CASE STUDY

Reducing Vulnerability Exposure from Weeks to Hours

MULTINATIONAL OIL AND GAS PROVIDER DRAMATICALLY IMPROVES TIME TO DETECT AND REMEDIATE VULNERABILITIES

CUSTOMER PROFILE

Headquartered in Spain and operating in more than 28 countries, our customer is one of the world's largest petroleum refining companies and employs more than 40,000 people globally.

CHALLENGES

- ✓ Large and complex network environment
- ✓ Disruptive and costly network scanning process
- ✓ Wide vulnerability exposure window
- ✓ Unacceptable corporate risk levels

RESULTS

- ✓ Reduced process to detect and remediate vulnerabilities from weeks to hours
- ✓ Realized a sizable reduction in resource drain through automated, prioritized action items
- ✓ Significantly reduced false positive rates to prevent unnecessary patching and wasted work
- ✓ Eliminated network disruption through scanless vulnerability assessment
- ✓ Implemented continuous vulnerability detection and daily reporting

THE PROBLEM

The IT 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 IT security team was focused on addressing threats as soon as they were identified, the time of exposure to vulnerabilities was too wide. The path from vulnerability detection to remediation took too long and created unacceptable levels of corporate risk.

In addition to improving the swiftness of remediation, the team needed to solve the problem upstream—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.

SCOPE AND SELECTION CRITERIA

The organization sought an alternative to traditional scanning that wouldn't impact network operations. The IT 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 IT security team selected Skybox® Vulnerability Control. The module offers scanless vulnerability assessment, detects vulnerabilities on traditionally "unscannable" devices and zones and prioritizes and remediates vulnerabilities every day.

> "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."
>
> *CISO, Multi-National Oil and Gas Company*

DEPLOYMENT

Skybox Vulnerability Control identified vulnerabilities across their entire attack surface, leveraging existing databases, intelligence repositories and its own advanced security analytics to determine vulnerabilities without a scan.

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 their infamous Sunday scans. Resource savings were also realized through improved workflow communications between the network operations and IT security teams, due to Vulnerability Control's yields of actionable intelligence. No more guessing, unnecessary patching or wasted work.

"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."

ABOUT SKYBOX VULNERABILITY CONTROL

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. It then applies attack simulation, superior vulnerability intelligence and powerful, analytics to quickly prioritize and eliminate attack vectors.

RESULTS

Using Skybox Vulnerability Control, the organization was able to identify vulnerabilities and execute remediation faster and more accurately, reducing the window of exposure from weeks to mere hours. Scanless 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.

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