SKYBOX SECURITY

Case Study

Oil and gas company reduced remediation time from weeks to hours

Skybox Vulnerability Control increases accuracy, efficiency and effectiveness of remediation process

Customer profile

+ One of the world's largest petroleum refining companies
+ Employs more than 40,000 employees
+ Headquartered in Spain and operating in 28 countries

Business value

+ Reduced MTTR from weeks to hours
+ Significantly reduced false positively rate
+ Improved operational efficiency through automation
+ Cost reduction due to less frequent scanning

Challenges

+ Large and complex network environment
+ Disruptive and costly network scanning process
+ Long remediation timelines
+ Unacceptable corporate risk levels

Results

+ Improved process to identify and remediate vulnerabilities
+ More effective prioritization and automation of remediation tasks
+ Eliminated network disruption through passive vulnerability assessment
+ Implemented continuous vulnerability discovery and daily reporting
+ Augmented scanning and minimized disruption

Solution

Skybox Vulnerability Control provides organizations with the full context of their attack surface – across their network, cloud and security infrastructure – to find where they are exposed to cyber-attacks, quantify the risks of exploitation, prioritize vulnerabilities and provide optimal remediation options to reduce the highest levels of risk.

“We no longer have to deal with false positives,” said the CISO. “We’ve been using Skybox Vulnerability Control for more than a year, and our false positive rate has dropped significantly from the 20 percent we were experiencing. We can now prioritize our efforts on deploying patches.”

Objectives

The security team was conducting regular network scans on core servers; however, scanning critical services across the firewall infrastructure caused disruption on the network. The team did not have access to scan the DMZ, and some portions of the network could only be scanned on Sundays at a premium price to avoid disruption of critical services. Further, the scan results generated a false positive rate of at least 20 percent. With thousands of servers and disparate firewalls, load balancers and routers, the company needed a more thorough solution.

While the security team was focused on addressing threats as soon as they were identified, the path from vulnerability discovery to remediation took too long and created unac ceptable levels of corporate risk.

In addition to improving the swiftness of remediation, the team needed to solve the problem earlier in the lifecycle —detecting threats faster and more accurately. To achieve this, the team needed total network visibility and frequent access to identify and prioritize vulnerabilities across the entire network.

Approach

The organization sought an alternative to traditional scanning that wouldn’t impact network operations. The security team also needed an accurate, continuous view of their attack surface. To identify vulnerabilities faster and shorten the time frame to remediation, the company wanted continuous monitoring and daily reporting to stay on track.

For these reasons, the security team selected Skybox® Vulnerability Control. This product offers passive vulnerability assessment, detects vulnerabilities on traditionally “unscannable” devices and zones and prioritizes and remediates vulnerabilities daily.

Skybox Vulnerability Control identified vul nerabilities across their entire attack surface, integrating with the customer’s own security stack and utilizing advanced security analytics to passively identify vulnerabilities.

Reduced costs due to less scanning
The organization continued to supplement Skybox with traditional active scanning. However, the company no longer needed to run active scans as often or scan critical services. This reduced the cost associated with the regular Sunday scans.

Improved communication between network operations and security teams
They also benefited from improved workflow communications between the network operations and security teams, as each team had access to a common intuitive dashboard highlighting immediate remediation actions. No more guessing, unnecessary patching or wasted work.

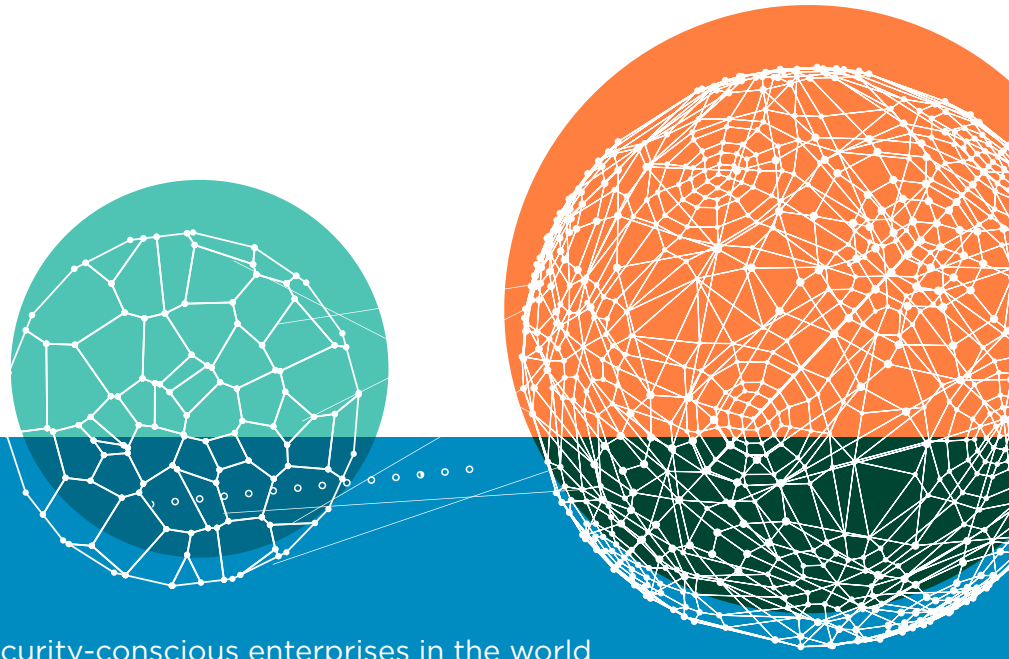
Results

Using Skybox Vulnerability Control, the organization was able to identify vulnerabilities and execute remediation more accurately and faster, reducing the window of exposure from weeks to hours. Passive vulnerability assessments eliminated network disruption, enabling access to critical services, providing daily, accurate vulnerability intelligence and reducing costs. The solution reduced false positives, and allowed the team to shift scarce security resources to other priorities.

See it live

Interested in a guided demo of Skybox solutions for vulnerability and threat management or security policy management?

Request a demo >



ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization.

skyboxsecurity.com

SKYBOX SECURITY