MainTegrity FIM+®

Need to ensure your backups are not compromised? You actually need to prevent and verify!

Backup files are your most valuable assets in recovering from any ransomware or malicious attack. As such, attackers now typically compromise backups before launching their real attack on sensitive data, like databases. FIM+ Backup Verify identifies corrupted backups and image copies and can alert you to the problem before an attack occurs. FIM+ can be implemented in a few minutes with no system changes and little administration.

Ransomware and Internal attacks

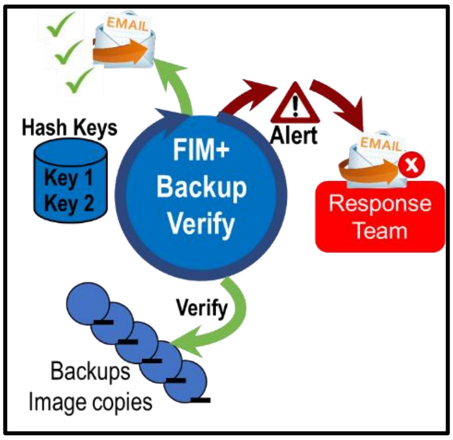
Whether state sponsored or independent, hackers are now persistent, intelligent and well-funded. In some parts of the world, cyber-attacks are a growth business. An efficient phishing program or buying legitimate credentials on the dark web will get hackers around access controls and onto your mainframe. Of course, disgruntled or desperate insiders can be an even bigger problem. They already have legitimate credentials and know what to attack. In either case, they often corrupt backups or image copies long before launching the real attack. By the time they encrypt your database, the bad actors may have been on your mainframe for days or weeks. Their mission is to ensure recovery is impossible. What are you to do?

Backup Verification

Once created, backups (DF/DSS, FDR, Db2 image copies, IMS and app backups) should never change. FIM+ Backup Verify creates a hash key from the contents of the datasets at creation capturing the trusted state. At regular intervals, the key can be recreated and compared. If they are the same, everything is fine. If they are different, the data has been altered and an alert is raised.

Efficiency

Backup and image copies can be very large, often running to several terabytes. To reduce overhead, processing is offloaded to the crypto cards now found on modern mainframes. This process provides 100% certainty that files have not been altered.



To further reduce resource consumption FIM+ provides super-fast sampling scans. Customers, in compliance with their own audit standards, can select a sampling rate from 1% to 100% which reduces the number of blocks to be processed, providing a proportionate saving in elapsed time, CPU time and I/O.

Continuous monitoring

However, it is far better to prevent the attack before assets are compromised. If a backup is opened (a sure sign of an attack) FIM+ will raise an alert. Further, backups should never be read except by an authorized (white listed) process or user. FIM+ detects this type of unexpected access. In some cases, JCL is modified so that the backup doesn't get created or writes no data. FIM+ also alerts you to backups not created on time or containing no data.

Forensics and Recovery

If, in some manner, files are corrupted, the FIM+ Incident Response tool will be of significant value, automatically gathering relevant security information and guiding the response team through required investigative steps and actions. This seamless process allows FIM+ to suggest customer specific actions necessary to recover infrastructure and suggest immutable or conventional sources for automated restore. Since FIM+ knows when things were last correct this process can be much faster and more reliable that the manual process it replaces.

Customers often say "I want to know if my backups have been compromised" but they what the really mean is "I want to be sure my backups can be trusted and that they have not been compromised". **BIG difference.**