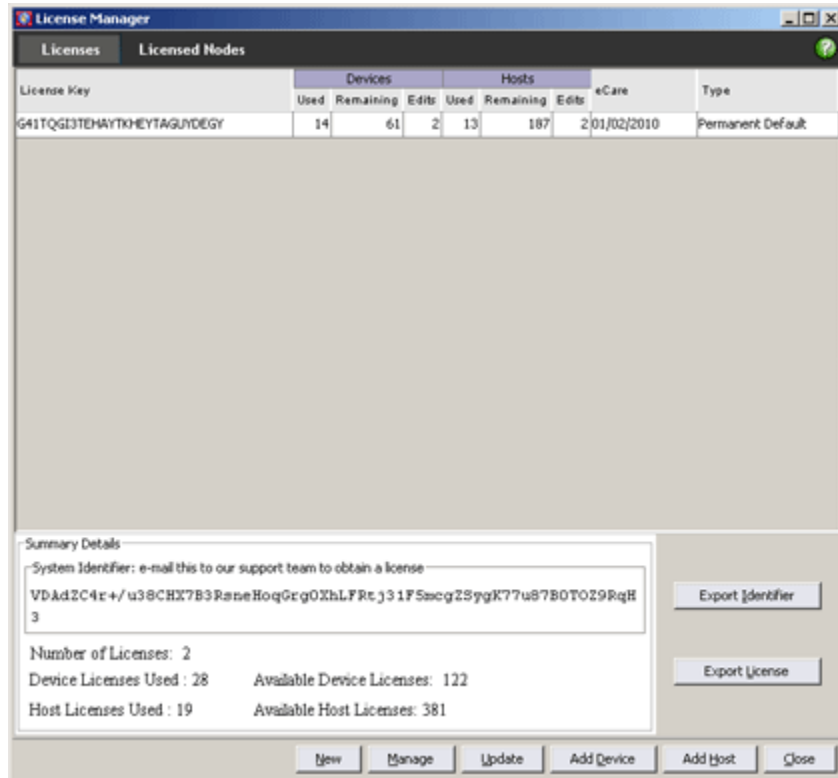
SecureVue Data Collector User Interface



Detailed instructions for manually adding devices can be found in the *SecureVue Deployment Guide*.

Once devices have been “discovered” by SecureVue they must be licensed in the product. After the License is acquired from the eIQ Support team and added in the License Manager, Nodes are licensed via the license manager which is available from the main SecureVue interface from the Setup menu.

From the license manager, nodes can be licensed via the “Manage” button once the device has been configured:



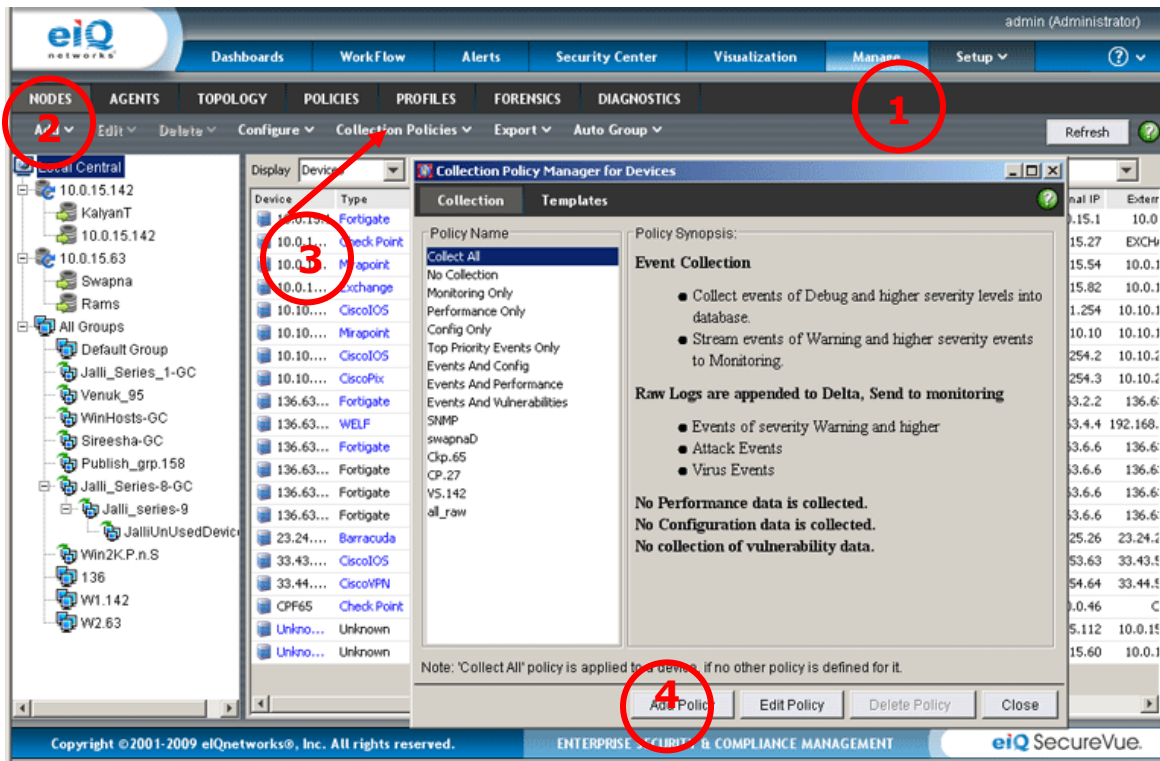
You can add a license for devices, hosts and applications from this user interface.

Please refer to the *SecureVue Deployment Guide* for more detailed information on setting up specific data sources or contact eIQnetworks support for further guidance.

5. Configuring Additional Data Collection

Once nodes have been licensed you are now ready to configure additional data collection capabilities, which include the collection of log, vulnerability, configuration, asset, performance and NBA data.

To configure additional data collection you must create a data collection policy for the node. This can be done from the "Manage" tab as shown below. Then by clicking on the "Nodes" tab and Selecting "Devices" or "Hosts".



1. Select the "Manage" tab
2. Select the Nodes tab
3. Select the Collection Polices button
4. Click on add or edit policy to configure a policy

From here you will be able to define the collection policy:

There are multiple data collection methods that can be defined in this dialog box:

- **Syslog events:** define filtering levels for data archival
- **Vulnerability scanner data:** define credentialed access to automate a Nessus scan
- **Performance data:** define SNMP community strings and/or credentialed access
- **Configuration:** define credentialed access and interval to collect configuration and asset data

Once the collection policies are defined and data collection has started you are ready to take advantage of alerting, monitoring, correlation, reporting and forensics capabilities of SecureVue.

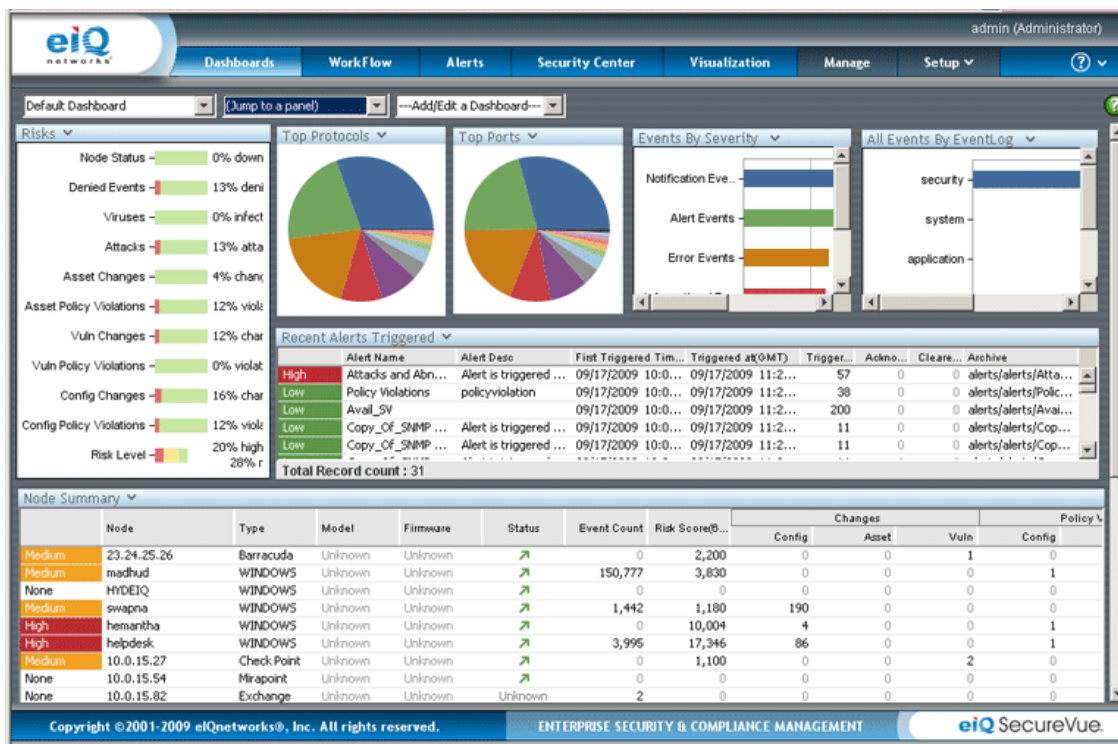
Note: Depending on the device/host, asset data is gathered from the performance and configuration settings.

6. Using SecureVue

Administrative Interface

Upon logging into SecureVue as admin you will see a dashboard. From this view you can access the log, vulnerability, configuration, asset, and performance and NBA data as well as begin utilizing the monitoring, alerting and reporting functionality.

