# FIM+ Leverages Dell Technologies SnapVx Snapsets to recover from Ransomware Attacks with Confidence

## Overview

Immutable snaps are highly efficient and useful for restoring mainframe data after a cyber attack. But, even after user data is restored, system and application software (infrastructure) that might have been corrupted needs to be inspected and restored to ensure the perpetrators cannot further destroy or ransom the system. Secondary attacks can only be eliminated by restoring both the correct data and trusted infrastructure components. Since modern attacks can take weeks to complete, it is likely that user data and software infrastructure will need to be restored to different points in time.

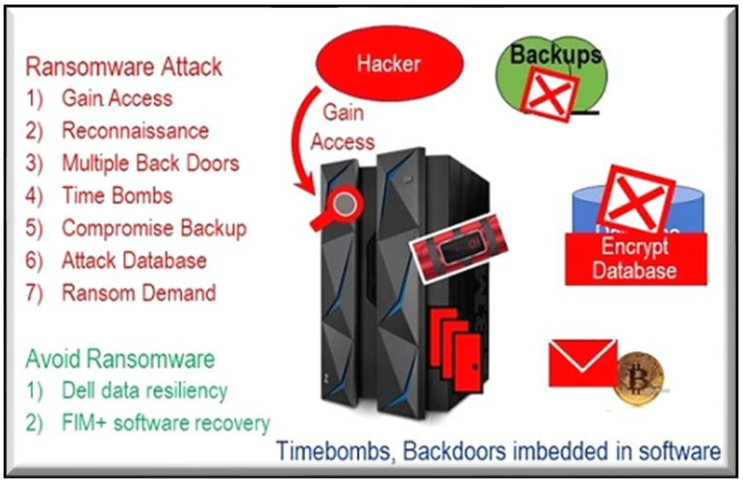
In cooperation with Dell Technologies, MainTegrity has implemented a snapset selection feature into its industry-leading file integrity monitoring product, FIM+. This feature corelates malicious attack detection information with the snapset creation records enabling users to easily select the correct snapset for restoration of the mainframe infrastructure as well as user data.

FIM+ Recovery Assist makes recovering the correct software infrastructure and the user data a straightforward process. Additionally, restoring only the components that were compromised avoids regressing desirable changes that were implemented in the attack interval.

## Restoring user data may not be sufficient

Snapsets are the best recovery asset in case of malicious attack. However, any restore process can be complex, requiring "trial and error" to find the correct snapset to restore from. Snapsets work well for highly active data, but, realistically, if your organization is unable to determine when the attack started and which portions of trusted system software or applications have been compromised, can you avoid repeat attacks.?

As an example, a malicious actor encrypts a DB2 or IMS database. The DB2 or IMS application would fail almost immediately. However, if only the database is restored from the latest snapset, the system may still be vulnerable to future attacks.




Why? Hackers are intelligent, well-funded and persistent. They typically start with an efficient phishing program or legitimate credentials purchased on the dark web. These credentials bypass even the best mainframe access controls enabling days or weeks of access before they are discovered. Internal to the organization, a disgruntled employee with proper access rights and malicious intent could be a longer-term threat.

Prolonged access makes full recovery more complex since bad actors not only have the time to find high-value targets to encrypt, they have time to obscure their entry point, destroy backups and implement multiple back doors and "time bombs". Recovery of the database (in the example) from the latest snapset may not restore the system components to the proper state. Fortunately, detection of malicious changes prior to encryption or destruction of user data is possible and must be a key element of your overall mainframe cyber-attack defense strategy.

## The solution: File Integrity Monitoring

FIM+ is the premier file integrity monitoring solution available for z/OS mainframes. Its primary mission is to detect unexpected and undesired changes to the mainframe's software infrastructure via an automated scanning process. It links together many other existing z/OS tools to provide a cohesive repository of shared intelligence, then makes that expert knowledge available in a z/OS native browser interface that is intuitive to both experienced and newer support staff.

It then uses that knowledge, combined with up to the second SMF data to recommend the Dell Technologies snapset(s) that should be restored. Because it leverages all relevant security information available in a z/OS environment, FIM+ does away with the need for multiple, time-consuming iterations of snapset selection and analysis to restore all system application and user data.

**FIM+ interoperates with:**

1. **ServiceNow, BMC Helix** for Problem / Change
2. **SPLUNK, QRadar, BMC AMI, other SIEMs**
3. **ISPW, Endevor, Changeman** for DevOps security
4. **RACF, TSS, ACF/2, firewalls** for perimeter security
5. **Dell / EMC zDP, VTL, DF/DSS, FDR** / storage tools

Concurrent with user and application data recovery, the compromised infrastructure components can also be restored to a point in time which eliminates all malicious changes that may have been introduced.

Using FIM+ in combination with Dell Technologies snapsets is faster and provides for a more surgical elimination of cyber intrusion than any conventional recovery processes.