CASE STUDY

Achieving Fully Automated Cybersecurity Risk Management and FISMA Compliance

USAID ELIMINATES THE GUESSWORK AROUND THREAT DETECTION, ASSESSMENT AND PRIORITIZATION AND SCORES AN A+ ON FISMA COMPLIANCE

CUSTOMER PROFILE

The United States Agency for International Development (USAID) is an independent agency that provides economic, development and humanitarian assistance worldwide to support U.S. foreign policy initiatives. The government agency fosters economic growth in poverty-stricken areas around the globe to help advance peace, stability and developing democracies. Headquartered in Washington, D.C., USAID has 8,000 employees across field offices and missions in more than 70 countries.

CHALLENGES

- ✓ Decentralized and complex IT infrastructure
- ✓ Lack of automated tools to detect, assess and prioritize threats for remediation
- ✓ Inability to correlate technology asset values with security information
- ✓ Problems with managing FISMA compliance requirements
- ✓ No way to assess how proposed changes could impact availability and risk exposure

RESULTS

- ✓ Provided total visibility across the entire attack surface
- ✓ Implemented continuous threat assessment with automated prioritized action items
- ✓ Correlated technology asset values with data in firewalls, routers and vulnerability scanners
- ✓ Raised the agency's FISMA compliance grade from a C- to an A+
- ✓ Incorporated risk modeling and attack simulation to assess impact before implementing changes

THE PROBLEM

Like all federal agencies, USAID is subject to stringent regulatory requirements. These regulations stipulate that a strict and verifiable threat and control management program be in place across the entire organization. The IT security team needed to understand the risk profile for each remote location and how these profiles were shifting over time.

The stakes were high—each year the federal government grades the effectiveness of USAID's information security program to ensure compliance with the Federal Information Security Management Act (FISMA). Before implementing Skybox®, the agency received a C-.

The agency was focused on establishing clear security metrics and ensuring that IT managers in remote offices were consistently following remediation procedures. To make sure they continuously assess risk, patch exposed systems, manage controls and maintain compliance, the CSO's office graded each remote office monthly.

Prioritizing identified risks to USAID's global network infrastructure was a never-ending process. With the agency relying on connectivity from more than 55 Internet service providers and managing more than 16,000 networked devices, it was clear that it needed continuous risk and mitigation assessment.

The network presented a complex infrastructure maintained by more than 100 firewalls and 300 routers with aggregated access rules reaching the tens of thousands. The diverse application environment included Apache Web servers, Windows 2000 Internet Information Servers, Linux and UNIX operating systems and Oracle and SQL server databases. The CSO and his team needed a way to determine what vulnerabilities—based on pre-defined metrics—posed the greatest risk.

"We wanted to be able to automate risk detection and assessment. Traditional tools helped but ultimately fell short," said the program manager for the USAID ISSO team. "Our vulnerability management program had been a tremendous success. However, we had no way to measure risk within the context of the network. With 16,000 devices, it's not helpful or practical to weigh risks evenly. We needed insight into actual risk levels based on threat profiles, asset values and security controls."

> "Skybox immediately helped us find problems we hadn't considered, and to fix things were would have never found. Skybox was the perfect fit for us."
>
> *Program Manager, USAID ISSO Team*

SCOPE AND SELECTION CRITERIA

As a government agency with a vast global IT infrastructure, continuously assessing and mitigating risks on the network was a key concern. With technology changing and accelerating rapidly, there was a never-ending rollout of new and enhanced applications, operating system updates and new software vendor security patches. Routine updates to access control lists, firewall rulesets and configuration changes further compounded network complexities. The agency needed to ensure that network traffic flowed safely through routers, gateways and firewalls.

The agency was unable to identify, assess, and prioritize threats for remediation based on actual risk to the business. Further, it needed to correlate the technology asset value with layers of security information held within its firewalls, routers and vulnerability scan information. While the agency's IT infrastructure was dependable, it was one mistake away from a misconfigured firewall, proxy or overlooked patch that could blow a hole through otherwise sound security. It was an intricate challenge to decipher critical misconfigurations and vulnerabilities that could lead to breach around the agency's most valuable assets and information.

With a complicated IT infrastructure and some of the most stringent compliance reporting around, USAID needed a comprehensive and streamlined solution to bring their entire network into view, simplify security tasks and easily maintain and prove compliance.

DEPLOYMENT

USAID deployed Skybox Vulnerability Control to gain a deeper understanding of the risks present on the network. Rather than relying on educated guesses around trouble spots on the network, the CSO and his team were empowered to detect, assess, prioritize and remediate threats through intelligent analysis of the context of the network.

Seeing Real Risk

The intelligence comes from Skybox's unique network modeling and attack simulation capabilities, visualizing and quantifying USAID's complete security risk profile. "Now we can see the likelihood as well as the impact analysis that a real-world attack scenario could impose on a specific vulnerability," said the program manager. "For the first time, we can understand the impact of a multi-faceted attack and even visualize how such attacks could happen."

For example, USAID can now quickly determine if a lower-ranking vulnerability could actually pose significant risk to the agency as a stepping stone for an attack on a mission-critical asset. "We can drive operations to mitigate only the most critical vulnerabilities—the ones that require immediate attention. It's vitally important that the agency be able to view risk from an operational and business perspective, and we needed to know if low or medium vulnerabilities were actually creating more risk than the agency had intended to accept."

Every day, Vulnerability Control automatically collects data across the entire attack surface, including network and security devices like firewalls, routers and third-party vulnerability scans, to generate the model. "Skybox looks at the mountain of data and identifies the top priorities. This gives us the context we need to see our current up-to-the-day risks. Vulnerability Control makes it possible for the entire security team to be in tune with anything that changes our risk profile and to respond accordingly using the fewest resources possible."

Mitigating the Risks of Control Change

USAID extended the initiative and rolled out more modules of the Skybox Security Suite—Skybox Firewall Assurance and Skybox Network Assurance. This enabled the firewall management team to visualize and understand how changes to complex firewall rules could impact system availability and risk exposure before those changes were actually implemented on the live network.

With Firewall Assurance and Network Assurance, USAID could now continuously measure the effectiveness of its network policy compliance and security control processes as well as perform automated firewall audits. The two solutions made it possible for the agency to monitor rogue changes to controls or systems that haven't been approved or properly documented. "That's a hard thing to control when you're working with a large, geographically dispersed network," said the program manager. "Following the implementation of Firewall Assurance and Network Assurance, we are now able to make sure that our change control process is working and effective, and that nothing happens outside the proper procedures."

ABOUT THE SOLUTION

Deploying three modules of the Skybox Security Suite—Vulnerability Control, Firewall Assurance and Network Assurance—USAID was able to implement a top-of-the-line risk management program and receive an A+ FISMA rating. Vulnerability Control took them beyond scanners, using analytics and the context of the attack surface to identify exposures, prioritize risks, fill in blind spots and quickly focus remediation efforts—every day. Firewall Assurance and Network Assurance helped to visualize the network and firewall state and continuously monitor security and compliance, even as the network changed.

RESULTS

The struggle to assess and mitigate risks posed by complex networks is challenging. USAID's progress from a traditional vulnerability management program to a continuous and quantified security risk management process has cleared the way for the agency to be able to focus on the vulnerabilities and risks that matter most. "From the start, Skybox solutions empowered USAID to spot and model potential risks the agency couldn't have seen or understood previously. "Skybox immediately helped us find problems we hadn't considered, and to fix things were would have never found. Skybox was the perfect fit for us."

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