FIM+ Augments SafeGuarded Copy

SafeGuarded Copy

IBM's SafeGuarded Copy (SGC) is a solution that creates point in time copies of data periodically. The solution operates at the storage complex level. This comprises a copy of the production data as it existed at the instant the SafeGuarded Copy (SGC) is taken. This backup copy is inaccessible from the production system thus providing immutability.

In the event of a cyberattack which includes data corruption, users will need to determine the latest SGC which predates the attack, stage the backup to available storage, then verify that the restored data is correct. This can be time consuming and error prone.

How FIM+ augments SafeGuarded Copy

FIM+ can access relevant information from the DS8000 Storage Director using a Restful-API. FIM+ will retrieve list of all SGCs and display them via the FIM+ Browser Interface. Previously there has been no good way for customers to see the available SGCs. Having a GUI-based view of this information makes recovery easier and faster. Since FIM+ also detects malicious activity, it provides relevant security information that can be used in a trusted data recovery incorporating immutable backup copies.

In addition, FIM+ has the capability to monitor the ongoing creation of SGCs. If an SGC was not created when expected, or encounters an error during creation, FIM+ can raise an alert and send it, via email or text, to the appropriate support staff. This provides a critical monitoring service for SCGs that is currently missing.

More Comprehensive Recovery

Bad actors are now patient, and frequently insert time bombs and additional back doors into your z/OS system well ahead of the primary attack. For this reason, it is likely that your software infrastructure will need to be restored to an earlier point in time than your application data.

The FIM+ recovery assist feature allows surgical recovery of compromised software components and verifies that they are the correct and trusted versions. Interoperating with the SGC restore for business data, FIM+ provides confidence that the recovery from a cyber incident is complete.

Preventing an attack

Immutable backups, by their nature do not prevent attacks. Out of the box, FIM+ will detect malicious activities that standard z/OS security tools often miss. FIM+ identifies changes made to the software infrastructure and raises real-time alerts when unexpected changes take place outside the normal deploy process. When an alert is received support staff can simply click on the imbedded link to start the FIM+ forensics browser. FIM+ gathers the relevant security information so that corrective action can be taken immediately.

Modern attacks often seek to corrupt backups and image copies to prevent recovery from the main attack. FIM+ monitors these datasets and if tampering is detected an alert is raised.
Improve cyber resiliency on your z platform with both SGC and FIM+. Not only will this provide state of the art useability, recoverability and detection, it will also reduce administrative effort while improving compliance with common security standards.

For more information visit our website today at maintegrity.com or email us at expert@maintegrity.com.

CONFIDENTIAL - CONTAINS TRADE SECRETS OF MAINTEGRITY