FIM+ Admin Savings
Operations, Recovery, Compliance Audit

Synopsis:

With greater demands and new regulations being imposed on a rapidly shrinking pool of experienced z/OS resources, the linear relationship between how you are currently supporting compliance and cybersecurity needs and the amount of effort you are expending must change.

MainTegrity FIM+ was created to break this conundrum by reducing the administrative burden, and associated cost, in every phase of operation - setup, detection, response, recovery, compliance and audit.

Savings on Ongoing Operations:

- Auto-Discovery allows FIM+ to learn your system's critical components, eliminating the manual setup effort, and continues to learn as changes occur, avoiding ongoing administrative effort. This means that as you add, change, or delete operating components support staff do not have to make manual updates to keep monitoring current.

- FIM+ is a learning system. False positives are not raised because FIM+ learns of expected changes via integration with your change control processes. Therefore, when an alert is raised by FIM+, it is an unexpected change and should be investigated. Other tools that look for suspicious activity, raise many false alerts since normal operations are hard to distinguish from malicious acts committed with legitimate, but stolen, credentials. Sites may reduce sensitivity to limit the numbers of false positives, but this results in the risk of malicious acts slipping through undetected.

Recovery in a Breach Situation:

- Reaction time is critical and knowledge is power. During the response phase the FIM+ forensics browser guides support staff through the investigative process. The interface gathers relevant information from SMF, ServiceNow, ITSM Helix and other tools in use at your site. It uses mainframe specific insight to guide the response process to improve precision while eliminating manual research and decision making. Further, with a simplified browser display, highly skilled senior staff can offload work to less experienced personnel making the right decisions, in a timely manner, based on all relevant information.

  With FIM+ in place you can:
  - Know every component that changed, and when. This will detect timebombs and back doors that have been implemented by perpetrators and is needed to invoke the required actions to restore your infrastructure in an automated fashion.
  - Identify the Userid(s) that made the malicious changes, so their privileges can be suspended before more damage occurs.
  - Quarantine compromised environments for later analysis without slowing down the restoration processes that get you back into normal operations quickly.

- FIM+ Restore Assist creates the required recovery steps eliminating the time-consuming process of identifying the components that must be restored and hand coding the JCL to return them to a trusted state. Additionally, FIM+ can now recommend the best snapset or Safe Guarded Copy that contains the most recent uncorrupted databases and active datasets. Using the insight that FIM+ has built up during the

preceding phases, time and effort are saved while ensuring that both data and system infrastructure can be restored in an integrated manner.

- There is a general misconception that recovering the data component after a breach will save your business and can be accomplished quickly. In reality, without the software infrastructure, recovery can take weeks and be a painful exercise. With FIM+ functionality in place, recovery time can be reduced from days to potentially hours.

Savings on Compliance:

Regarding compliance, the biggest labor saver involves having FIM+ flow all required information directly onto specifically designed audit reports. PCI, SOX, cyber resiliency, and other standards require that compliance be proven with stringent reporting. This is often labor intensive and error prone. By having FIM+ create the reports and email them directly to the right staff, significant savings can occur potentially resulting in reduced staffing requirements. The improved accuracy, consistent delivery, and ability to make auditors more self-sufficient reduce audit costs and associated time. Compliance scores are also often improved.

Savings in Audit:

Every compliance standard typically uses time-to-time audits as proof that processes are being followed. These can be time consuming and expensive and if non-compliance is found even more painful. They usually involve both management and security staff for extended periods of time. With a superior information base built by FIM+, automated reporting audits can be completed more quickly and provide additional time to be more focused on year over year improvements not errors.

The FIM+ forensics browser with its advanced knowledge and ease of use, can make auditors more self-sufficient saving even more time and cost.