CASE STUDY

Unifying Risk Management Solutions to Meet Government and Industry Standards

STATE HEALTH AND HUMAN SERVICES AGENCY INTEGRATES RISK MANAGEMENT SOLUTIONS TO BUILD BEST-IN-CLASS NETWORK SECURITY AND COMPLIANCE PROFILE

CUSTOMER PROFILE

Our customer is a state Health and Human Services (HHS) agency that provides eligibility and enrollment services to manage benefits including Medicaid, children's health insurance and other national and state assistance programs. The organization runs one of the largest integrated eligibility information systems in the United States.

CHALLENGES

- ✓ Implementing new technologies while minimizing risk
- ✓ Building a strong network security and compliance profile
- ✓ Navigating complex government and industry regulations
- ✓ Avoiding investment in disjointed systems from multiple vendors
- ✓ Achieving seamless integration to ensure continuous network security and compliance

RESULTS

- ✓ Automated network discovery, firewall audits and network compliance assessments
- ✓ Achieved a holistic understanding of security risk and compliance across the IT infrastructure
- ✓ Created a centralized view of the network topology, all security controls and endpoints
- ✓ Incorporated risk and impact modeling including sandbox and "what-if" analysis
- ✓ Integrated seamlessly with Symantec Control Compliance Suite (CCS) for IT governance, risk management and compliance

THE PROBLEM

As an HHS agency processing data from health services and other governmental programs, the customer was subject to both industry and governmental data security regulations. The security team was tasked with achieving and maintaining compliance with automated and transparent processes. They also needed to leverage new technologies to support the benefits system while managing and minimizing risk, and doing so in a way that provided auditable compliance.

Managing one of the largest systems of its kind in the nation, the security team understood it would have to go beyond mandated security standards and compliance requirements to implement a broader security risk management strategy that would continuously protect all data and resources in the system.

SCOPE AND SELECTION CRITERIA

Often multiple vendor solutions, are used together to assess cybersecurity risk exposures, but those solutions only address separate pieces of a much larger network security puzzle. Making sense of this piecemeal approach is time consuming, prone to error and, by the time the analysis is complete, the information is stale or the environment has changed.

The customer needed an integrated solution that provided comprehensive and prioritized intelligence for security and compliance management. They turned to a trusted partner to help determine the best combination of security solutions to meet their needs. The partner recommended deploying Symantec CCS integrated with the Skybox® Security Suite.

DEPLOYMENT

Generating a Holistic View for Security and Compliance Management

To secure their benefits system, the security team needed to achieve a holistic and continuous understanding of security risk and compliance status across the entire IT infrastructure, including both the network layer and endpoints. Skybox joined forces with Symantec CCS to create a centralized, system-wide view of the network topology and policy compliance for all network security controls and endpoints.

The Skybox Security Suite provided automated network discovery, firewall audits and network compliance assessments. Skybox empowered the security team to achieve total network visibility; they could now view network topology and monitor assets for changes, including modeling the level of risk prior to implementation that a proposed change could introduce. This risk and impact assessment includes sandbox and "what-if" capabilities for scenario-based analysis. Skybox Firewall Assurance and Skybox Network Assurance ensured common builds across enterprise firewalls, routers and other devices. By deploying Skybox, the customer reduced overall risks associated with network security and infrastructure.

The Symantec CCS integration provided a broad IT Governance, Risk Management and Compliance (IT-GRC) framework and endpoint compliance analysis tool. Symantec CCS gives a centralized view of all server configurations and reports security risks associated with server-based assets. This includes monitoring server assets for any and all changes and assessing their level of risk and impact.

Implementing a 4-Step Risk Management & Compliance Process

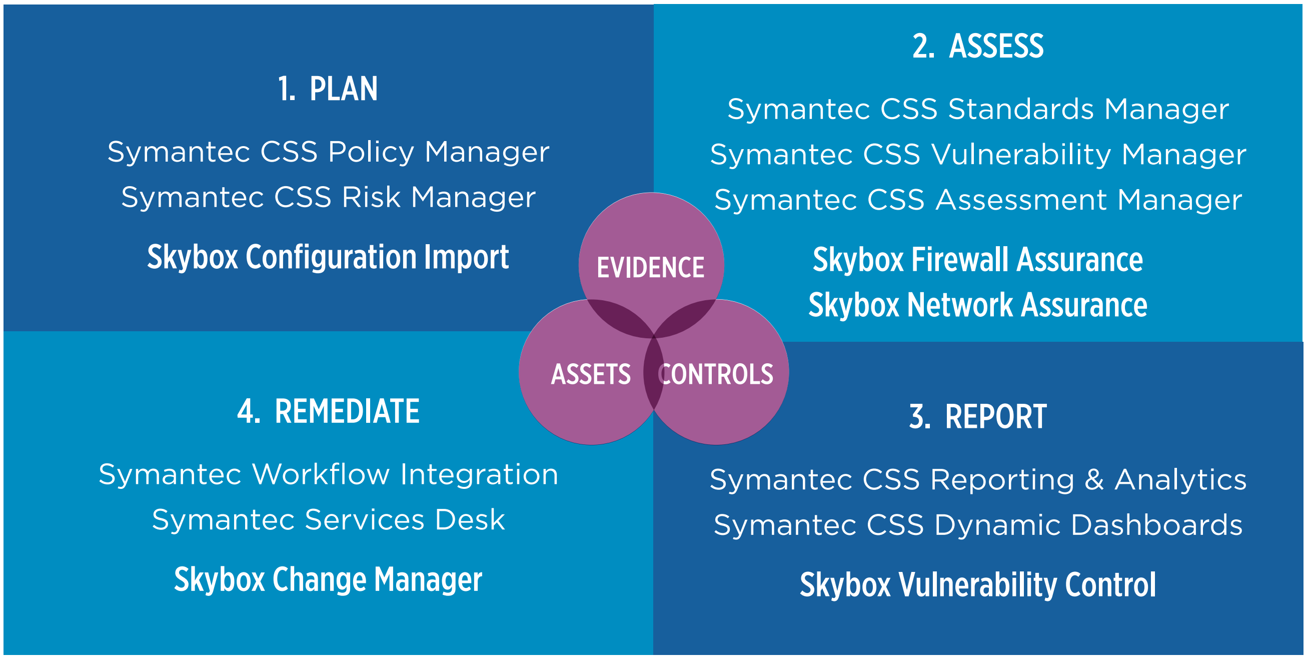
The integration of the Skybox Security Suite and Symantec CCS presented the security team with a four-step approach to continuous compliance: plan, assess, prioritize and remediate. After remediation, new security plans are established that impact future rounds of assessment and reporting.

