LARGE INTERNET SERVICES COMPANY OVER-COMES COMPLIANCE VISIBILITY CHALLENGES

The Cavirin solution provides a single, unified view across this organization's complex hybrid infrastructure mapping ISO and NIST CSF frameworks to each asset to strengthen its cybersecurity posture.

CAVIRIN BENEFITS

- A single, unified view, including a CyberPosture Score, across a hybrid infrastructure

- Automation of manual and tedious compliance assess-ment processes

- A wizard-based approach to OS hardening

- Secure agentless cloud migration with multi-cloud deployments

- Access to a rich set of security policy frameworks

Overview

As one of the largest global data center and "colocation" providers—this company's IT team manages upwards of 15,000 servers and 13,500 endpoints spanning traditional data centers, Azure, and AWS environments—compliance, visibility, and OS hardening (making an operating system more secure) across this diverse/hybrid environment were critical in this organization's decision to choose Cavirin.

Visibility

Concerns this company had when selecting a solution, as it continues along the journey to grow and migrate applications to Azure and AWS, was the overall lack of visibility into cloud endpoints and fears of an inaccurate view presented by disjointed security tools across its hybrid infrastructure attack surface. These concerns were eliminated when evaluators and decision mak-ers were provided a single, unified view that included a CyberPosture Score across their hybrid infrastructure, in which they were able to drill down into to further assess the risk coming from asset groups, individual resources and policy control families and operating systems.

Compliance

The ability to map and automate ISO and NIST CSF frameworks to each asset, supporting the company's FEDRAMP-approved system (the stamp of approval for government cloud computing), was a key requirement for this organization. In addition, the company is utilizing customizable policy frameworks, with remediation guidance, to meet other mission critical organization requirements critical for this company's hybrid cloud security posture.

Automated OS Hardening

A differentiator of the Cavirin solution is a wizard-based approach to OS hardening. OS hardening, (according to Pearson IT Certification) is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services. Cavirin's approach automates discovery, assessment, and remediation guidance, shortening the time and effort required to secure a complex environment. In the case of this organization, the choice was easy —either roll out a new customer one at a time or automate deployment. The company's desired third-party integration was Ansible, used for configuration management for Linux systems. At the front-end as part of Dev and QA, Cavirin will be used to harden 'golden' configurations before deployment. This creates a known security posture baseline, with all production instances verified. Once deployed, Cavirin will periodically assess all instances, checking for drift against the known baseline and recommending and carrying out remediation to re-establish the instances' golden posture.

Automate Security Policies Across The Hybrid Cloud

By implementing the Cavirin solution, this internet services company is able to take a leadership role in ensuring best security practices and automating industry guidelines across their diverse Windows and Linux environments. They are excited to now have the ability to monitor their CyberPosture and compliance across their entire hybrid environment from a single, unified view. They believe this visibility will help them build a sustainable competitive advantage moving forward.

ADDITIONAL INFORMATION

To learn more about the benefits of the Cavirin CyberPosture Intelligence Platform email us at, **info@cavirin.com** or visit our Web site, **www.cavirin.com**

Cavirin is a global provider of risk, cybersecurity, and compliance posture intelligence for the hybrid cloud. Our machine learning driven CyberPosture intelligence delivers real-time risk & cybersecurity posture management, automated compliance, and facilitates secure cloud migration.