MAINTEGRITY

IBM Partner Plus

MainTegrity Cyber Security Framework (CSF) + IBM SGC

The industry's most complete mainframe cyber resilience solution.

Why IBM Safeguarded Copy?

IBM® Safeguarded Copy (SGC) creates immutable, point-in-time copies of critical data and isolates them from production—so organizations can safeguard information against user error, malicious changes, or ransomware and recover with confidence.

How CSF Supports SGC

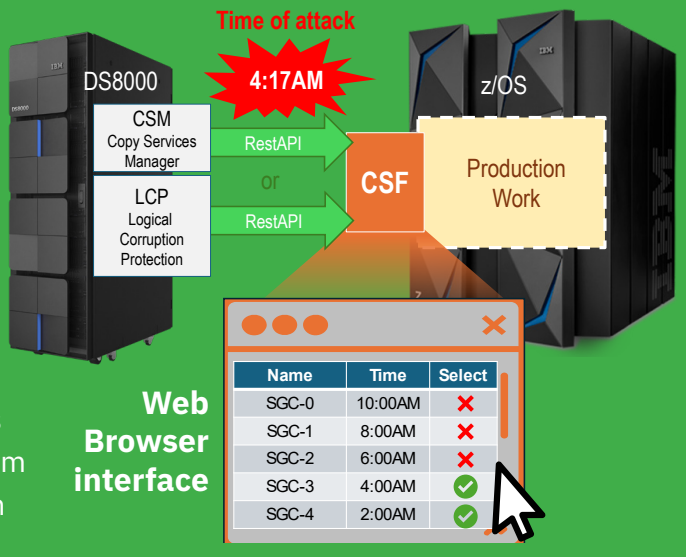
Building on SGC's strength, CSF connects directly to DS80xx storage via CSM or LCP, pinpointing the pre-attack SGCs needed for surgical data restore. In addition, CSF can monitor the creation of SGC backups and report any failures encountered.

CSF's Intelligent Browser-Based UI

CSF integrates directly with CSM (Copy Storage Manager) or LCP (Logical Corruption Protection) on DS8000 via RestAPI to find and display the list of available SGCs. **Since CSF knows the time of attack, it can identify the right SGC to recover your data using existing tools.**

Working in tandem, CSF automates the recovery of compromised system software. This ensures both system and data can be returned to their trusted state quickly and precisely.

Book an Expert



Web Browser interface

CSF automates selection of appropriate SGC backup(s)

CSF + SGC

SGC Capability	CSF Enhancement	Combined Benefit
Whole site backups	Identify what was compromised	Faster, more accurate recovery decisions
Immutable	Forensic timeline integration	Know exactly which SGC to use
Frequent snapshots	Continuous monitoring	Protection between backup windows
Multiple recovery points	Attack intelligence	Understand when/what must be recovered
Comprehensive recovery assets	Links to Copy Services Manager	Know when SGC creation succeeds/fails

How CSF Amplifies SGC Value

1. Improved Visibility

- GUI-based SGC viewer showing all available recovery points
- Visual timeline of SGC creation history
- Quick identification of optimal recovery points
- Simplified recovery initiation
- Optional integration with surgical recovery tools

2. Proactive Monitoring

- Automated SGC creation monitoring via DS8000 REST API
- Real-time alerts for failed or incomplete SGC creation
- Email/SMS notifications to support staff
- Complementary attack prevention

3. Surgical Recovery

- File Integrity Monitoring (FIM+) shows exactly what changed and when
- Forensic timeline correlates attack with SGC recovery points
- Trusted intelligence about which SGC predates compromise
- Recovery Assist automates system restoration while data recovery proceeds
- Verify integrity of system recovery

Unlike other mainframe products, CSF can:

- **Identify and eliminate malware/ransomware**
- **Detect and stop rogue encryptions instantly**
- **Freeze offending actors to mitigate damage and reduce human reaction time**
- **Send real-time alerts with automated actions to assist support staff**
- **Dynamic exfiltration intervention – prevent outage/damage**
- **Support recovery from Conventional & Immutable Backups**
- **Automate surgical restore of components to the trusted state**
- **Integrate with ServiceNow, Splunk, Rocket, Vertali, IBM, Dell, Hitachi, BMC**
- **Neutralize insider threats by monitoring suspicious actions**