CASE STUDY

Protecting Customer Banking While Ensuring **Regulatory Compliance**

LEADING FINANCIAL SERVICES FIRM LEVERAGES NETWORK MODELING AND AUTOMATION TO STAY AHEAD OF CYBERTHREATS

CUSTOMER PROFILE

Our customer is a United Kingdom-based financial services firm subject to rigorous objectives around customer protection and regulatory compliance. Founded in 2002 and serving 9 million customers, the organization is part of a larger cooperative that provides banking, mortgages, credit cards, loans, pensions, trusts and insurance services.

CHALLENGES

- ✓ Managing 200+ firewall estate
- ✓ Maintaining compliance with government and financial industry regulations, including PCI
- ✓ Protecting customer financial data while ensuring its constant availability

RESULTS

- ✓ Identified and remediated key areas of concern to prevent data breach
- ✓ Created a complete network model using configuration data from firewalls and routers
- ✓ Reduced risk to satisfactory levels
- ✓ Automated security tasks including connectivity and compliance status

THE PROBLEM

The organization went through a period of rapid growth fueled by multiple mergers, which created a large, complex multi-vendor network. With hundreds of firewalls and tens of thousands of rules, the IT security team was struggling to support a growing user base and more complex network.

To protect the continuous availability of customer data, the team needed to ensure that firewalls were secure and compliant with both internal policies and industry regulations, including PCI DSS.

The team was relying on resource-intensive, manual assessments to monitor network security status. Identifying security gaps and potential compliance issues was laborious and often based on subjective viewpoints among teams of engineers.

They needed not only more effective management and control of the distributed network but also automated security processes to free up IT administration time and allow staff to focus on other important strategic issues.

SCOPE AND SELECTION CRITERIA

The chief security officer (CSO) was looking for a strong layer of security analysis and process automation that would provide the most rigorous security protocols possible. To address these network security concerns, the company evaluated a number of vendors that offered rule-based management.

However, these improvements would only solve only a small part of the problem. The CSO also wanted a solution that provided total network visibility and quick identification of security gaps.

The organization purchased the Skybox® Security Suite, activating the Skybox® Network Assurance, Skybox® Firewall Assurance and Skybox® Vulnerability Control modules to pinpoint risk and exposures, create network models, identify connectivity issues, fix conflicting firewall rules and demonstrate continuous compliance.

> "The ability to visualize actual threats and create a simulated attack scenario quickly identifies any asset that is susceptible to a potential security breach. It's the only solution that could handle all of the security requirements of our growing organization."
>
> *CSO, UK Financial Services Firm*

DEPLOYMENT

Given the complexities created by multiple mergers, gaining visibility was the first order of business. Skybox solutions created a comprehensive network model using configuration data from firewalls and routers, providing the foundation to identify key areas of concern and put remediation plans into action.

Not long after implementation, the customer was to visualize its complex network, identify and mitigate asset threats and reduce risk levels across the board.

Automation for Daily Security Status

Prior to deploying Skybox, penetration testing was used regularly; however, with a limited scope, these tests couldn't provide a full view of potential firewall rule errors or mistakes. Post deployment, firewall managers were able to pinpoint problematic rules and fix them before a breach could occur.

Vulnerability and compliance analysis is now run daily and automatically, providing clear reports on the network's current connectivity and compliance status.

"With Skybox, the automation that has replaced manual processes will introduce efficiency gains that we could have never achieved on our own," said the company's CSO. "The ability to test future changes in a virtual environment prior to deployment will save time that was previously dedicated to problem-solving discussions within change control teams."

Security that Scales

Yet another merger that introduced 3,000 employees, an unknown network and scores of new devices presented a fresh challenge for the recent Skybox deployment. “The solution has already proven to be more than capable of automating the analysis of large amounts of data that would be unfathomable if we tried to digest them manually. We are very happy to have this working, living model of our network,” said the CSO. “The ability to visualize actual threats and create a simulated attack scenario quickly identifies any asset that is susceptible to a potential security breach. It’s the only solution that could handle all of the security requirements of our growing organization.”

ABOUT THE SOLUTION

By combining Firewall Assurance, Network Assurance and Vulnerability Control, security was able to keep pace with a complex and evolving business. Using Skybox, the organization successfully navigated multiple mergers to create an efficient and fully integrated network security management program while maintaining continuous compliance and availability.

Designed as a context-aware vulnerability management solution, Vulnerability Control goes beyond traditional assessments and consolidates vulnerability sources without a scan to detect vulnerabilities and fill in blind spots other tools may miss. Vulnerability Control also applies attack simulation, superior vulnerability intelligence and powerful analytics to help customers eliminate critical attack vectors fast.

Firewall Assurance completely automates firewall management tasks across different firewall vendors and complex rule sets. It continuously verifies that firewalls are clean, optimized and working effectively. Extending beyond firewall rule checks, it analyzes possible traffic between network zones to find hidden risk factors, flagging unauthorized changes and finding vulnerabilities on firewalls.

Network Assurance provides total network visibility by taking in the context of existing network devices and security controls. It shows how these controls work together or leave you exposed; highlights potential attack vectors; verifies implementation of security zone policies; and troubleshoots root causes of network outages.

RESULTS

With Skybox solutions, the financial services company successfully automated security tasks, comprehensively modeled the network and was able to systematically reduce risk by identifying and remediating critical security concerns. The customer was able to implement the most rigorous protocols available to ensure security and continuous compliance and availability.

About Skybox Security

REQUEST A DEMO!

We arm security leaders with a powerful set of integrated security solutions that give unprecedented visibility of the attack surface and key Indicators of Exposure (IOEs) such as exploitable attack vectors, hot spots of vulnerabilities, network security misconfigurations and non-compliant firewalls. We help security professionals break down silos of information through integration with dozens of security solutions that enterprises are already using. By extracting actionable intelligence from data using modeling and simulation, Skybox gives security leaders the insight they need to quickly make decisions about how to best address threat exposures that put their organization at risk, increasing operational efficiency by as much as 90 percent. Our award-winning solutions are used by the world's most security-conscious enterprises, government agencies and organizations for vulnerability management, threat intelligence management and security policy management. Many of our customers are on Forbes' Global 2000 List, including six of the top 10 global banks and six of the 10 largest NATO member countries.