CASE STUDY

Risk Assessment in 5-10 Minutes Instead of Days

COUNTY COUNCIL GAINS TOTAL NETWORK VISIBILITY, AUTOMATES PROCESSES TO SAVE 30 DAYS OF WORK PER YEAR

CUSTOMER PROFILE

Our customer is a county council is an upper-tier local authority for a non-metropolitan county in the United Kingdom and a member of the East of England Local Government Association. The council employs more than 5,000 people at two main offices and 50 satellite offices. Their complex IT infrastructure contains more than 50 firewalls, 8,000 users, siz networks and 5,000 endpoints. The organization also had more than 10 DMZs exchanging data with partners and more than 130 public-facing IPs. Additionally, the council is subject to internal security policies and other regulatory standards.

CHALLENGES

- ✓ Time-consuming manual firewall management processes
- ✓ Decentralized change management
- ✓ Lack of network and endpoint visibility
- ✓ Inability to assess change impact prior to implementation
- ✓ Maintaining continuous compliance

RESULTS

- ✓ Narrowed risk assessment window from days to minutes
- ✓ Reduced manual change management processes by more than 60%
- ✓ Achieved total network visibility across all endpoints
- ✓ Implemented change modeling to avoid introducing new risk
- ✓ Ensured continuous compliance with internal and regulatory requirements

THE PROBLEM

The council had about 30 outsourced service providers managing different parts of the infrastructure. Each change made impacted multiple organizations, and no single person was responsible for the end-to-end process. To reduce risk, the organization needed auditing and oversight of the firewall change process, a definitive view of all firewall data and verification that changes were implemented as intended.

"With so many contracted agencies, we need to connect to all of their infrastructures, sharing systems and data," said the council's technical security director. "As a manager, I worry about these things, and I wasn't happy with the view I had of my firewall network. I didn't have insight into firewall rulesets. I would breathe a sigh of relief every year when we received our penetration testing results, but I'd like not to worry throughout the other 11 months of the year." With numerous zones, firewalls and other interactions, the council lacked total network and endpoint visibility and intelligence.

The security team needed an automated process to effectively respond to approximately 40 firewall change requests per week in a secure and timely manner. Every firewall request was requiring a labor-intensive, manual process, handcrafting each access control list and filtering the firewall to determine the downstream and upstream impact. About a handful of those change controls evolved into a major rule change every month.

"We wanted a better understanding of the impact of our firewall rulesets over time," said the technical security director. "We knew why we implemented those rules two years ago, but did we still need those rules?"

Similarly, they needed to model how proposed changes would impact the broader network prior to implementation to avoid introducing new risk. "Previously, we didn't have an automated way to understand the downstream impact of a firewall change request," said the technical security director. "We spent a huge amount of time investigating a single change request because we didn't want to open up too much access."

> "Manually, risk assessment would take us days, or even a week. With Skybox, the same assessment takes 5-10 minutes, sometimes instantly."
>
> *Head of Technology, UK County Council*

Maintaining continuous compliance was also an issue. The council has a third-party vendor that processes credit card payments, so the organization is not directly subject to PCI DDS compliance. However, as a matter of good security practice, they wanted to meet industry standards around PCI and ISO 27001. "As a local authority, we adhere to PSN (Public Service Network) requirements," said the head of technology at the council. "For accreditation, I needed evidence that were compliant and validation that were doing what we said we were doing."

SCOPE AND SELECTION CRITERIA

The council was looking for a solution to automate time-consuming routine tasks that were draining valuable resources. And, with such a large, complex, and fragmented network, the organization needed to centralize firewall management and implement a fully automated end-to-end process. Subject to both internal security policies and regulatory requirements, the customer needed continuous compliance monitoring and reporting to ensure that there were no surprises during the yearly audit.

DEPLOYMENT

The council selected Skybox® Firewall Assurance and Skybox® Vulnerability Control to automate risk management on their network. After one day of training, the team was up and running on Firewall Assurance, using network configuration files to create a model of the network, showing the firewalls, rulesets, endpoints, threats and more. For the first time, they have complete visibility into their network and endpoints.