Dashboards

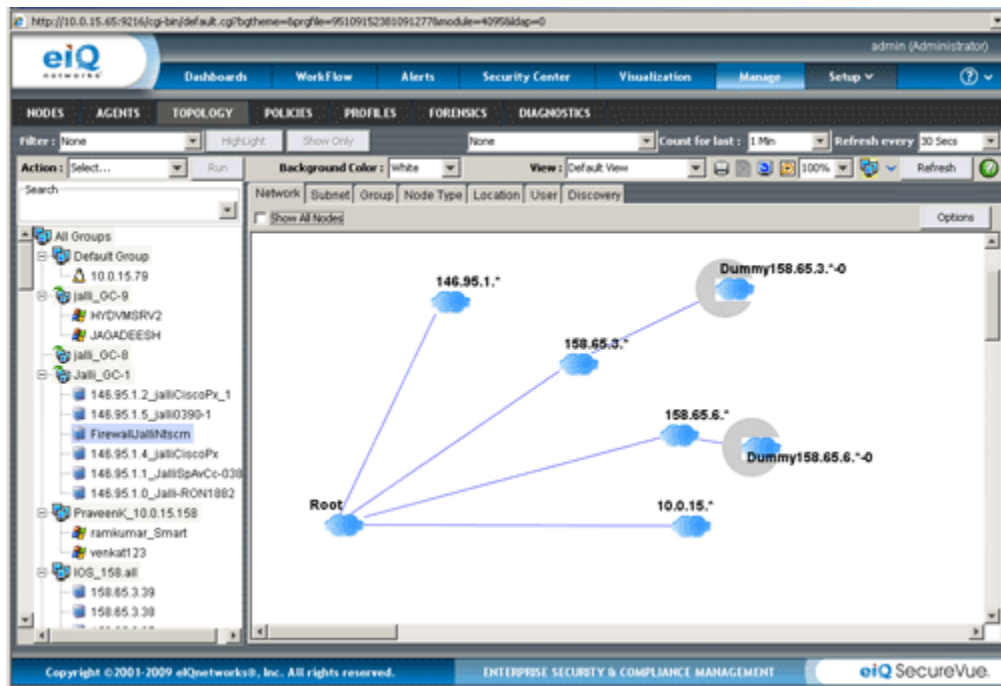


SecureVue ships with over 50 pre-defined dashboards. Each dashboard provides a real-time view into activity being monitored and contains data that is organized to meet specific user requirements. For instance, C-level dashboards contain high-level snapshots while operations dashboards detail more complex monitoring, correlated alerting, forensics and reporting data.

Users have the ability to modify existing dashboards as well as create new dashboards to provide a compelling, customized view of what's most important from a monitoring and reporting perspective. For example, a Administrator can configure a custom dashboard to provide such details as:

1. Compliance
2. Configuration changes
3. Asset changes

4. Device performance / throughput based on memory and CPU usage
5. Node status including 'up/down' information and risk scores
6. Netflow statistics
7. Most vulnerable nodes
8. Attack events against the network



Auto-Discovery

SecureVue can be used to automatically discover your network. You can choose how far back you wish to display this information as well as how often the screen refreshes. Right clicking on any node brings up a menu that allows you easy access to drilldown, forensic and policy violation data. Right clicking also provides access to filtered monitoring.

From the "Monitoring Center" window, you can double click any event to bring up a workbench. The workbench feature presents a structured view into all event detail as well as provides drilldown access to monitoring filters and forensics capabilities.

For example, if you are viewing an attack event on one of your devices, you could select the attackers source IP and pull detail from the last two weeks to see a detailed history into all activity particular to that user.

The drilldown feature is also available for select dashboard monitors. It allows for detailed information about what the monitor is actually telling you and allows you in some cases to access further forensic and filtered monitoring.

Drilldown Topology

The screenshot displays the eIQ Networks management console interface. The top navigation bar includes tabs for Dashboards, WorkFlow, Alerts, Security Center, Visualization, Manage, and Setup. Below this, a secondary navigation bar shows various functional areas: NODES, AGENTS, TOPOLOGY, POLICIES, PROFILES, FORENSICS, and DIAGNOSTICS. The main interface is divided into a left-hand tree view and a right-hand detail pane.

In the left-hand tree view, a node labeled "FirewallJallINscm" is highlighted with a red circle. This node is part of a larger structure under "IOS_158.all". The right-hand pane shows the "QuickVue" interface for the selected device, "FGT1002104201786_158". The QuickVue interface includes a "Summary" tab, a "Node Summary" table, and several summary cards for "Configs (OMT+5:30)", "Assets (OMT+5:30)", and "Vulnerabilities (OMT+5:30)". Below these are sections for "Forensic View" and "Event Viewer".

Node	Type	Model	Firmware	Status	Event Count	Risk Score
Total Record count : 1						

SNo	Date	Time	OMT Offset	Device Inter...	Device Exter...	Virtual Device	Device ID	Interface
Total Record count : 674								

From any dashboard users are able to access the "Topology" tab to view all of the devices and hosts being monitored. In this view, all security event information is displayed to provide a graphical view of security, risk and compliance posture. As such, the nodes are color-coded based on the last highest severity security event the device has experienced. Nodes can also be configured to be highlighted by risk score to highlight nodes that are potential security issues. Topology has more than 30 different views such as event severity, configuration changes, asset changes, configuration policy violations, asset policy violation, risk score, performance status, vulnerabilities, etc.

Users can right click on any node any and drilldown using "QuickVue" on any node to find out why the risk score is high, why there are so many emergency events, etc.

QuickVue

The screenshot displays the QuickVue interface for a device with IP 10.0.15.1. The interface is organized into several sections:

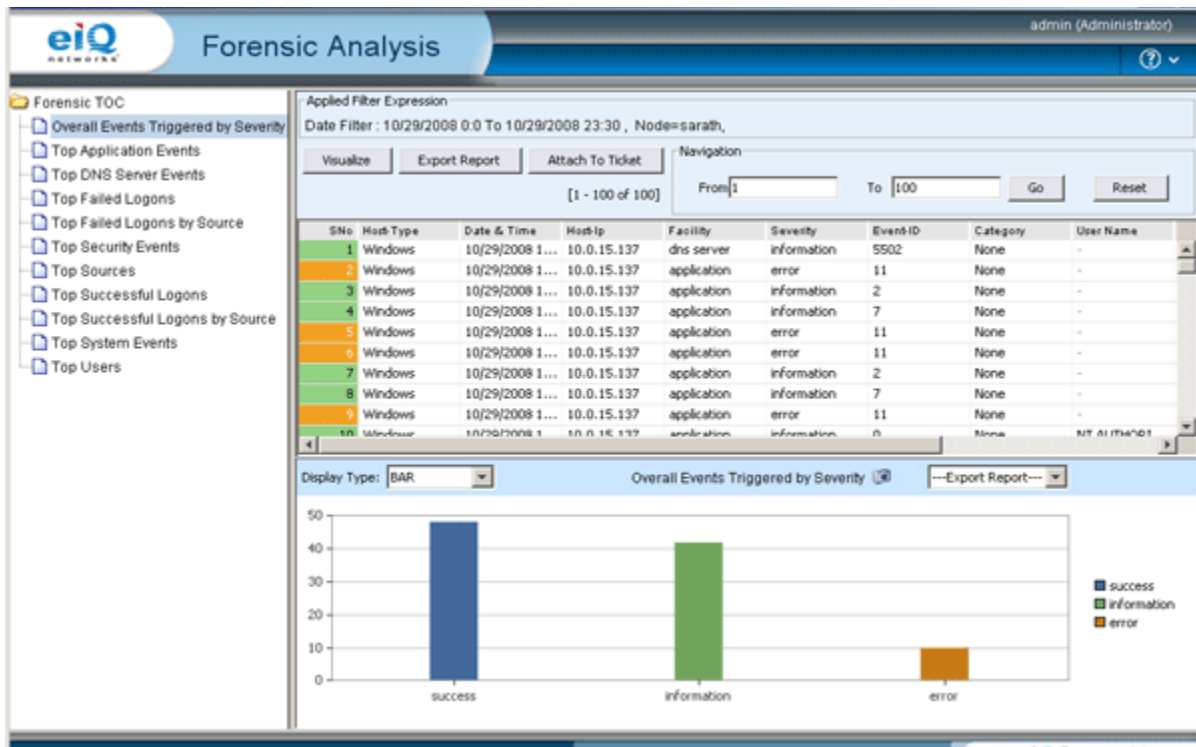
- Node Summary:** A table listing node details. The visible row is: Node: 10.0.15.1, Type: Fortigate, Model: Fortigate-1..., Firmware: Fortigate-1..., Status: (green arrow), Event Count: 3,476, Risk Score: 0.
- Configurations:** A section with buttons for 'Diff', 'View', and 'Policy History'. It shows two entries for 10/29/2008 at 12:32:26 (BL).
- Assets:** A section with buttons for 'Diff', 'View', and 'Policy History'. It shows two entries for 10/29/2008 at 12:32:31 (BL).
- Vulnerabilities:** A section with buttons for 'Diff', 'View', and 'Policy History'. It displays the message: 'No baseline set for 10.0.15.1' and 'No Vulnerability data for 10.0.15.1'.
- Forensic View:** Includes an 'Applied Filter Expression' box with 'Date Filter: 10/22/2008 00:00 To 10/29/2008 14:31, Device Filter: 10.0.15.1'. It has buttons for 'Visualize', 'Export Report', and 'Attach To Ticket'. A record count of '[1 - 1000 of 1000]' is shown.
- Event Viewer:** A table with columns: SNo, Date, Time, GMT, Device Interna..., Device Extern..., Virtual Device, Device ID, Interface. It shows three entries for 10/29/2008 at 14:00:03, 14:00:02, and 14:00:01.
- Event Viewer (Detailed):** A table with columns: Date & Time, Device/Host, Device/Host..., BII, Flow, Source IP, Destination. It shows three entries for 10/29/2008 at 14:31:52, 14:31:51, and 14:31:50, all with BII 0.000 and Source IP/Destination Unknown.

