CASE STUDY

Acquiring Actionable Intelligence to Protect Critical Business Assets

NATIONAL CREDIT UNION DEPLOYS SKYBOX® SECURITY TO AUTOMATE VULNERABILITY MANAGEMENT AND STAY AHEAD OF MULTI-STEP ATTACKS

CUSTOMER PROFILE

Our customer is a large, federal credit union with employees distributed worldwide, and a complex global network. The company generates more than $500 million in revenue annually and holds in excess of $20 billion in financial assets.

CHALLENGES

- ✓ Complex IT architecture with thousands of interdependencies
- ✓ Unable to effectively prioritize vulnerabilities and turn analysis into meaningful action
- ✓ Lack of visibility into the value of business assets
- ✓ No tools to correlate vulnerabilities and threats with likelihood and business impact
- ✓ Compliance with government and financial industry regulations

RESULTS

- ✓ Significantly reduced vulnerability exposure window
- ✓ Harnessed total visibility to analyze access paths and connectivity for improved security—even during changes
- ✓ Automated vulnerability management processes, prioritizing risk and remediation in context
- ✓ Simulated attacks to identify access paths and vulnerabilities
- ✓ Ensured continuous compliance and implemented a Security Risk Management (SRM) program

THE PROBLEM

The complexities of its network and the thousands of application interdependencies created a huge challenge for the credit union. The continuous flow of application and network changes along with software vulnerabilities overwhelmed the company. Security managers struggled to keep up with identifying, addressing and remediating threats before critical applications and data was compromised.

Lacking visibility across their network and into the value of their business assets, the credit union was forced to base remediation plans on vague vendor-provided risk labels, such as low, medium and high. As a result, administrators wasted countless hours rushing to implement patches for minor risks that weren't actually relevant within the context of the network.

SCOPE

Security managers needed to be able to correlate vulnerabilities and threats against their infrastructure, their critical assets, and the likelihood and potential business impact of a data breach. Only then could the company move beyond reactive firefighting to a proactive approach that effectively reduced risk, maximized return on investment and ensured continuous compliance.

With heightened concerns over security breaches and spikes in identity theft, the IT security team was on high alert and the CISO knew their security posture had to change.

DEPLOYMENT

Transforming an imprecise vulnerability management process into a focused, intelligent business risk management program was the first step. The company started by moving away from manual, sporadic scans to regular, automated monitoring. While this action reduced the window of vulnerability caused by software flaws, the CISO and his team still couldn't correlate vulnerabilities to business risk. "You get scan reports telling you that you have 5,000 critical vulnerabilities. But what does that actually mean?" asked the CISO.

> "We're focused on making Skybox the risk management center of our universe. We're building dashboards that show risk across the entire enterprise to gain deep insight into our overall risk. It's only possible because Skybox correlates our relevant business information with our real-world risks. It's phenomenal technology."
>
> *CISO, National Federal Credit Union*

Understanding Real Business Risk

The IT team had been responding to these threats with a fast and furious approach, downloading, testing and deploying patches throughout their infrastructure "We still had to manually correlate whether we should patch all our vulnerable systems and accept the business impact that meant to the organization," said the CISO. The credit union turned to Skybox to better understand risks and vulnerabilities within the context of the network.

Skybox Network Assurance collected data on network infrastructure, access and security device configurations, access paths, dependencies among devices and the risk exposure of critical assets. Network Assurance then used this data to model the network environment. From there, the organization was able to run access simulations and analyze connectivity paths and policy compliance in context with risk exposures.

With the addition of Skybox Vulnerability Control, the credit union collected network infrastructure and security configurations, evaluated vulnerability scan results, and better leveraged the modeling data from Network Assurance. Using patented attack simulation, Vulnerability Control calculated all possible access paths and highlighted vulnerabilities that could be exploited by internal and external attacks and tBy modeling the credit union's IT environment with Network Assurance and simulating multi-step attacks with Vulnerability Control, the security team was

able to focus on real-world threats that could bypass the company's deeply layered security defenses. Skybox contextually validated critical risks, empowering the security team to pinpoint the most critical vulnerabilities and have a visual representation of all possible attack vectors. From there, the solution evaluated the probability of successful exploitation and the severity of the impending business impact.