During initial planning, the security team established the parameters in on-going risk assessments. They put policies in place to address government, health industry and other compliance regulatory requirements as well as internal policies. They ensured that policies mapped to appropriate controls, and that duplications were eliminated. They also established key performance indicators and determined asset criticality to support risk prioritization.

In the assessment phase, data was gathered by both Skybox and Symantec and was combined for a composite view. The solutions also enable the security team to combine input from other third-party tools already in use to make the most of their investments. This data was evaluated against the policies and objectives that were established by the security team during the planning stage, allowing them to identify vulnerabilities and deviations from technical standards, evaluate procedural controls and prioritize risk.

During reporting, the data gathered during assessment from Skybox, Symantec and third-party tools was aggregated and analyzed into an overall IT risk and compliance profile, incorporating all assets used to support the benefits system. The security team was able to generate Web-based dashboards and reports specific to various stakeholders, including IT operations, management and auditors: for example, reports for senior management focused on business risk. These customized dashboards and reports are designed to address the concerns and priorities of each group, thereby helping the security team drive change and accountability to ensure security and compliance.

Lastly, the security team was able to establish remediation priorities based on the degree of risk posed to the benefit system. Both Skybox and Symantec CCS assess risk by looking at context-aware criteria, including asset criticality, security controls and business objectives. The team was able to prioritize remediation as well as identify low-priority risks that didn't need to be addressed because mitigating controls were in place. The risk management solutions automated remediation tickets, integrating with popular ticketing systems. Closed-loop tracking was used to reassess asset status once the ticket was closed, confirming that changes were made correctly to eliminate risk.


1. PLAN

Symantec CSS Policy Manager
Symantec CSS Risk Manager
Skybox Configuration Import

2. ASSESS

Symantec CSS Standards Manager
Symantec CSS Vulnerability Manager
Symantec CSS Assessment Manager
Skybox Firewall Assurance
Skybox Network Assurance

3. REPORT

Symantec CSS Reporting & Analytics
Symantec CSS Dynamic Dashboards
Skybox Vulnerability Control

4. REMEDIATE

Symantec Workflow Integration
Symantec Services Desk
Skybox Change Manager

ABOUT THE SOLUTION

The agency deployed three modules two modules of the Skybox Security Suite—Firewall Assurance and Network Assurance—both integrated with Symantec CCS. Firewall Assurance helped them continuously maintain clean, optimized and compliant firewall state, bringing all firewalls and their rulesets into one view. Network Assurance illuminated complex network security zones and policy compliance violations, giving the insight needed to reduce attack vectors and network disruptions. Combined, the solutions positioned the agency to efficiently reduce risk, easily maintaining compliance and producing audits at any time to prove security and compliance posture.

RESULTS

With the largest benefits system in the United States, the security team realized that manual processes were unsustainable and implemented an automated risk management solution to continuously monitor network security and compliance status. This approach greatly minimized the agency's time spent ensuring compliance with internal and external standards and reduced their audit burden. This allowed the organization to focus its IT resources on other tasks to support the core functionality of the benefits system. Beyond compliance, automation of the agency's IT GRC processes provided more accurate and timely data. This enabled the security team to respond faster to critical IT issues, improving their overall security posture.

The security team now has a centralized view of its network assets and IT infrastructure. This integrated, automated solution is a key component of their continuous monitoring initiative. With the combined power of Skybox Security Suite and Symantec CCS, the security team can maintain compliance across the entire IT infrastructure, meeting government, industry and internal requirements and establishing security best practices.

About Skybox Security

Skybox arms security leaders with a powerful set of integrated cybersecurity solutions that give unprecedented visibility of the attack surface and key Indicators of Exposure (IOEs). This gives security professionals the insight they need to quickly make decisions about how to prioritize and address threat exposures that put their organization at risk.

REQUEST A DEMO!

SKYBOX™ SECURITY

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