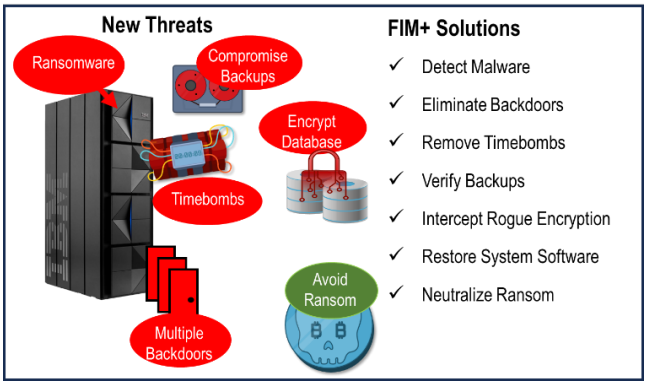
MainTegrity FIM+®

Fight Back Against Ransomware

In a constantly evolving threat landscape, MainTegrity FIM+® Early Warning (EW) provides a critical new layer of cyber security. This z/OS software can intercept malicious encryption activity in process, monitor suspicious user behavior and provide real-time corrective action. Combined with existing File Integrity Monitoring services, it creates a complete resiliency environment. In short, FIM+ puts you in control.

Complementing Enterprise Security Managers (ESMs) such as RACF®, ACF/2®, and Top Secret®, FIM+ enables mainframe and enterprise IT teams to ensure business-critical systems and applications are protected with the best-in-class detection, response, and recovery solutions.



External attackers steal credentials. Malicious insiders already have the access needed. Traditional tools that scan event logs, like SMF, find it difficult to distinguish between normal and malevolent activity. Often detection can take weeks or months, with response and containment taking even longer. FIM+ takes action immediately, resulting in faster, more precise detection and recovery.

Benefit from improved cyber resilience, reduced risk, and delivery of uninterrupted IT services.

Early Warning, A Technology Breakthrough:

In a revolutionary step forward for the IT industry, MainTegrity FIM+® EW can now detect and help neutralize the most common type of ransom attack, malicious encryption. Encryption can be valuable in defense against cyber-attacks on business data. However, it can be weaponized in the hands of unscrupulous criminals, disgruntled employees, or rogue state entities. FIM+ can now identify malicious encryption processes in their first seconds of operation. Legitimate encryption events are allowed to proceed, but those not recognized are immediately suspended. A real-time alert is sent to security staff which allows them to either resume the process from the point of suspension, or, if the encryption is of unknown origin, immediately initiate automated corrective actions.

In addition, Early Warning provides protection against other common attack vectors including mass deletes, data overwrites, suspicious user behavior, and much more. Rather than waiting hours or days for conventional tools to indicate a problem exists, customers can react immediately, limiting the damage done to sensitive data by orders of magnitude.

Zero Trust Foundational Elements:

With mainframes more powerful and prevalent than ever, supporting key sectors including banking and finance, utilities, healthcare, and government, FIM+ is a vital weapon in your company's arsenal in working toward a Zero Trust security posture. Specifically, MainTegrity FIM+ trusts no one and instead takes the approach that every system and application change must be verified to ensure that no malware has been imbedded. No other tool looks inside critical components to provide advance warning and surgical recovery of system components to prevent outages before damage occurs.

Continuous Cyber Security Monitoring:

FIM+ is a self-contained z/OS solution that requires no other hardware or software. FIM+ can quickly detect when files have deviated from their correct and trusted state. It learns about authorized changes as they are deployed, ensuring that unexpected changes raise an alert which is routed directly to designated response staff. Then, with a single click, FIM+ fetches the relevant SMF data, and displays it in its web interface to ensure attacks are stopped before major damage occurs.

MainTegrity FIM+®

Fight Back Against Ransomware

How MainTegrity FIM+ Works:

Was it approved? Because FIM+ learns about every approved change, it knows if anything is amiss. It can also integrate with ServiceNow or Remedy to open an incident, retrieve configuration info and even display the reason for the change.

Who did it? Since FIM+ knows when the problem started and exactly which components were affected, it can fetch the relevant SMF access records and identify the perpetrator. This can save countless hours of redundant searching.

Who needs to know? FIM+ sends real-time alerts via text or email to support staff, as well as updating tools like Splunk® or QRadar®.

How can we recover? FIM+ has a browser-based GUI with relevant security information displayed in one place. FIM+ selects the right components and creates the right restore jobs to ensure everything is returned to its trusted state.

The FIM+ Advantage:

Reduced time and effort - You are up and running in minutes with a familiar web interface, meaning new or inexperienced staff are productive (and can respond to issues) fast.

Internal threats - Staff sometimes go rogue. They have the credentials needed to attack. Only FIM+ can detect bad insiders changing the trusted state.

Learning on the job - FIM+ auto-discovery maps your systems and keeps things current by learning about desired changes as they are deployed.

Performance – By offloading hashing requests, FIM+ saves mainframe CPU cycles and reduces elapsed time.

Alerts - Sent by text or email to your response team and central tools like Splunk or QRadar.

MainTegrity FIM+ Enables You To:

- **Neutralize** insider and external threats: FIM+ catches intrusions that other tools miss.
- **Combat** ransomware and malware attacks to better protect your business.
- **Eliminate** false alarms while making genuine malicious attacks impossible to miss.
- **Comply** with data protection and security standards such as PCI DSS, NIST, HIPAA, and GDPR.
- **Simplify** audits by providing comprehensive reporting on components that are verified as being correct.
- **Respond** to attacks quickly and completely using GUI-driven forensics.
- **Enable** surgical recovery in the event of an attack using intuitive Recovery Assist.
- **Integrate** with immutable and conventional backup solutions.

About MainTegrity

MainTegrity Inc. is a world-class mainframe cyber resiliency company providing next-generation threat detection, advanced file integrity monitoring, automated forensics, and recovery solutions. Combining thoughtful leadership and advanced software, MainTegrity's team delivers solutions that work.

MainTegrity FIM+ saves time & effort, adding a critical layer of cyber resiliency for z/OS.