MainTegrity FIM+ Base Package

MainTegrity FIM+® Base Package provides a full function File Integrity Monitoring and system recovery solution. It runs completely on z/OS and requires no other hardware or software. FIM+ supports both z/OS and USS file systems. FIM+ Base provides the protection and compliance required to meet many of today's security standards.

The MainTegrity FIM+ Base Package includes:

- **FIM+ Server, FIM+ Agent, FIM+ Secure Vault -** FIM+ scans and creates a unique hash tag of a fully tested and approved version of a component, capturing available creation/change meta data and storing this information in a secure repository called the Trust Vault. Periodically or on demand, scans are run on the production component in use and the same information is gathered. These new hash tags are then compared to the trusted version in the vault. If the keys match this means components have not been altered and the trusted state is verified. If a difference is detected, real-time alerts are generated and sent to a client-defined response team for corrective action.

- **Browser Interface –** FIM+ provides a z/OS native browser that helps reduce and eliminate redundant administration effort by providing an easy-to-use GUI style interface that enables even less experienced staff to take the right actions quickly. FIM+ also provides full function 3270 "green screen" interface preferred by more experienced support staff.

- **ISPF, Batch and REST API Interfaces –** FIM+ provides a full configuration and operational interface in ISPF. All functionality is also provided in a batch utility as well as a set of REST API. This allows easy tie in with site tools and processes used for scheduling and automation.

- **On Demand and Scheduled Scans –** Scanning can be performed either at client scheduled intervals or on-demand as a result of a programmatic or human request. Either method provides the capability to scan when required to ensure files remain in a correct trusted state.

- **Support for z/OS Datasets -** FIM+ works with PDS, PDS/E, Sequential and USS format datasets. Related datasets can be monitored as a group called a Resource Set to ensure all alerts go to the desired response team responsible for verifying the integrity of the entire group. By grouping this way, the response team can monitor, report, and take automated actions more easily.

- **Auto-Discovery –** FIM+ provides an Auto-Discovery feature that will identify key system and configuration datasets. Those datasets can be automatically included in scans. As system and configuration datasets change, FIM+ will automatically detect the changes and update the scanning accordingly. This saves administration effort and eliminates the possibility of missing key datasets in the scans.

- **Recovery Assist –** FIM+ can speed up recovery from malicious changes to the production environment. FIM+ is aware of what was changed, when it was changed and the userid responsible for the change. This allows the assist feature to build JCL from the correct backups to complete the system restore. If recovery to the trusted state is required after an alert, FIM+ can perform a surgical restore for only the compromised components, avoiding unnecessary regression. Recovery of damaged data files can be accomplished in parallel using conventional tools.

- **PCI, NIST, GDPR, SOX Compliance and Automated Audit Reports -** Compliance with international security standards, such as PCI DSS, NIST CSF, GDPR, Financial Services Cyber Resiliency Guideline, and many others, is also provided with the required reporting.