FIM+ Case Study:
Improved PCI/DSS Compliance for Major Airline

Challenge: Meet Payment Card Industry Data Security Standard Requirements (PCI/DSS)

A large outsourcer needed to meet PCI/DSS requirements 10.5 and 11.5 for a major airline client. These requirements were currently being met using a manually intensive compensating control. Since V4 of the Data Security Standard was coming out and was going to tighten the PCI's acceptance criteria for compensating controls, the company needed real file integrity monitoring on their mainframe.

Solution: MainTegrity® FIM+
FIM+ is a full function File Integrity Monitoring software product that runs on IBM mainframes running z/OS. FIM+ detects any changes on at the member and dataset level by creating and comparing keys from the contents of the files. It supports both z/OS and USS file systems.

FIM+ provides a hardening of the cybersecurity posture for z/OS mainframes and enables organizations to comply with security standards produced by the PCI and NIST. Specifically, FIM+ meets PCI/DSS section 10.5 (FIM required) and 11.5 (monitor logs) compliance and provides the following report weekly.

With FIM+, it was a simple task to set up ongoing scans of application software, system software, logs and backups and parameter sets on a schedule established by the client. Compliance reports were automatically emailed to the clients PCI Compliance Officer. The following report is the report being emailed.

PCI Audit Report **Date: Oct 27, 2021**

Date/Time	Component	System	Scan Stat	Scan Type	Entries	Added	Removed	Modified	Malicious
2020/09/29 09:06:24	AuthSystemLibs	SYSA	NoChange	Quick	42757	0	0	0	0
2020/09/29 09:00:08	AuthSystemLibs	SYSA	NoChange	Full	42757	0	0	0	0
2020/09/29 08:53:20	ProdConfig	SYSA	NoChange	Full	826	0	0	0	0
2020/09/29 08:52:44	ProdConfig	SYSA	NoChange	Quick	826	0	0	0	0
2020/09/29 08:51:52	ProdConfig	SYSA	NoChange	Full	826	0	0	0	0
2020/09/29 07:02:26	Monitor00010	SYSC	NoChange	Full	14	0	0	0	0

This report shows the date the scans were run, which system and application components were scanned, the LPAR the scan was run on and whether or not any changes were detected.

Effort Savings

The outsourcer indicated that this solution saved one FTE (full time equivalent) of effort, improved the accuracy of the detection and, most importantly, improved the PCI compliance audit scores.

In addition, the advanced forensics contained within FIM+ enabled rapid investigation and resolution for all detected change incidents.