CASE STUDY

Achieving PCI Compliance

An industry-leading Financial Tech company provides cloud-based accounts payable and payment automation solutions for mid-market finance professionals and includes guaranteed fraud protection. As such, they are required to be PCI compliant to assure current and future customers that their data is secure. Using F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, the company achieved their compliance goals, and at the same time, significantly improved security visibility in their infrastructure.

The Challenge

In order to assure customers that their data was secure and protected, the company's Director of Operations needed to organize and monitor his environment to pass a PCI audit. To satisfy the audit, his team set up multiple new technologies including NTP for clock synchronization, host and network intrusion detection, log management and archiving, file integrity management, and encryption key management.

> *"[Distributed Cloud AIP] enabled us to meet several PCI requirements simultaneously with one solution."*
>
> **Director of Operations**

The Solution: Distributed Cloud AIP

The company chose Distributed Cloud AIP because its suite of security features significantly mitigates risk and provides deep security visibility into cloud environments. These features include real-time monitoring of users and system activity via Distributed Cloud AIP's Host Intrusion Detection (HIDS), as well as ongoing vulnerability assessments that allow them

Founded
2010

Industry
FinTech

Employees
50+

to update their systems to the most recent, and least vulnerable packages. Additionally, File Integrity Monitoring (FIM) enables them to ensure the safety of sensitive data by alerting whenever sensitive files are accessed.

To obtain the highest level of PCI certification, the team engaged a third-party Qualified Security Assessor (QSA) to audit their environment. The audit was a rigorous assessment that required the documentation of all relevant policies and procedures as well as technical details and evidence. Additionally they were required to demonstrate that the Distributed Cloud AIP agent does not manipulate or collect any sensitive data, and cannot perform any command and control.

The Result

Distributed Cloud AIP greatly simplified the process of achieving PCI compliance for them. The Director of Operations and his team continue to be successful and efficient with their cloud security strategy because "[Distributed Cloud AIP] enabled us to meet several PCI requirements simultaneously with one solution. Specifically, [Distributed Cloud AIP] provides Host Intrusion Detection, Network Intrusion Detection, system access monitoring, system user activity logging, file integrity monitoring, and the logging and archiving of all related events in the event that a breach occurs and a forensic analysis is required. This includes the ability to maintain archived logs in a manner that they cannot be tampered with."

He went on to state that "[Distributed Cloud AIP] continues to innovate and improve their platform. Over time it has become easier to use, and they have added useful features, like a daily report of installed applications with newly identified security issues that need to be mitigated."

Since passing its PCI audit, the company has been offering a valuable and secure service for their financial clients.

A Bit About PCI Compliance

PCI DSS (the Payment Card Industry Data Security Standard) was created by a cooperative of credit card providers in 2004, including Visa, MasterCard, American Express, Discover, and JCB. The purpose was to introduce a standard for handling cardholder data and to reduce credit card fraud.

To pass a PCI audit, organizations must show a Qualified Security Assessor (QSA) that they have documented controls that they can use to handle cardholder data securely. Any systems inside the network that process or otherwise contain cardholder data are considered to be inside the PCI gap, and require that these controls be applied. It is standard practice to segregate these systems and networks from everything else as a way to improve security, and it's also imperative that these involved systems have tools to protect the security of the cardholder data.

Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.