Improving the SOC Through Visibility and Automation

CENTRALIZED SECURITY MANAGEMENT AND UNIFIED VISIBILITY GIVES DISPERSED SECURITY TEAMS COMMON GROUND

THE PROBLEM

The company was experiencing rapid growth which led to a network environment in constant flux — and security struggling to keep up. The network was also dispersed across several regional offices with various teams and processes, presenting a huge challenge to getting comprehensive visibility and intelligence that took in the complete context of the organization. Each team was relatively small and struggling with day–to–day management, let alone strategic security goals.

CHALLENGES

- ✓ Business scaling faster than security
- ✓ Decentralized network making it difficult to gain visibility and accurate intelligence
- ✓ Small security team with big responsibilities
- ✓ Maturing the security program beyond baseline standards

RESULTS

- ✓ Efficient, automated processes
- ✓ Data and teams brought out of their silos
- ✓ Strong foundation of comprehensive visibility and network modeling
- ✓ Complete context to inform daily action and long–term strategy

SCOPE AND CRITERIA

First and foremost, the company needed to gain visibility across the network. They were looking for a network mapping solution that could provide a foundation of accurate information from anywhere in the network. They sought integration with their Qualys solutions as well as integration with their own product offerings used internally.

As part of the maturity goals, the company also planned to improve vulnerability analysis capabilities down the road, with the ability to see their critical vulnerabilities at a glance. It was important that they find a solution that would help create a security ecosystem within their environment, a centralized platform with common information that any security personnel could access and utilize across the organization.

The company evaluated Skybox™ Security and one other company, but it quickly became clear who was the winner. "During the PoC, Skybox overcame an issue that I thought was a show-stopper within 48 hours. The other vendor never really figured it out," said the network security leader. "The sales engineers and professional services pros were outstanding from vetting to deployment. They made it easy to get the internal buy-in I needed to go with the right choice for our security program and our business."

DEPLOYMENT

Implementing the Skybox™ Security Suite, our customer was able first to build a comprehensive model of their network. More than just a map, the model provided an automatically updated, near-live environment that broke down silos of data between technologies and teams and unified it in a visual, interactive medium. The model, a key component of the Skybox platform, enhanced and simplified tasks such as access queries, attack path analysis and assessing potential impact of attacks on business and network functions.

The benefits to vulnerability management, especially, were evident almost immediately. Skybox automatically collected, normalized and analyzed vulnerability scan data, creating a vulnerability database unique to our customer where they could reference historical vulnerability data.

> "Along with SIEMs, Skybox is the most important tool in our infosecurity arsenal and a cornerstone of our SOC."
>
> — Network security leader, Skybox customer

The customer also quickly found a large amount of exposures, even on critical assets. "I was going to call Skybox support with a false positive because I thought there's no way this could be exposed," said the network security leader. "Turns out it had been sitting that way for a long time. Now we had the visibility we needed to know what to fix and how."

PROTECTING AGAINST WANNACRY

Our customer needed to know where their global network was exposed to the WannaCry ransomware attack.

Before using Skybox, they would have handed over routing tables to be analyzed, but that information wouldn't make clear how it related to geographic locations.

With Skybox, the company could quickly assess vulnerabilities and exposures to understand where in the network was most at risk. The same day as WannaCry broke out, all their critical vulnerabilities and exposures were in sight. Within 48 hours, all potentially at-risk networks had been properly assessed.

From the hundreds of un-patched systems discovered — even some thought to be patched — the company could fully mitigate all at-risk systems quickly.

ABOUT THE SOLUTION

The Skybox Security Suite provides the industry's broadest security management platform. By integrating with more than 120 networking and security technologies, including HPE ArcSight SIEM, Skybox gives comprehensive attack surface visibility and the context needed to accurately prioritize security issues. The company in this case study deployed four of the Suite's modules:

Skybox™ Vulnerability Control: eliminates blind spots and gives context of how vulnerabilities and threats impact you, prioritizing remediation in a way that makes sense for your organization

Skybox™ Network Assurance: illuminates on-prem and multi-cloud networks, complex network security zones and policy compliance violations, giving the insight needed to reduce attack vectors and network disruptions

Skybox™ Firewall Assurance: brings multi-vendor firewall estates into a single view and continuously monitors policy compliance, optimizes firewall rulesets and finds attack vectors that others miss

Skybox™ Change Manager: ends risky changes with network-aware planning and risk assessment, speeding up firewall change processes with customizable workflows and automation

RESULTS

With Skybox, the company had the comprehensive visibility they needed to start building an informed, effective security program. Efficient and automated processes greatly improved operations of their teams across the organization. And integration with a variety of solutions the company was already using broke down data silos to analyze information in context and more accurately prioritize security issues. "Along with SIEMs, Skybox is the most important tool in our infosecurity arsenal and a cornerstone of our SOC," said the network security leader.

"In cybersecurity, there's so many technologies and vendors and ways of looking at things. Skybox is the best tool for making sense of all those perspectives, even if what you see is, 'We have a major problem here.' It keeps us rooted in reality rather than in theory. It keeps us honest."

About Skybox Security

Skybox provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

REQUEST A DEMO!

SKYBOX™ SECURITY

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