QuickVue™ presents all device and host details in one consolidated view. This view can be accessed by right clicking on any node within the SecureVue interface. Within the QuickVue window, the following tabbed information is available:

- **Summary:** shows node details such as up/down status, risk score, configuration changes, forensics and vulnerability details specific to the selected node
- **Dashboard:** displays panels related to the selected node, including ports, protocols, attacks, attack sources, bandwidth, node summary, event viewer and more
- **Configuration:** provides direct access to the Configuration portal, where you can compare configs and view reports in a single click.
- **Assets:** provides direct access to the Asset portal, where you can view the asset information of a nodes and view reports in a single click.
- **Vulnerability:** provides direct access to the vulnerability portal, where you can view vulnerability data and reports specific to the node selected

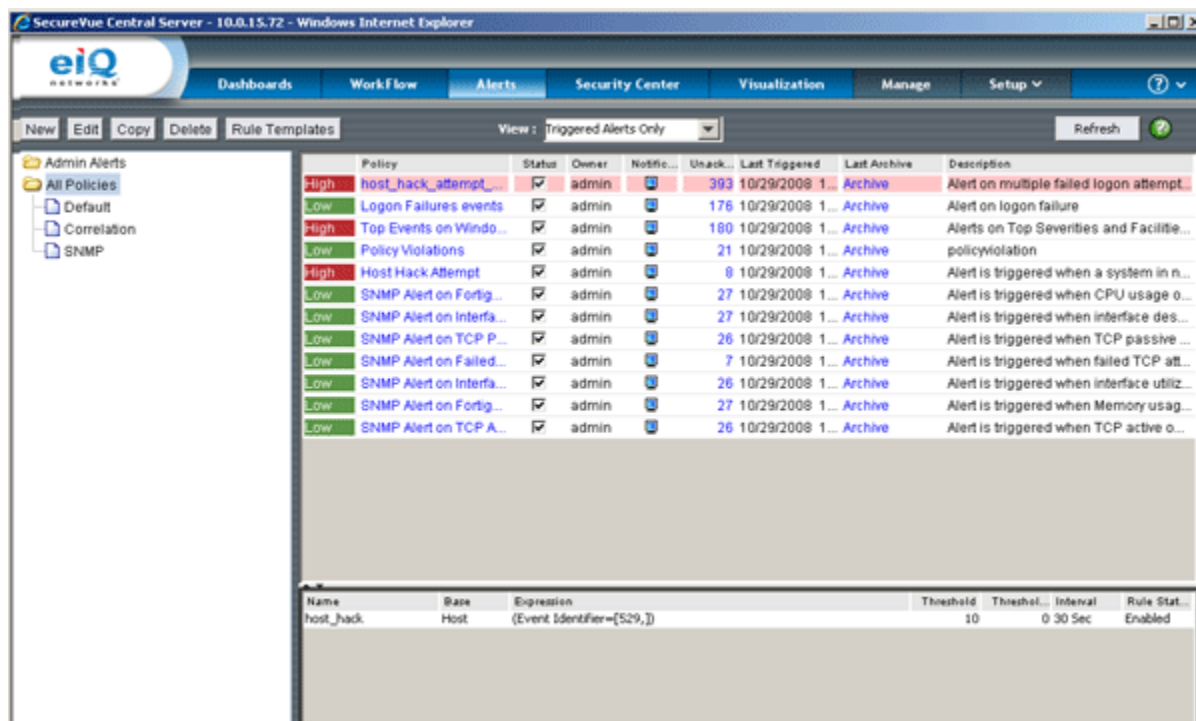
In QuickVue a user or security analyst can pinpoint why the risk score is high by drilling down through the workbench.

From the "workbench" window, users can run a forensic search to show exactly why the risk score was high. Users can also drilldown into reporting and monitoring from this window.



The above screen illustrates the results from the workbench forensic drilldown. These details show that an internal host was compromised, therefore causing the risk score to be high.

Correlation Policies and Alerts



Policy	Status	Owner	Notific...	Unack...	Last Triggered	Last Archive	Description
High host_hack_attempt...	<input checked="" type="checkbox"/>	admin		393	10/29/2008 1...	Archive	Alert on multiple failed logon attempt...
Low Logon Failures events	<input checked="" type="checkbox"/>	admin		176	10/29/2008 1...	Archive	Alert on logon failure
High Top Events on Windo...	<input checked="" type="checkbox"/>	admin		180	10/29/2008 1...	Archive	Alerts on Top Severities and Facilit...
Low Policy Violations	<input checked="" type="checkbox"/>	admin		21	10/29/2008 1...	Archive	policyviolation
High Host Hack Attempt	<input checked="" type="checkbox"/>	admin		8	10/29/2008 1...	Archive	Alert is triggered when a system in n...
Low SNMP Alert on Fortig...	<input checked="" type="checkbox"/>	admin		27	10/29/2008 1...	Archive	Alert is triggered when CPU usage o...
Low SNMP Alert on Interfa...	<input checked="" type="checkbox"/>	admin		27	10/29/2008 1...	Archive	Alert is triggered when interface des...
Low SNMP Alert on TCP P...	<input checked="" type="checkbox"/>	admin		26	10/29/2008 1...	Archive	Alert is triggered when TCP passive ...
Low SNMP Alert on Failed...	<input checked="" type="checkbox"/>	admin		7	10/29/2008 1...	Archive	Alert is triggered when failed TCP att...
Low SNMP Alert on Interfa...	<input checked="" type="checkbox"/>	admin		26	10/29/2008 1...	Archive	Alert is triggered when interface utiliz...
Low SNMP Alert on Fortig...	<input checked="" type="checkbox"/>	admin		27	10/29/2008 1...	Archive	Alert is triggered when Memory usag...
Low SNMP Alert on TCP A...	<input checked="" type="checkbox"/>	admin		26	10/29/2008 1...	Archive	Alert is triggered when TCP active o...

Name	Base	Expression	Threshold	Threshol...	Interval	Rule Stat...
host_hack	Host	(Event Identifier={529,})	10		0 30 Sec	Enabled

With powerful end-to-end correlation across log, vulnerability, configuration, asset, performance and NBA data, SecureVue enables users to define policies and alerts to automate the security management and monitoring process throughout the enterprise. Users can access over 200 out-of-the-box correlation templates via the "Policies" tab within the main console. Each of these templates can be customized to meet specific network requirements.

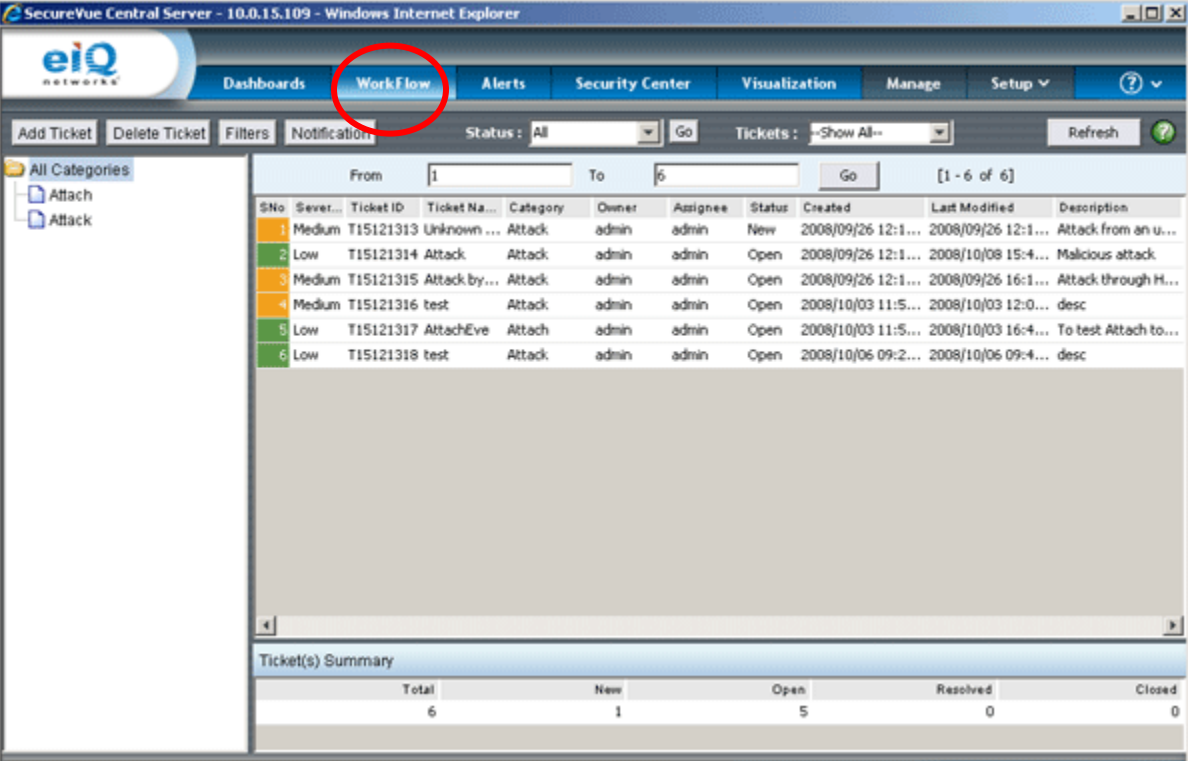
Policies allow users to define risk and quarantine rules based on all of the data SecureVue collects. This enables administrators to quickly address and correct issues by providing the ability to easily drilldown to determine the cause of devices and systems at risk. Users can create event class policies and establish filters to highlight suspicious activity.

Alerts enable you to set policies to watch for baselines and automatically notify when specific thresholds have been met or exceeded. For instance, you could set an alert to:

- Monitor all events that occur across firewalls and notify when a set of events are followed by a failed login attempt across server systems. This could be correlated with a successful login followed by an increase in CPU activity, which is indicative of a system breach.
- Monitor all traffic between devices and mission critical assets (e.g., databases) and notify when an attempt to connect outside of allowed ports occur.
- Monitor the network and notify when rogue application is loaded onto servers. Such an alert could be invaluable to stopping Trojans and keyloggers and preventing serious data breaches.

Please refer to the *SecureVue User Guide* for more detailed information on policies and alerts.

Workflow



The screenshot shows the SecureVue Central Server interface in a Windows Internet Explorer browser. The 'Work Flow' tab is highlighted with a red circle. The interface displays a list of tickets with columns for SNo, Severity, Ticket ID, Ticket Name, Category, Owner, Assignee, Status, Created, Last Modified, and Description. A 'Ticket(s) Summary' table is also visible at the bottom.

SNo	Sever...	Ticket ID	Ticket Na...	Category	Owner	Assignee	Status	Created	Last Modified	Description
1	Medium	T15121313	Unknown ...	Attack	admin	admin	New	2008/09/26 12:1...	2008/09/26 12:1...	Attack from an u...
2	Low	T15121314	Attack	Attack	admin	admin	Open	2008/09/26 12:1...	2008/10/08 15:4...	Malicious attack
3	Medium	T15121315	Attack by...	Attack	admin	admin	Open	2008/09/26 12:1...	2008/09/26 16:1...	Attack through H...
4	Medium	T15121316	test	Attack	admin	admin	Open	2008/10/03 11:5...	2008/10/03 12:0...	desc
5	Low	T15121317	AttachEve	Attach	admin	admin	Open	2008/10/03 11:5...	2008/10/03 16:4...	To test Attach to...
6	Low	T15121318	test	Attack	admin	admin	Open	2008/10/06 09:2...	2008/10/06 09:4...	desc

Ticket(s) Summary					
Total	New	Open	Resolved	Closed	
6	1	5	0	0	

Security analysis and administration depend on implementation of modules. Each module in SecureVue may be governed by one or more users. "Workflow" can automate the interactions among SecureVue users by providing a common platform where they can raise issues in the implementation by lodging and assigning tickets. SecureVue users can then take necessary actions based on the ticket to rectify the anomaly in the implementation, then update the ticket and close the ticket.