Skybox provided a precise and prioritized battle plan, and management gained unprecedented visibility into the organization's risk and governance profile. The organization transformed security management from a defensive practice to a business enablement tool.

Reducing the Attack Surface

Through implementing Skybox, the credit union could mitigate daily threats quickly. Using the simulated model, the CISO was able to visualize all potential attack vectors that a new vulnerability or attack could create. When he received reports from his vulnerability scanner that 400 servers were affected by a specific vulnerability, Skybox security analytics could deduce the three servers actually at risk. The analysis showed that the company's layers of security defenses—including firewall rules and network segmentation—provided sufficient mitigation. "The model shows us what systems need immediate attention and focuses our resources on fixing our most critical at-risk systems immediately. We can do the remaining patchwork at will," said the CISO.

Skybox helped the organization mitigate risks faster and reduce the vulnerability exposure window. "Actionable intelligence is really critical. You want to be able to make the best decisions in the shortest amount of time with the least amount of business impact. Instead of looking at four hundred servers, I can focus on three. It's about concentrating our efforts on the right things for the right reasons in the shortest amount of time."

Avoiding Risks of Network Changes

Skybox modeling capabilities proved exceptionally valuable to the CISO. Now—before the credit union deploys any new services, applications or network changes—the CISO can model planned changes within a virtual environment without experimenting on the live network and risking disruption or worse.

"It's actionable intelligence when I need it," said the CISO. "The organization can maximize connectivity, minimize risk exposure, reduce IT workload and improve accuracy and timeliness through automated risk modeling."

Ensuring Continuous Compliance

Deploying Skybox radically changed the federal regulatory audit process. "This was the first year where rather than tearing through firewall rules, IDS logs and incident reports, the examiners focused on our risk management and assessment plans and our infrastructure strategy," said the CISO. "The reports that Skybox generated made it completely self-explanatory to regulators as to why certain assets were more critical than others. It was a dramatic shift for us."

With the ability to associate the credit union's security threats and vulnerabilities to their actual business impact and likelihood of breach, it's no surprise that the CISO positioned Skybox as the cornerstone of the organization's information security management program. "We're focused on making Skybox the risk management center of our universe. We're building dashboards that show risk across the entire enterprise to gain deep insight into our overall risk. It's only possible because Skybox correlates our relevant business information with our real-world risks."

ABOUT THE SOLUTION

The credit union deployed two modules of the Skybox Security Suite—Network Assurance and Vulnerability Control. Using Network Assurance's comprehensive and automated modeling capabilities, the customer was able to gain complete visibility and command of network access and routes, laying the foundation for strategic security initiatives and maintaining continuous compliance. Adding Vulnerability Control not only gave the customer unique insight to how vulnerabilities could impact their network, but enabled them to work with the network model and simulate multi-step attacks without affecting the network. The robust solution gave them an in-depth understanding of how their security would perform under a real attack and helped them better protect critical assets.

RESULTS

Using Skybox, the credit union achieved total network visibility across devices and interdependent systems. The organization fully automated vulnerability detection, assessment, prioritization and remediation within the context of the network. With patented attack simulation tools, the company was able to identify access paths and vulnerabilities even for complex, multi-step attacks. The credit union also incorporated modeling tools to assess the impact of a proposed change prior to implementation, preventing disruption to the live network. Automated compliance reports transformed the compliance audit process, elevating the discourse from dissecting rules, logs and reports to a strategic discussion on risk management and assessment and infrastructure plans. In the words of the CISO, "Skybox is phenomenal technology."

About Skybox Security

Skybox arms security teams with a powerful set of security management solutions that extract insight from traditionally siloed data 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