Reinventing Change Management

Assessing the risk impact of a proposed change is the most difficult aspect of firewall change management. The firewall team quickly embraced the modeling approach of Skybox solutions. With Firewall Assurance, they are able to see risk before a change is made, validate implemented changes and, if more insight is needed, they use the Skybox model to simulate scenarios prior to implementation.

"With 50+ firewalls, can you imagine how many zones there are? And if you make a change on one part of the firewall higher up the hierarchy, what's the impact on the bottom of the hierarchy?" These are the questions that the technical security director struggled to address daily.

Before deploying Skybox, the director would review network map drawings, taking at least a week to estimate downstream impact. With Skybox, they simulate the change on the network model to assess risk instantly.

"Skybox takes a copy of the live firewall rules and can actually show me the scenario and the impact it's going to have five firewalls down," said the director. "What's even better is that after the change has been implemented, I can take a fresh copy of the rules and run it through again and see that the change was implemented as we intended. That's the beauty of it."

Skybox automation reduced manual effort by more than 60 percent. Manually, risk assessment would take about three days due to the number of drawings to be reviewed. With Skybox, the organization is able to assess risk within five to 10 minutes – sometimes, instantly.

"Over the course of a year," said the director, "I estimate that Skybox automation will result in at least 30 days of work saved."

Compliance

Using Firewall Assurance's standard templates, the customer confirmed they had no security gaps; but they did discover a need for increased precision in their rules. Specifically, most firewalls were no public-facing but, rather, used to control communication between network zones. Skybox was able to highlight trusted zones that were trusting semi-trusted zones. This lead the customer to implement a more granular approach to firewall rules.

Reducing Risk

The council also purchased Skybox Vulnerability Control for vulnerability management and risk reduction. They used a Nessus vulnerability scanner and third-party penetration testing every quarter. But penetration tests were disruptive, expensive and time-consuming and did not help them identify and focus on real risk.

"Skybox allows me to model threat and attack vectors. If we make a change and need to assess risk impact, we don't have to commission an expensive penetration test," said the director. "I've got a third party looking after my external points; but our internal infrastructure is quite large, so we use a Nessus scanner that runs vulnerability scans against the internal box. Then we use Skybox Vulnerability Control to analyze and prioritize that data, and Vulnerability Control tells me where I need to hone in my internal penetration testing." This way, penetration testing is used sparingly on critical areas that are vulnerable, saving time and money.

Security-Minded, Risk-Focused

With Skybox security analytics automating the process, the security team no longer thinks about the actual firewall rules and ACLs, instead focusing on the outcome. The role has shifted to more policing and ensuring that the intent of a change request matches implementation.

"Skybox security analytics have changed our processes and the way we think," said the Head of Technology. "We think about security from the ground up, and it's really helped us focus our risk assessment methodology. We're thinking in security questions now like, 'What is the total impact of this change?' It's opening a lot of new doors."

ABOUT THE SOLUTION

Skybox Firewall Assurance completely automates firewall management tasks across different firewall vendors and complex rule sets. It readies your network for action by continuously verifying that firewalls are clean, optimized and working effectively. Firewall Assurance extends beyond firewall rule checks, analyzing possible traffic between network zones to find hidden risk factors, flagging unauthorized changes and finding vulnerabilities on firewalls.

Skybox Vulnerability Control is a context-aware vulnerability management solution that goes beyond traditional vulnerability assessment. Vulnerability Control consolidates vulnerability sources and uses scanless vulnerability detection to fill in blind spots other tools may miss. It then applies attack simulation, superior vulnerability intelligence and powerful analytics to quickly prioritize and eliminate attack vectors.

RESULTS

Using the Skybox Firewall Assurance and Skybox Vulnerability Control, the council not only automated time-consuming, resource intensive firewall management but also narrowed the risk assessment window from days to minutes. The 60 percent reduction in manual processes freed up IT security staff to focus on other important initiatives. The council was finally able to get a handle on network security and compliance even as the network changed, and have confidence that the right solutions were in place to support growth and evolving needs.

About Skybox Security

Skybox arms security teams with a powerful set of security management solutions that extract insight from security data silos to give unprecedented visibility of the attack surface, including all Indicators of Exposure (IOEs). With Skybox, security leaders can quickly and accurately prioritize and address vulnerabilities and threat exposures.

REQUEST A DEMO!

SKYBOX™ SECURITY

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060