Workflow provides:

- Single point of contact for reporting local problems
- Identifies and analyzes what has happened including the impact and threat
- Researches solutions and mitigation strategies
- Shares response options, information, and lessons learned

Profiles

The screenshot shows the eiQ SecureVue interface. The 'PROFILES' tab is highlighted with a red circle. The main area displays a table of profiles with columns for Profile Name, Owner, Report Last Generated, and Reports. A detailed view for the 'praveen_21775' profile is shown at the bottom.

Profile Name	Owner	Report Last Generated	Reports
praveen_21775	admin	2009/09/12 18:42:20	complete report_praveend
compliance Word	admin	2009/09/15 14:29:05	CISwin2003DC_BySections
norma Word	admin	2009/09/16 11:06:26	custom
orma excel	admin	2009/09/15 11:12:38	custom
orma text	admin	2009/09/15 11:02:57	custom
orma csv	admin	2009/09/15 14:12:44	CISwin2003DC_AuditSummary
2	admin	2009/09/15 14:47:46	CISwin2000-L1_BySections
3	admin	2009/09/15 14:48:59	Sample_policy_BySections
123	admin	N/A	test142
AA	admin	2009/09/17 16:03:16	AA

Field	Value
Profile Name	praveen_21775
Data Source	Data Collector
Selected Nodes	ALL
DNS Lookup	Do not resolve IP addresses to host names
Filter Template	[NONE]
Report Type	single combined report for all selected Device/Host.

Profiles allow for processing of logs from manually added nodes. Users can choose filters that help narrow down data to the most needed information, thereby saving time and resources.

In addition users can schedule reports to automatically run and be delivered via screen, FTP or email. All reports are available in HTML, Text, PDF, MHTML, Excel and Word formats.

Security Center

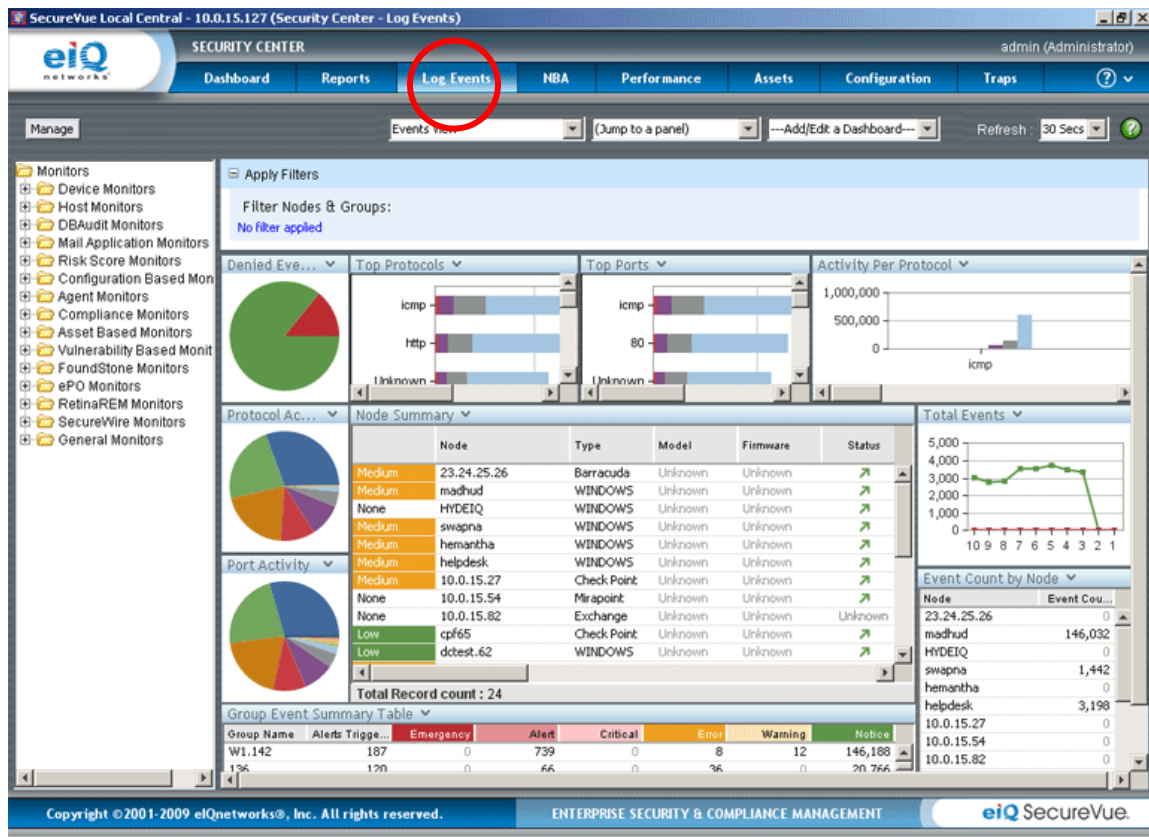
SecureVue's Security Center is a role-based portal that provides access to the following:

- **Log Management:** collects, archives and correlates event data across devices, servers and applications
- **Vulnerability Analytics:** scans assets on demand to identify, track and report system vulnerabilities
- **Configuration Analytics:** detects, correlates, alerts and reconciles configuration changes from all devices and servers
- **Assets Analytics:** tracks and analyzes all hardware, software and processes on all devices and servers
- **Performance Analytics:** monitors, collects and analyzes performance data from all devices and servers
- **NBA Analytics:** profiles all NetFlow, C-Flow, S-Flow and J-Flow data to identify and alert on anomalies based on resource utilization, applications usage and behavioral patterns
- **Availability:** User definable monitoring of availability of network and host resources
- **Quarantine:** Quarantine logs suspicious access into a resources based on policies.

In addition to collecting, correlating, archiving, analyzing and monitoring log, vulnerability, configuration, asset, performance and NBA data, the Security Center also provides access to:

- **SNMP Traps:** monitors, collects and analyzes performance data in real time from any MIB enabled node to detect, isolate and repair incidents before business is impacted
- **Comprehensive Reporting:** provides over 1,500 out-of-the-box reports that enable users to gain visibility into infrastructure activity by accessing network, system, application and security details
- **Forensics Analysis:** searches volumes of archived data across the enterprise to speed incident identification and remediation
- **3-D Visualization:** supports millions of nodes and allows users to view log data, security incidents, access control lists effectiveness, profiler data, node specific traffic patterns and forensics detail in an easy-to-understand graphical view
- **Audit Center:** provides enterprise-wide visibility and support for best practices and regulations (e.g. SOX, PCI-DSS, GLBA, HIPAA, FISMA, CoBIT, ITIL and ISO 17799)

Using Log Management



The "Log Events" tab within the Security Center provides detailed information about real-time log events taking place across all of the devices, hosts and applications being monitored. By clicking on any event displayed in the monitor, users can easily drill into and focus on important security events and incidents. This provides you the ability to monitor and manage all network traffic (e.g., devices, mission critical systems). You can also customize the dashboard to meet specific needs as well as add additional monitors by clicking on "Add Monitor" button.

Vulnerability Analytics

The screenshot displays the 'Vulnerabilities' tab in the SecureVue Local Central interface. The top navigation bar includes 'Dashboard', 'Reports', 'Log Events', 'NBA', 'Performance', 'Assets', 'Configuration', 'Vulnerabilities', and 'More'. The 'Vulnerabilities' tab is selected and circled in red. Below the navigation bar, there are tabs for 'Dashboard', 'Summary', 'Details', and 'Policies'. The main content area is divided into three sections:

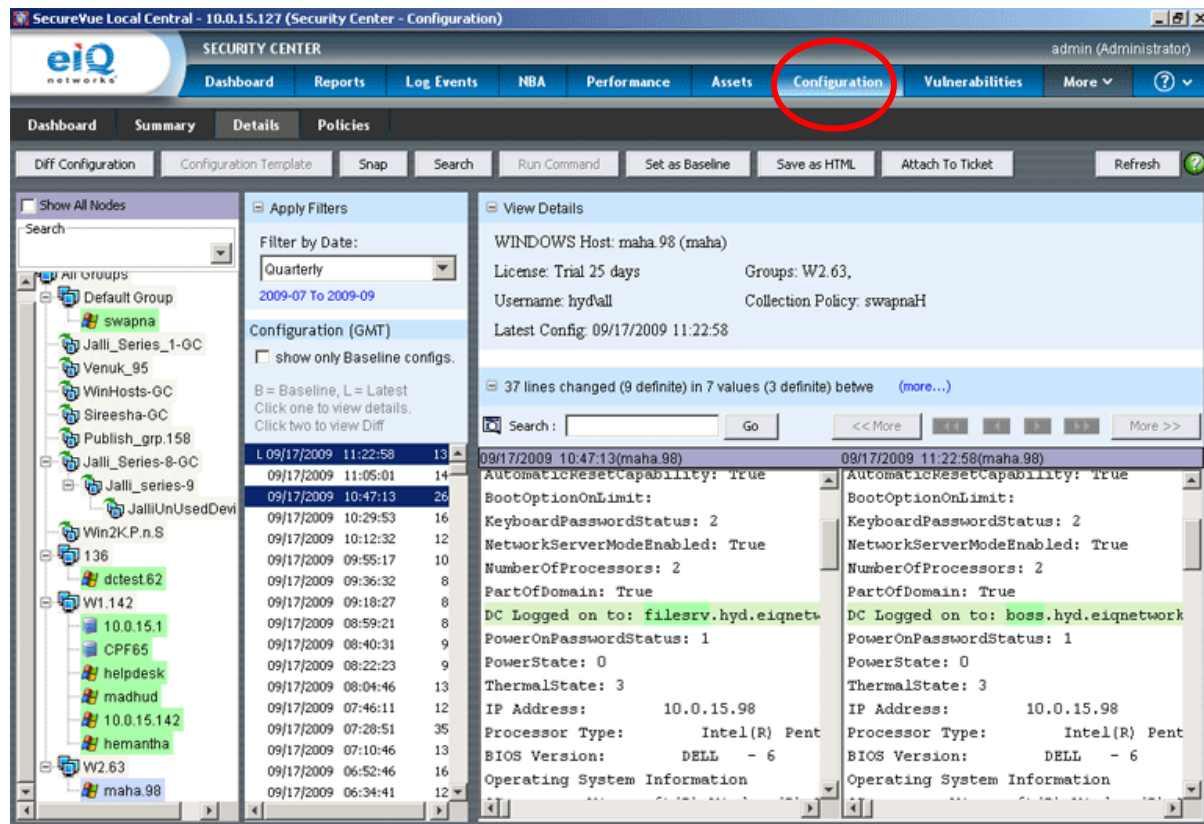
- Show All Nodes:** A tree view on the left showing a hierarchy of nodes, including 'All Groups', 'Default Group', and various host groups like 'Jalli_Series_1-GC', 'Venuk_95', 'WinHosts-GC', 'Sireesha-GC', 'Publish_grp.158', 'Jalli_Series-8-GC', 'Win2K.P.n.S', '136', 'dctest.62', 'W1.142', '23.24.25.26', '33.43.53.63', '33.44.54.64', '10.0.15.27', '10.0.15.1', '10.0.15.142', 'W2.63', and 'maha.98'.
- Apply Filters:** A section for filtering vulnerabilities by date (Quarterly, 2009-07 To 2009-09) and a checkbox for 'show only Baseline vulnerabilities'. It also includes a legend for 'B = Baseline, L = Latest' and instructions to click on items to view details or to view differences.
- View Details:** A pane showing details for the selected host 'dctest.62'. It includes information such as 'WINDOWS Host: dctest.62 (dctest)', 'License: Trial 25 days', 'Groups: 136', and 'Collection Policy: swapnaH'. Below this, it shows a comparison of vulnerabilities between two snapshots: '09/17/2009 06:58:38(dctest.62)' and '09/17/2009 10:58:50(dctest.62)'. The table below shows the changes:

