



How SecureVue from eIQnetworks Provides Situational Awareness to an International Retail and Investment Bank

Case Study

SecureVue from eIQnetworks delivers security visibility, fosters collaboration, and provides a low TCO to this international retail and investment bank.

“SecureVue allowed us to consolidate and replace several other technologies, saving us significant money over the long run.”

- Bank CISO

Challenge

As a \$50 billion financial services powerhouse with 160,000 employees operating in over 70 countries around the globe, an international retail and investment bank was initially seeking a solution to comply with a broad range of regulations mandating centralized logging and continuous security and configuration monitoring, including PCI DSS, the Gramm-Leach-Bliley Act (GLBA), the Federal Financial Institutions Examination Council (FFIEC) IS Handbook, Sarbanes-Oxley (SOX) and others. Additionally, the bank had recently initiated an internal policy requiring that all logs – regardless of whether they were generated from an operating system, application, database or network device – be stored in a central enterprise repository.

Solution

After a rigorous evaluation process that involved reviewing multiple point security products including SIEM and configuration auditing, the bank selected SecureVue from eIQnetworks as a unified situational awareness platform to meet the complex requirements of its global projects. The bank was also able to leverage SecureVue's unified situational awareness capabilities to deliver security and IT operations value far beyond the original scope of the project.

Benefits

- **Lower Total Cost of Ownership (TCO).** One of the immediate results of using SecureVue was the ability to replace multiple redundant technologies across the enterprise. The bank was previously using Symantec's Enterprise Security Manager (ESM) to conduct prescriptive configuration audits on servers. Using SecureVue, they were able to completely replicate Symantec ESM's capability while extending configuration audits beyond servers to network infrastructure and security devices. The bank's CISO identified these cost-reduction benefits as critical, stating, "SecureVue allowed us to consolidate and replace several other technologies, saving us significant money over the long run."
- **Collaboration Between IT and Security Operations.** Like any large enterprise, the bank maintains a dedicated security operations center (SOC) manned by dedicated security professionals responsible for ensuring the security of IT assets across the organization. One of the key methods in which the SOC works with IT teams is the concept of "fire accounts," one-time-use accounts that provide non-security IT personnel with temporary privileged access to systems. Before the SecureVue implementation, the bank was generating a large number of fire accounts to meet the requests of IT developers, DBAs, administrators and other technology personnel. However, once SecureVue was in place, the SOC team noticed that the vast majority of fire accounts were being used solely for view-only functions, such as monitoring processes, events and users. Rarely were fire accounts being used to install components or modify systems.

Leveraging the fact that eIQnetworks does not charge for SecureVue users, the bank established a series of customized SecureVue dashboards and reports and provided IT operations personnel with direct access to these components through the SecureVue console. Coupled with SecureVue's granular role-based access control, the SOC team was able to drastically reduce the use of fire accounts – and the corresponding risk of using them – while providing IT operations teams with the security information they needed to meet their goals.

“We’re now expanding into SecureVue capabilities including compliance reporting and automation.”

- Bank CISO

- **The Value of True, Unified Situational Awareness.** As a true unified situational awareness platform, SecureVue provides unparalleled visibility into security and compliance data by allowing the correlation of all security elements – including events, users, assets and configurations, network behavior, performance metrics, file integrity and others – to see the often complex inter-relationships between these pieces of data.

For example, the bank experienced the power of unified situational awareness first-hand when they noticed that a new security administrator was remotely logging onto several critical UNIX servers as “root,” something that should have been disallowed based on the company’s server configuration standards and policies. The log-based evidence collected by SecureVue showed that the administrator was logging onto these systems remotely using the highly-privileged “root” identity on a regular basis. This meant one of two things: either the admin was changing the security policy on these systems, logging in, and then changing the configuration back after logging out, or there was a major configuration issue on the servers. Using SecureVue’s ability to agentlessly collect and correlate native, real-time asset and configuration data, in addition to logs – the SOC team identified that there were multiple versions of the “ssh” remote shell utility running on their UNIX servers. One was the standard GNU “ssh” installed as part of the operating system, and the other was the “OpenSSH” package, installed as part of another product on the servers. While the native “ssh” was disabled, “OpenSSH” was running and configured to allow remote logons – including “root.” Using this information, the bank quickly generated a report identifying all UNIX servers with multiple versions of remote shell running and immediately disabled instances of “OpenSSH,” rapidly closing the hole by correlating event-based information with asset and configuration security data. By analyzing log, asset and configuration data in the same unified platform with a single console, the bank was able to quickly identify a critical security vulnerability that would have been extremely difficult to detect using individual point products such as SIEM and dedicated configuration auditing tools. Without SecureVue, the bank would have been forced to use two different point products, two different consoles and potentially two different security operations personnel working collaboratively to investigate the above scenario. With SecureVue, the bank was able to get to the root cause quickly and efficiently with low TCO.

With SecureVue, the bank was also able to address a significant potential threat by correlating event-based data with network traffic patterns via netflow analysis. By bringing together remote access logs and netflow data such as IP addresses, hostnames and user names, the bank established a daily report of all “suspicious” remote access activity, including users who were logging on to remote access services across the enterprise from unusual or unexpected systems or abnormal times of day

Summary

While log centralization and consolidation was a key initial purchase driver, the bank also acquired the ability to solve both new and previously unknown problems – including the integration of configuration information and netflow data to discover “signatureless” vulnerabilities as well as greatly reduce the risk of using highly privileged accounts.

Today, this international bank continues to discover new ways to leverage SecureVue’s unified situational awareness capability to further enhance information security operations. “Not only do we continue to use SecureVue to consolidate existing toolsets,” said the bank’s CISO, “but we’re now expanding into SecureVue capabilities including compliance reporting and automation.”

By leveraging the SecureVue unified situational awareness platform, the bank was able to rapidly gain visibility across the enterprise by consolidating onto SecureVue’s single, flexible console. Because SecureVue requires no DBA, has low hardware overhead and minimal administrative requirements, they were able to achieve new security operations capabilities with a low total cost of ownership.

elQnetworks’ SecureVue benefits the bank and other customers with:

- Enterprise Wide True Situational Awareness
- Operational Efficiency
- Low Total Cost of Ownership

Want to know how SecureVue from elQnetworks can help you? Contact us at +1 877.564.7787 or email sales@elQnetworks.com to learn more.



elQnetworks

31 Nagog Park

Acton, MA 01720

t. +1 978.266.9933

f. +1 978.266.0004

www.elQnetworks.com