



# MineralTree Achieves PCI Compliance and Improved Security Visibility

## Customer Problem

MineralTree 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, MineralTree not only achieved their compliance goals but also significantly improved security visibility throughout their infrastructure.

## The Solution

MineralTree chose Distributed Cloud AIP because its security features significantly mitigate risk and provide deep security visibility into cloud environments. These features include real-time monitoring of user and system activity via Host Intrusion Detection (HIDS), as well as ongoing vulnerability assessments that allow MineralTree to update their systems to the most recent, and least vulnerable packages. Additionally, File Integrity Monitoring (FIM) enables MineralTree to ensure the safety of sensitive data by alerting whenever sensitive files are accessed.

To obtain the highest level of PCI certification, MineralTree 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, MineralTree was required to demonstrate that the Distributed Cloud AIP agent does not manipulate or collect any sensitive data, and cannot perform any command and control.



**Founded**  
2010

**Headquarters**  
Cambridge, MA

**Industry**  
FinTech

**Employees**  
127

## Outcomes and Benefits

Distributed Cloud AIP's platform greatly simplified MineralTree's process for achieving PCI compliance and enabled them to meet several PCI requirements simultaneously with one solution. As part of their cloud security strategy, MineralTree continues to leverage Distributed Cloud AIP's 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 if a breach occurs and a forensic analysis is required. This includes the ability to maintain archived logs in a manner that cannot be tampered with.

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

**Kevin Eberman, Director of Operations, MineralTree**

According to Kevin Eberman, MineralTree's Director of Operations, "[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."

## 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.**