Snapshot 1	Snapshot 2
SERVER~NOTE~10.0.15.62~general/icn	SERVER~NOTE~10.0.15.62~general/icn
SERVER~NOTE~10.0.15.62~general/tcp	SERVER~NOTE~10.0.15.62~general/tcp
SERVER~HOLE~10.0.15.62~general/tcp	SERVER~HOLE~10.0.15.62~general/tcp
SERVER~NOTE~10.0.15.62~ldap (389/t	SERVER~NOTE~10.0.15.62~ldap (389/t

The "Vulnerabilities" tab within the Security Center provides access to vulnerability information on network devices and hosts. SecureVue integrates with most commonly used vulnerability scanners to provide an in-depth look into open security issues across all devices and hosts.

All vulnerabilities can be tracked and alerted on via this module. This enables users to monitor and review the status of open issues and ensure that appropriate steps have been taken to secure mission critical systems. You can also configure alerts to automatically be sent when new vulnerabilities are discovered. Additionally, you can evaluate vulnerability status at various points in time by comparing vulnerability snap shots. In some cases, the vulnerabilities are connected to CVE database for more details.

Configuration Analytics



The “Configuration” tab within the Security Center provides access to information that allows users to monitor host and device configurations. When collecting configurations from IT assets, users can set the appropriate baseline configurations (known-good configuration) to measure other configurations against and alert when appropriate. When configuration changes are made, users can quickly drill into and review the differences.

Alerts can be defined to look for general changes or specific things such as inappropriate configuration changes. For example if a corporate policy does not allow “Telnet” then an alert can be set up to notify when a violation occurs. SecureVue will automatically scan all configurations snap shots to monitor for any nodes with telnet and send an alert.

Users can also easily get differences in configuration at two different points in time by using the comparison feature. This feature allows users to create specific configuration policies and alerts.

Furthermore, you can also run scripts to make configuration changes across one or multiple nodes.

Assets Analytics

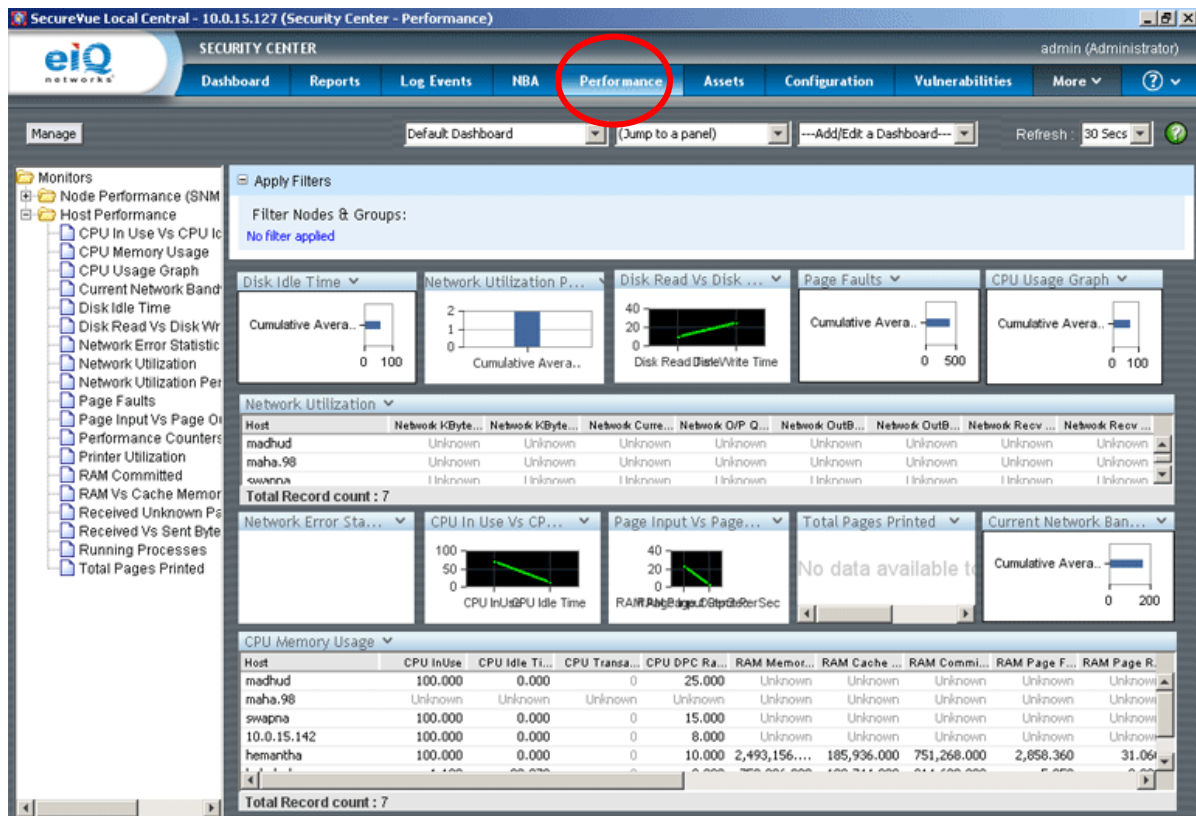
The screenshot shows the SecureVue Local Central Security Center interface. The 'Assets' tab is highlighted with a red circle. The interface is divided into several sections:

- Left Panel:** A tree view showing a hierarchy of assets. The root is 'All Groups', followed by 'Default Group'. Under 'Default Group', there are several sub-groups, including '10.10.254.3', 'Jalli_Series_1-GC', 'Venuk_95', 'WinHosts-GC', 'Sireesha-GC', 'Publish_grp.158', 'Jalli_Series-8-GC', 'Jalli_series-9', 'JalliUnUsedDev', 'Win2K.P.n.S', '136', 'dctest.62', 'W1.142', and '10.10.254.2'. The '10.10.254.2' group is expanded, showing individual assets like '10.10.1.254', '10.0.15.1', 'helpdesk', 'madhud', and '10.0.15.142'.
- Middle Panel:** An 'Apply Filters' section. It includes a 'Filter by Date' dropdown set to 'Quarterly' with a range of '2009-07 To 2009-09'. Below this is a section for 'Assets (GMT)' with a checkbox for 'show only Baseline assets.' and a legend: 'B = Baseline, L = Latest. Click one to view details. Click two to view Diff'. A table shows a single entry: 'L B 09/15/2009 05:03:28 0'.
- Right Panel:** A 'View Details' section for a 'CiscoPix Device: 10.10.254.3'. It shows 'License: Trial 28 days', 'Groups: Default Group.', and 'Collection Policy: SNMP Latest Asset: 09/17/2009 11:14:02'. Below this is a 'Returning Asset' section with a search bar and navigation buttons. A table shows a single entry: '09/15/2009 05:03:28 devIP=10.10.254.3'. Below the table is a 'START Scalar data Asset' section with a list of system parameters: 'Name | Value |', 'sysDescr | Cisco IOS Software C2600 Software (C2600-ADVENTERPRISEK9-M) Version 12.4(23) RELEASE SOFTWARE (...)', 'sysObjectID | .1.3.6.1.4.1.9.1.468 |', 'sysContact | |', 'sysName | qa2600a.eiqqa.com |', 'sysLocation | |', 'ifNumber | 4 |', 'ipForwarding | 1 |', 'ipDefaultTTL | 255 |', 'tcpRtoAlgorithm | 4 |', 'tcpRtoMin | 300 |', 'tcpRtoMax | 60000 |', 'tcpMaxConn | -1 |', 'sysServices | 78 |', and 'END Scalar Data Asset'.

The "Assets" tab within the Security Center provides access to information that allows users to track and analyze hardware, software and processes on all devices and servers. By looking at asset trends and providing the ability to create, monitor and enforce asset policies, SecureVue empowers users to make more intelligent decisions regarding asset upgrades and replacements.

Asset analytics gives users the ability to report and alert on assets being monitored by SecureVue. Alerts can be configured to notify administrators of occurrences such as network interface failures, new shares opened on key servers, new system drives, processes and software being loaded. By looking at asset detail trends for devices or hosts, users can make intelligent decisions regarding asset upgrades and replacements.

