# MainTegrity CSF v3.2

**MainTegrity CSF** closes critical security gaps that have led to devastating cyberattacks and significant data loss on z/OS systems. As the leader in ransomware avoidance, CSF has been enhanced to provide immediate damage control and instant attack detection. CSF V3.2 now adds data exfiltration defenses and delivers a unified control in a crisis.

## New in v3.2

**Data Theft Protection:** Detect & stop data transfer to unknown IP address

Detect & halt data transfers exceeding thresholds (TSO & batch)

Alert on suspicious network traffic

Learn normal transfer behavior to reduce false positives

**Instant user lockout:** Revoke offending user IDs when compromised

**Tamper detection:** Flag use of AMASPZAP and VTOC manipulation

**Block dangerous commands:** Prevent malicious operator commands and privilege escalation before damage occurs

**Monitor reconnaissance:** Detects suspicious user activity before attack

**Enhanced Human Interface:** web-based interface for quicker investigation and customer specific recovery guidance

**Gather network statistics:** Discover mainframe network connections and monitor abnormal usage patterns

## Core Features

**Ransomware Avoidance:** Find malware/ransomware and restore integrity before an attack with FIM+

**No False Positives:** Learning system accurately identifies unauthorized changes without false alerts

**Continuous Detection:** Identify, intercept, and resolve many attack vectors not protected by z/OS

**Instant Damage Control:** Suspend attackers to stop damage, effectively reducing human reaction time

**Integrated Recovery:** Restore from conventional and immutable backups (Dell, IBM, Hitachi)

**Browser-Based Support GUI:** Intuitive UI allows faster reaction for both new and experienced support staff

**Audit reports:** Save time and effort with built-in automated reports

**Mass Deletes / Overwrites:** Monitor excessive deletion or updating of datasets and enable corrective actions

**Encryption Detection:** Real-time monitoring for malicious encryptions, a common attack vector

| Feature | MainTegrity CSF | Traditional Solutions |
|---|---|---|
| Malware/Ransomware Prevention (FIM+) | Yes | No |
| z/OS Authorization Tampering (Root Authority) | Yes | No |
| Privilege Escalation Detection (RACF, ACF2, TSS / SMF bypass) | Yes | Delayed |
| Immediate Suspend / Resume / Countermeasures | Yes | No |
| Real-Time Alerts with False Positive Elimination | Yes | Some |
| One-click Browser-Based GUI with integrated forensics | Yes | No |
| Integration with Immutable Backups, Recovery Plans | Yes | Manual |
| Network Data Flow and Behavior Monitoring | Yes | No |
| Immediate User Lockout | Immediate | Manual |
| Surgical System Recovery | Yes | Manual |
| Immutable + Conventional Backup Recovery | Yes | Partial or Manual |
| Compliance (NIST, DORA, Zero-Trust, ISO, etc.) | Yes | Limited |

Maintegrity inc.
Suite 1000, 888, 3rd Street SW
Calgary, AB, T2P 5C5, Canada

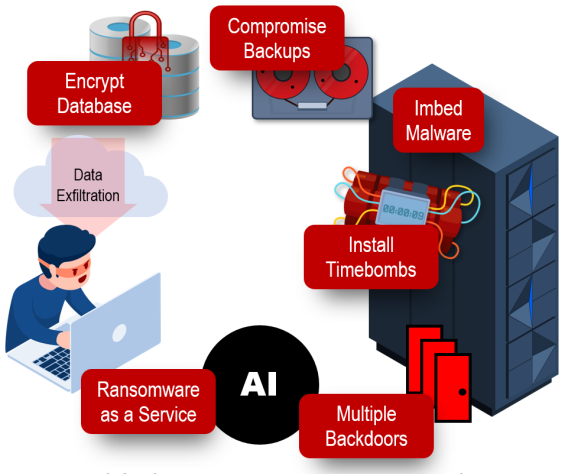
maintegrity.com
expert@maintegrity.com | +1 (720) 245-2246

# MainTegrity CSF v3.2

## Early Warning

The Early Warning system detects threats before damage happens by monitoring the system for signs of an attack

- Detects unusual access patterns, excessive reads, and privilege escalation attempts
- Flags unauthorized command usage and configuration probing
- Identifies attack planning behaviors like footprinting or user impersonation
- Triggers real-time alerts tied to specific recovery actions and playbooks




CSF defends against common ransomware attacks

## Operational Simplicity, Built for Action

MainTegrity CSF was designed for teams of any size and skill level. Get the insights, actions, and recovery you need without deep mainframe expertise

- Early Warning detects suspicious behavior before damage occurs
- Guided response shows staff exactly what changed, who did it, and how to recover
- Faster recovery with smart automation, built-in forensics, and the right backups pre-selected
- Fewer false alarms, less manual work, and easy integration with SIEM and ITSM tools

## The Leader in Ransomware Defense

**Was it approved?** FIM+ tracks every approved change and identifies malicious alterations.

**Who did it?** FIM+ knows when issues started and which components were affected, allowing it to select SMF records to identify the offender, saving hours of searching

**Who needs to know?** FIM+ sends real-time alerts to support staff via text or email, and updates tools like ServiceNow, Remedy, Splunk, QRadar and others

**How can we recover?** FIM+ provides a browser-based GUI that displays forensic information, selects the right components for recovery, and automatically creates restore jobs to return systems to their trusted state

## Compliance and Standards

MainTegrity CSF enhances compliance with international security standards, including NIST CSF, PCI DSS, DORA, ZeroTrust, ISO, HIPAA, and many others, providing the required reporting and audit capabilities.

## Enhanced Cyber-Resiliency

MainTegrity CSF excels in today's evolving threat landscape by preventing attacks and automating recovery. It introduces a critical new layer of security to z/OS, offering unmatched capabilities to protect, detect, respond, and recover. With instant detection, real-time alerts, and immediate suspension of malicious activities, CSF enables rapid human intervention and precise recovery, drastically reducing potential damage.

Maintegrity inc.
Suite 1000, 888, 3rd Street SW
Calgary, AB, T2P 5C5, Canada

maintegrity.com
expert@maintegrity.com | +1 (720) 245-2246