



## CAVIRIN BENEFITS

- A single, unified view, including a Cyber Posture Score, across a hybrid infrastructure
- Automation of manual and tedious compliance assessment processes to mitigate vulnerabilities
- A wizard-based approach to OS hardening
- Access to a rich set of security policy frameworks with customizable options
- Visibility across all IT asset types

## A FINANCIAL APPLICATIONS SOFTWARE COMPANY USES CAVIRIN TO STRENGTHEN ITS SECURITY POSTURE

An American software company providing financial data aggregation and analytics for banks, developers and innovators uses Cavirin to strengthen its overall cybersecurity posture for its AWS, Docker and on-premise implementations. Being part of a fintech ecosystem, protecting sensitive client data at all times and proving security and compliance to external regulators, as well as internal stakeholders, is essential; therefore, Cavirin built-in additional safeguards on top of the chosen PCI, SOC 2, Patches and Vulnerabilities frameworks to further strengthen their overall CyberPosture.

### Challenge

Partnering with the top financial institutions in the United States, this organization enables a massive data network, and is bound to the same high security standards as its clients. This organization wanted to ensure that its hybrid environment was continually protected at all times, with not only visibility but remediation guidelines to adhere to its strict company safeguards. Maintaining its “golden posture” amongst its various operating systems leveraging packaged and custom scripts with one central view was key to this company choosing Cavirin.

### Beyond Compliance

Coming into the project this organization knew that it wanted to map all its assets to the Cavirin PCI, SOC 2 and Patches and Vulnerabilities frameworks and receive remediation guidance but, in addition, it was critical the company could integrate its customized scripts, running across various operating systems validating specific configurations, into the Cavirin platform so they could have visibility and be alerted to risks further accommodating their advanced security requirements. This organization’s IT team is regularly changing, suppressing and modifying the default policies to maintain high accuracy of compliance across this diverse environment, and is using Cavirin to push the limits of its current processes and tool kits.

## Case Study: Software Company

---

### Reducing Attack Surface of Docker Containers

A differentiator of the Cavirin platform is a wizard-based approach to OS hardening, shortening the time and effort required to connect to existing systems. 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. By utilizing Cavirin's Docker Image Hardening, Patches and Vulnerabilities, along with the various CIS Policy Packs within this security process it is able to analyze the Docker container for security risks without pushing into production until verified.

### In Summary

Flexibility was key for this client. The short amount of time it took to bring the company's hybrid environment, with inherited security tools and scripts, into a single and accurate view focused on further strengthening their security posture was the tipping point for this organization. By implementing the Cavirin solution this company is able to take a lean forward approach in ensuring best practices and industry guidelines are automatically applied across their diverse windows and Linux environment. They now have the ability to monitor the CyberPosture and compliance of their entire environment from a single view.

## ADDITIONAL INFORMATION

To learn more about the benefits of the Cavirin CyberPosture Intelligence Platform email us at, [info@cavirin.com](mailto:info@cavirin.com) or visit our Web site, [www.cavirin.com](http://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.