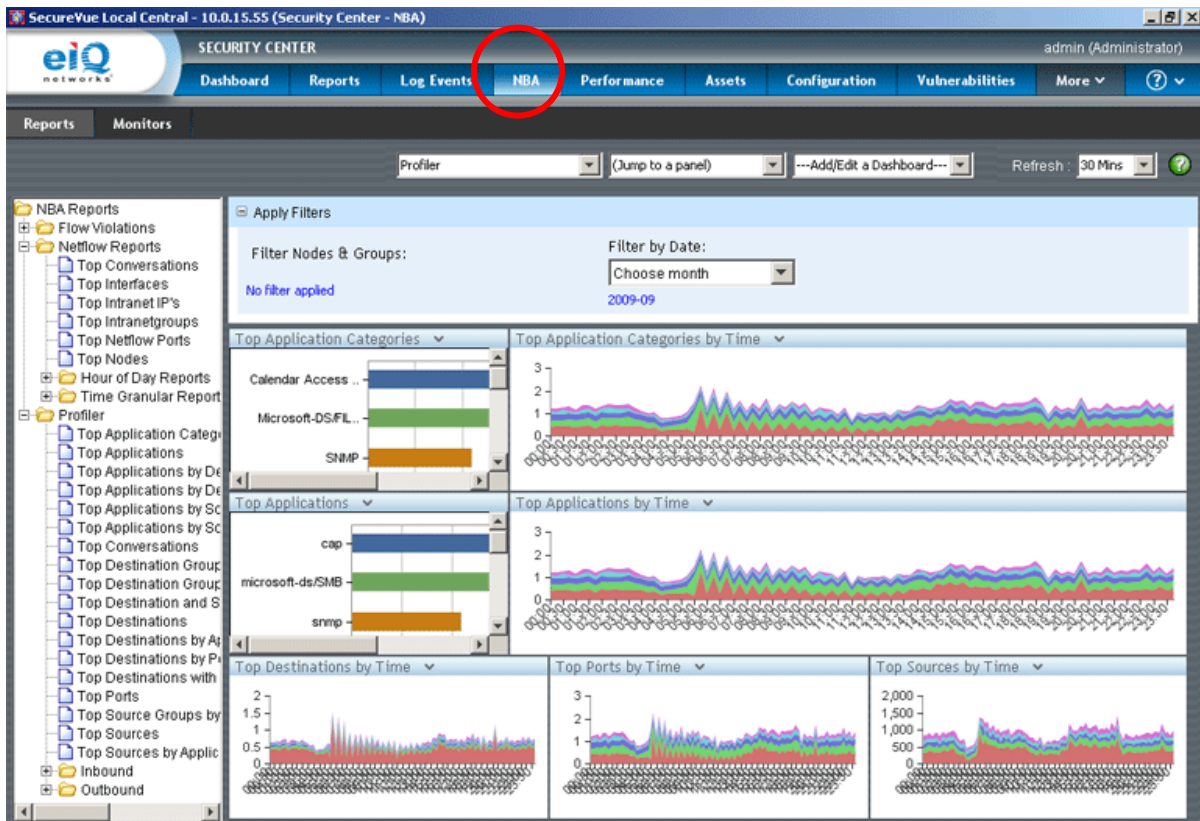
Performance Analytics



The "Performance" tab within the Security Center provides detailed performance information. Performance analytics is used to monitor and analyze the performance metrics of network devices and hosts. This provides valuable insight as to where an IT asset may be as part of its lifecycle as well as presents details around anomalous behavior.

Alerts can be configured to notify on items such as CPU spikes, memory and disk usage, network interface statistics, etc. Such notifications can indicate systems under heavy stress, which could possibly designate a security breach.

NBA Analytics and Flow Profiler



The “NBA” tab within the Security Center provides real-time visibility into how traffic impacts overall network health. It also allows users to profile nodes within the network. This information provides insight into the cause of network incidents as well as enables users to understand patterns in network performance, which enables the faster remediation of incidents.

NetFlow, C-Flow, S-Flow, J-Flow and Profiler data can be monitored and alerted on via this interface, enabling you to review network traffic, conversations, ports, protocols, bandwidth, top hosts and devices to ensure systems are operating optimally. In addition, reports can be run to show historical trending of flow and profiler data.

Availability

The screenshot shows the 'Availability' report in the SecureVue Local Central interface. The 'Availability' tab is highlighted with a red circle. The report displays a bar chart and a table of component availability distribution data.

Component Availability Distribution

This report provides information on component availability distribution.

Apply Filters and Adjust Content

Filter Nodes & Groups: No filter supported
Filter by Date: Choose month (2009-09)
Filter by Criteria: Global Filter (No Criteria Selected)
Aggregate Data by Default (Show trend data)

Graph

Y-axis: Count, BAR, Show legend

Distribution Range	Count	%Count
0.00-6.00	2	22.22%
6.00-12.00	1	11.11%
18.00-24.00	1	11.11%
42.00-48.00	2	22.22%
48.00-54.00	2	22.22%
54.00-60.00	1	11.11%

Total Record count : 6

“Availability” allows for the monitoring of availability of network and host resources. Users can define services and processes within the availability tab. Based on setup, you can constantly check the availability status and evaluate whether a node is reliable or not.

Quarantine

The screenshot shows the SecureVue Local Central interface. The top navigation bar includes 'Dashboard', 'Reports', 'Log Events', 'Vulnerabilities', 'ComplianceVue', 'Availability', and 'Quarantine' (highlighted with a red circle). The 'Quarantine' tab is active, displaying a table of log events. The table has columns for s.no, host-type, date & time, HostIP.Name..., facility, severity, event-id, category, username, and source. The events are filtered by 'FailedLogonActivity' and show a list of 21 entries, all with a severity of 'notice' or 'info' and a category of 'Unknown'. The interface also includes a search bar, a filter expression, and a navigation bar with 'Export Report' and 'Go' buttons.

s.no	host-type	date & time	HostIP.Name...	facility	severity	event-id	category	username	source
1	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
2	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
3	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
4	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
5	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
6	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
7	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
8	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
9	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
10	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
11	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
12	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
13	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
14	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
15	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
16	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
17	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
18	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
19	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd
20	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	info	86	Unknown	Unknown	sshd
21	Unix	09/17/2009 ...	(10.0.15.11...	authpriv	notice	85	Unknown	Unknown	sshd

Quarantine logs suspicious access into a resources based on policies. During the logging process, most devices make the decision to grant or deny event access into the network. If an event is deemed infected or suspicious it is quarantined or isolated to prevent network compromise. The quarantine feature also enables users to generate device, host and application-specific quarantine reports based on set policies.

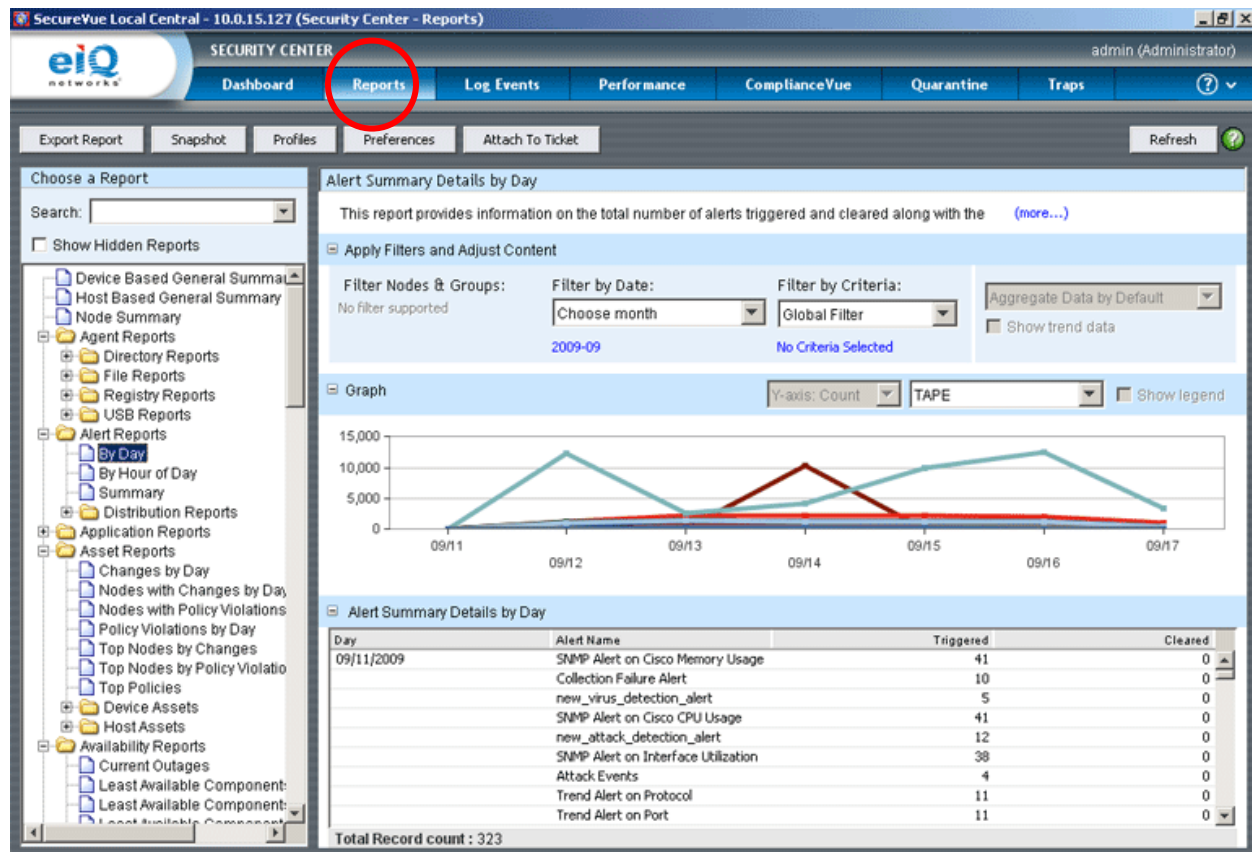
The ability to quarantine is especially important in high-traffic networks. Instead of starting a time-consuming forensics search after an incident is triggered, the quarantine feature automatically places events that meet certain criteria in a separate bucket to enable quick remediation.

Traps (SNMP)

The screenshot shows the SecureVue Local Central interface. The top navigation bar includes 'Dashboard', 'Reports', 'Log Events', 'Performance', 'ComplianceVue', and 'Traps' (highlighted with a red circle). The 'Traps' tab is active, displaying a table of recent SNMP trap events. The table has columns for Date & Time (GMT), Source UpTi..., Device/Host, Protocol, Source Port, Trap OID, and Tra. The main table below shows a list of traps with columns for SI N..., Source, OID, Type, Timestamp(0..., Trap Description, and Comment. The traps are all of type 'Authentic...' and have a timestamp of '09/17/2009 0...'. The bottom of the interface shows the copyright notice: 'Copyright © 2001-2009 eIQnetworks®, Inc. All rights reserved.' and the logo for 'eIQ SecureVue'.

The "Traps" tab within the Security Center allows users to remotely manage and monitor any MIB-enabled node in the network. For example, if a device interface is down or the number of packets coming through a router's interface increases users will be able to quickly identify the problem.

Comprehensive Reporting



The "Reports" tab within the Security Center provides access to over 1,500 out-of-the-box reports that enable users to gain visibility into infrastructure activity by accessing network, system, application and security details.

All reports can be accessed from the table of contents feature located below the calendar. In addition, while the initial data presented is near real time, the calendar feature provides the ability to go back and view historical data by entering a custom date range.

Users have the option to apply filters to any query to easily find specific information. To access more detailed log information as well as filtered real-time monitoring, all of the data presented can easily be drilled into by right clicking.

For instance, you can view top attackers and then drill into forensics data to discover how long the attacker has been trying to break in and by what means. You can also easily pinpoint users attempting to access prohibited systems.

Users can start with summary reports, and use drill down to launch forensics search, or monitor a certain activity, etc.

Forensics Analysis

The screenshot displays the 'Forensic Analysis' interface. On the left is a 'Forensic TOC' menu with options like 'Overall Events Triggered by Severity', 'Top Application Events', 'Top DNS Server Events', 'Top Security Events', 'Top Sources', 'Top Successful Logons', 'Top Successful Logons by Source', 'Top System Events', and 'Top Users'. The main area shows a table of events with columns: SNo, Date & Time, Source IP, Severity, Host-IP, Host Type, Event-ID, Facility, and Event Descrip... The table contains 12 rows of data, with the first four rows highlighted in orange. Below the table is a 'Display Type' dropdown set to 'Table' and an 'Export Report' button. A summary table shows the count of hits for each severity level: notice (3), success (125476), error (13749), and warning (7,753). The total record count is 4.

SNo	Date & Time	Source IP	Severity	Host-IP	Host Type	Event-ID	Facility	Event Descrip...
1	10/29/2008 1...	-	warning	10.0.15.72	Windows	14	system	The time pro...
2	10/29/2008 1...	-	error	10.0.15.72	Windows	29	system	The time pro...
3	10/29/2008 1...	-	error	10.0.15.72	Windows	7	system	The kerberos...
4	10/29/2008 1...	-	error	10.0.15.72	Windows	7	system	The kerberos...
5	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
6	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
7	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
8	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
9	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
10	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
11	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...
12	10/29/2008 1...	-	warning	10.0.15.72	Windows	3019	system	The redirecto...

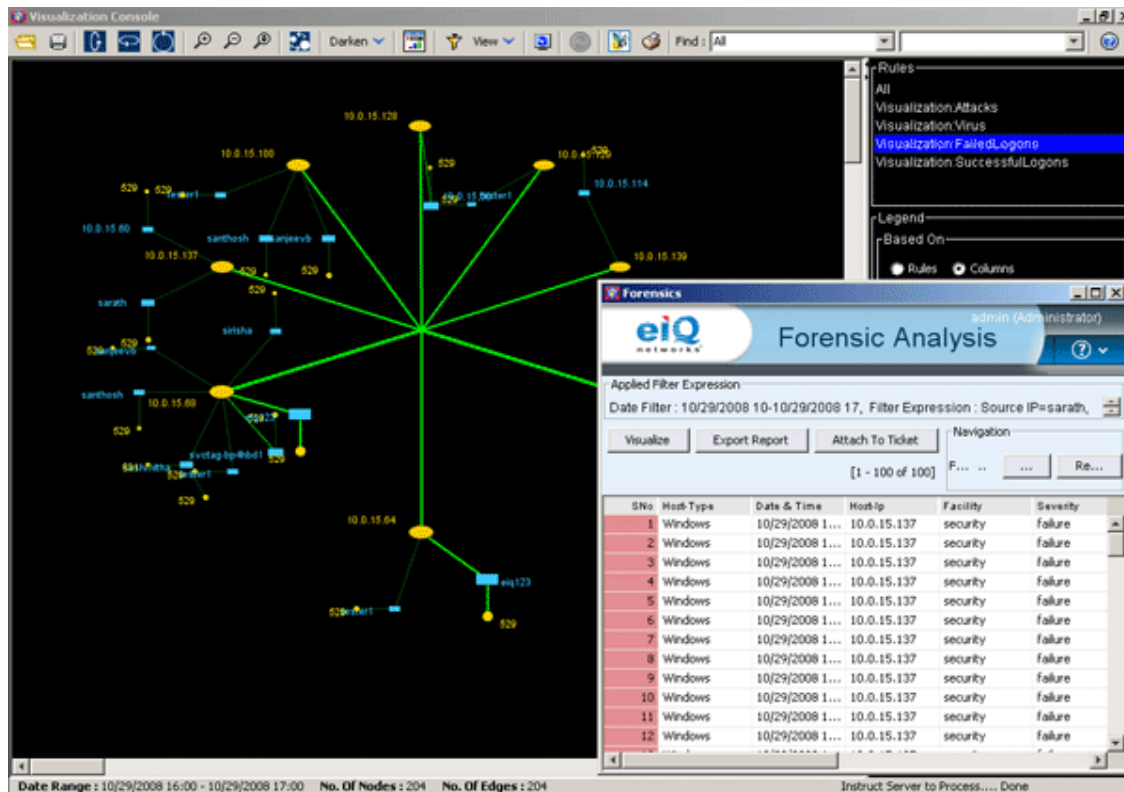
Severity	Hits
notice	3
success	125476
error	13749
warning	7,753

Forensics enables users to easily search volumes of archived log, vulnerability, configuration, asset, performance and NBA data. This provides the ability for users to investigate specific events that have occurred on the network to vector security breaches, speed remediation and ensure regulatory requirements are being met.

Forensic investigation allows you to more easily detect anomalies, identify policy violations and display suspicious behavior in chronological order. For instance, you could track all activity from a particular user over a period of time. Once the search data is returned you can further drill in to narrow down suspicious activity. The output of this report can then be exported.

Forensics can also be viewed in 3-D visualization. The next section provides more information.

3-D Visualization

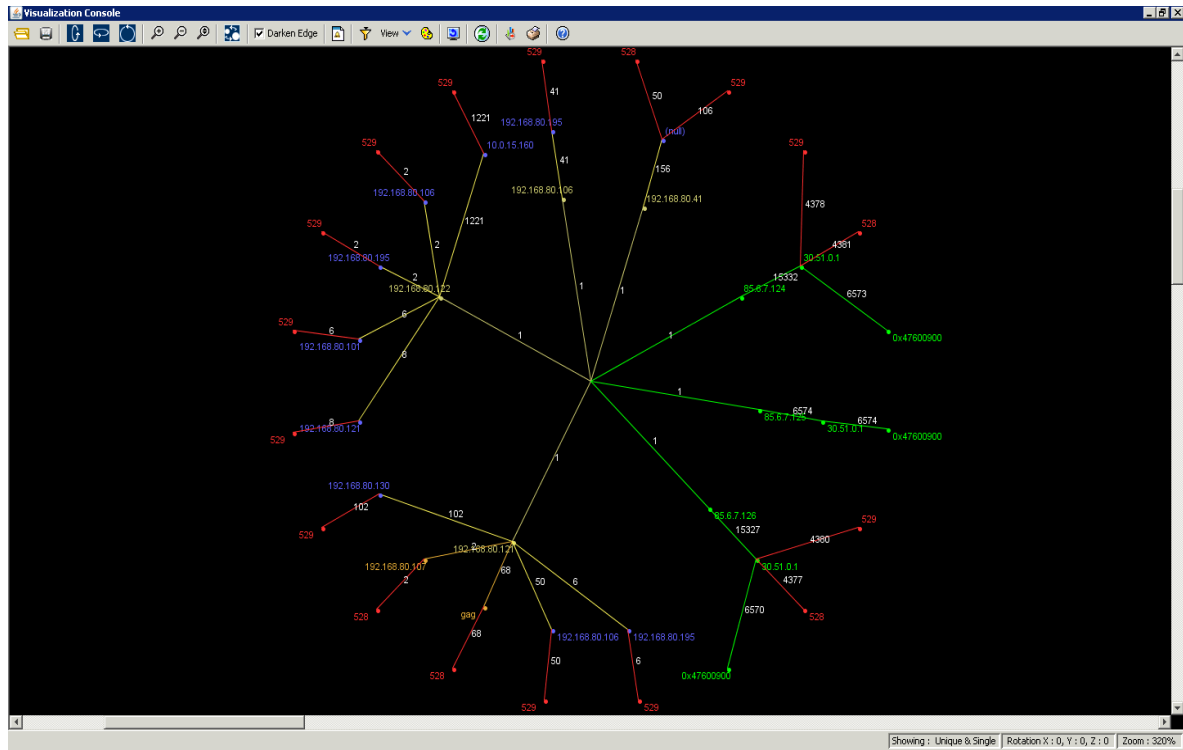


Supporting millions of nodes, visualization allows users to view log data, security incidents, access control lists effectiveness, profiler data, node specific traffic patterns and forensics detail in an easy-to-understand graphical view. 3-D visualization can be accessed by drilling down from any report and forensic windows. The visual representation of data allows users to more effectively analyze how networks are connected.

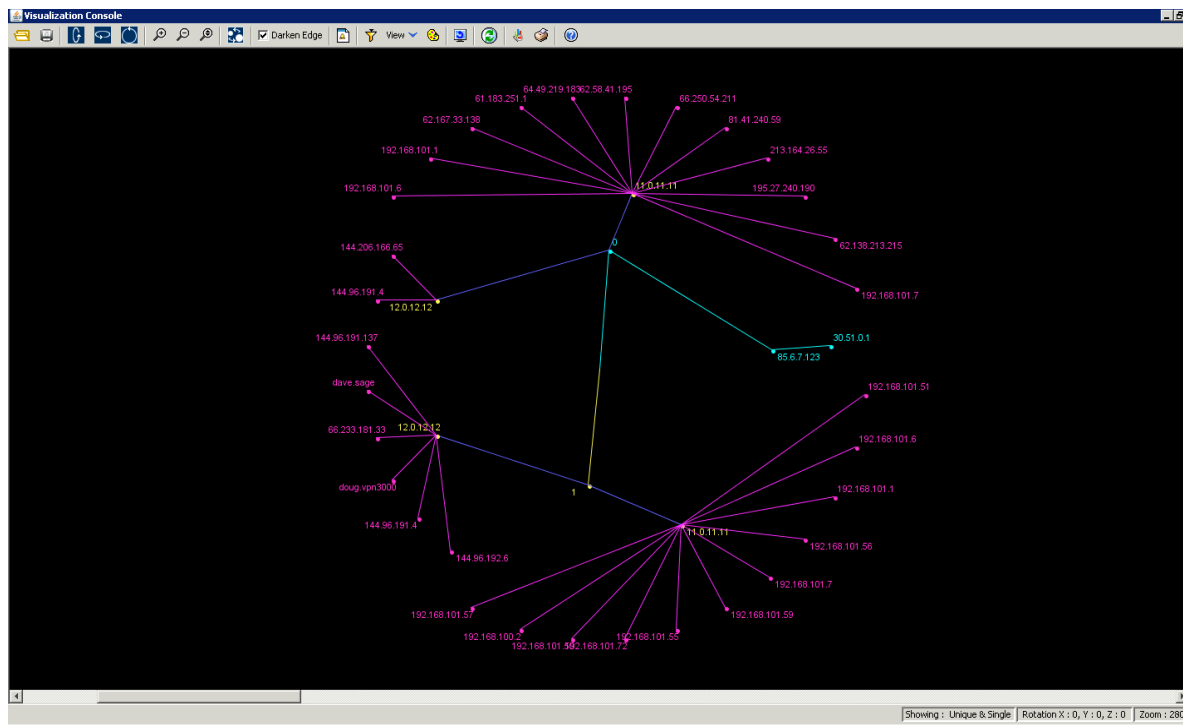
Through visualization, users can customize the information being displayed to meet specific needs. For example, you can access a simple, high-level overview to support monitoring or display a more complex view that illustrates all data from heterogeneous sources, thus supporting analysis and diagnosis.

Visualization Scenarios

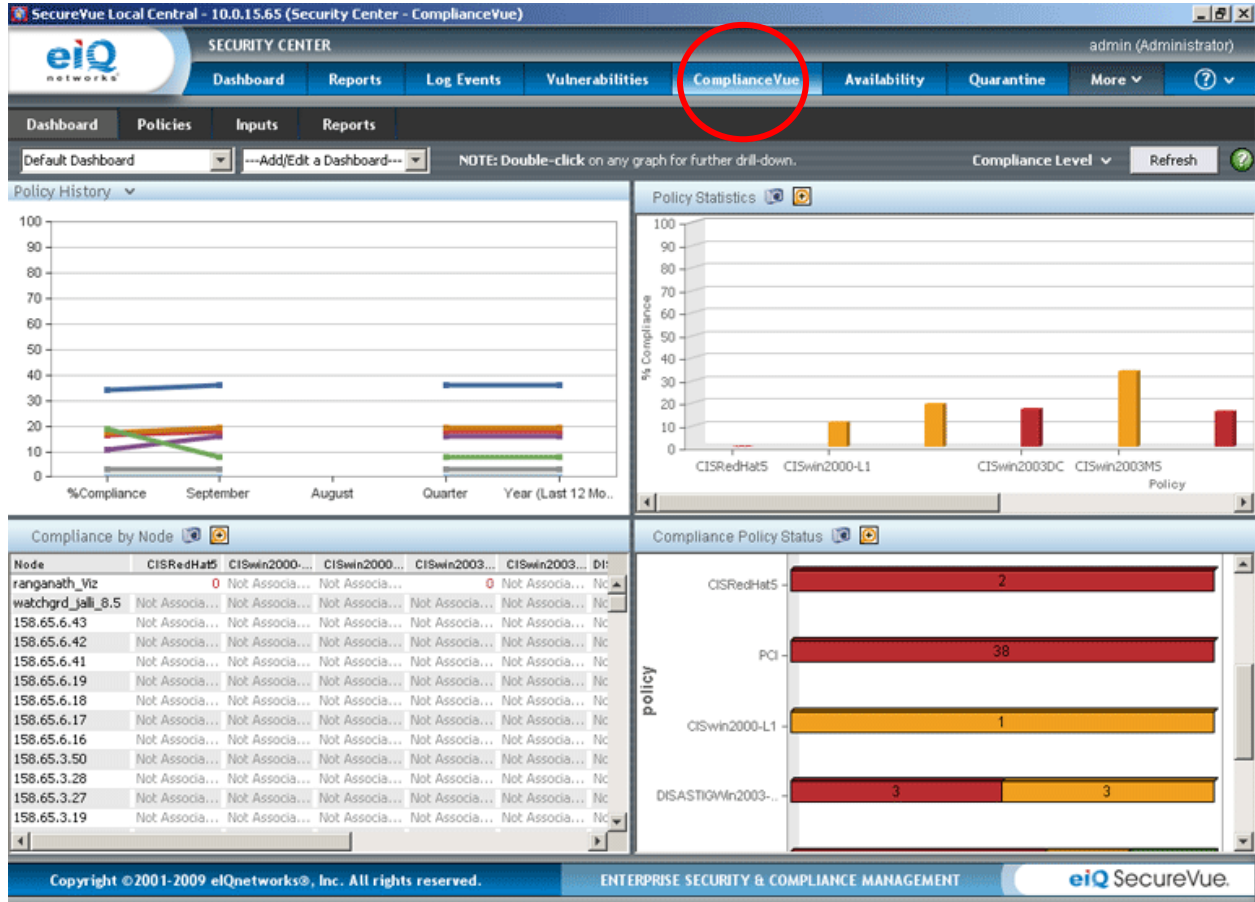
Host and Device Correlation



Perimeter Block Sources



ComplianceVue



ComplianceVue, offered in Security Center, provides a common framework and an integrated approach to manage all compliance requirements faced by an organization. It helps protect your network from the most severe threats to critical IT systems and operational processes by showing you which nodes are not in compliance with legal regulations or enterprise standards that include:

- The Health Insurance Portability and Accountability Act (HIPAA) regulations have widespread impact on healthcare providers and insurance companies to ensure the integrity of customer data.
- The Gramm-Leach-Bliley Act (GLBA) requires significant reporting on the processes to ensure the integrity of customer data for financial institutions including banks, mortgage brokers, lenders, credit unions, insurance and real-estate companies.
- The Federal Information Security Management Act (FISMA) outlines requirements that federal agencies must develop, document and implement to ensure information security.
- The Payment Card Industry Data Security Standard (PCI-DSS) includes requirements to ensure consistent data security measures across all member banking institutions, merchants and service providers
- Sarbanes-Oxley (SOX) documents specific regulations required for publicly traded companies to document internal controls over security processes.

- CoBIT (Control Objectives for Information and related Technology) is a set of best practices for IT professionals that provide generally accepted measures, indicators and processes to assist in the development of appropriate IT governance and controls.

Built on a fully extensible architecture, the ComplianceVue allows users to establish internal policies, tailor business requirements and add additional regulations and best practices. Wizard-based mapping automates policy and audit management to accelerate the creation, approval and maintenance of evolving internal and external requirements. This module helps answer questions like:

- ***How compliant is an organization by regulation, best practice and policy?***
- ***What are the historical compliancy trends?***
- ***Where is an organization failing? Which nodes are in violation and why?***
- ***How can full compliance be achieved?***
- ***What are the specific IT control implementation guidelines by technology, regulation and framework?***

7. Troubleshooting

I installed and am running SecureVue, however I'm not seeing devices in the device list.

Automatic discovery of devices requires that the device is configured to stream logs to the SecureVue server and data collector. To understand configuration for streaming logs for a device, please refer to vendor-specific device documentation. Some more common errors for proper configuration are:

- The device has not been configured properly to stream logs to the SecureVue server
- The port that logs are being streamed differs from the port the data collector is listening on
- A firewall is not allowing the stream to get to the SecureVue server (streamed port is blocked)
- Another application is listening on the same port as syslog (UDP 514) so SecureVue cannot collect the files

I have added devices and I am seeing real time information, but there is no data within the reports.

When devices are added SecureVue collects all of the log information that is stored on that system and begins to process that information starting with the oldest log entry. SecureVue will need time to catch up in its processing of data before the data can be viewed within reports. This process usually takes less than 24 hours.

I manually added a device, but I am not receiving data in SecureVue.

Files that have been manually added cannot include data that is streamed via the data collector.

I was collecting data from a device, but it has recently stopped.

This is most likely because something has interrupted the success of streaming logs to the SecureVue server. See question #1 for more help.

I've installed IIS 6.0 and things aren't working.

See the *SecureVue Deployment Guide* for instructions on configuring SecureVue with IIS 6.0.

I've installed and am running SecureVue, however none of the reports have populated.

Reports typically take at least an hour to populate and become more meaningful as the database populates. If you are seeing monitoring data, yet are not seeing report data after an hour passes then contact eIQnetworks customer support. For immediate feedback view the Monitoring Portal.

I've installed and am running SecureVue, however some reports say "No Data".

This is most likely because the logs for a particular device do not contain the information necessary for a specific report. For example, one device might support an anti-virus report and one device may not. In addition, the level of logging (i.e., severity) may not contain certain information required for a specific report.

8. About eIQnetworks

eIQnetworks, Inc., a global provider of integrated security, risk and audit management solutions, enables enterprise, government and MSSP customers to simplify IT assurance by improving collaboration between network, security and compliance teams. More than 2,500 organizations worldwide rely on the power of eIQ's next-generation security information management (SIM) and governance, risk and compliance (GRC) technology to proactively detect security breaches, speed incident remediation and support evolving best practices and compliance regulations across the enterprise. eIQ customers include Atos Origin, Avaya, BT, Casio, Celgene, Fujitsu, Hess, Malaysia Telecom, The New York Times, Nuspire, Rackspace, Singapore Telecom, The South Financial Group and Sprint. eIQ solutions are sold both direct and through a global network of distributors, resellers and strategic OEM partners, which include Astaro, CITTIO, Clavister, H3C (3COM), iPolicy Networks, Mirapoint, NEC, PioLink, Reflex Security, Secure Computing and Top Layer Networks. For additional information, please visit www.eIQnetworks.com or call +1 877.564.7787.

© 2010, eIQnetworks, Inc. eIQnetworks and the eIQnetworks logo are registered trademarks and SecureVue is a trademark of eIQnetworks, Inc. All rights reserved.