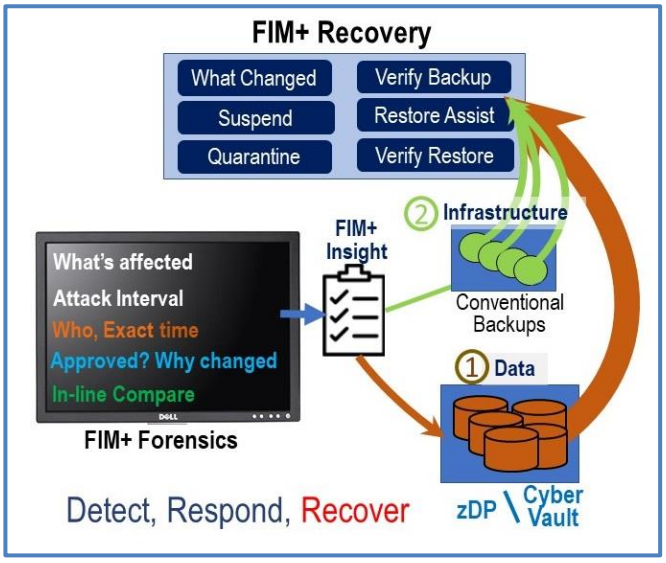
Case Study:
Worry-free integrity monitoring for Financial Services

Challenge: Improve Cyber Resiliency
A large Financial Services company needed to improve cyber resiliency on their mainframe systems. They knew immutable backups were highly useful for recovering active databases, but they worried that that they needed better detection and forensics processes to protect them from advanced persistent threats (APT) like ransomware. They also knew that compliance would need to be addressed. What were they to do?

Solution: SafeGuarded Copy plus MainTegrity® FIM+
Immutable backups are a superior recovery asset in case of malicious attack. The customer had already selected SafeGuarded Copy (SCG) as the best option for recovering large and highly active databases. However even when the data was recovered successfully, an exposure still be existed. What would stop the attackers from using the original or secondary access point to just encrypt the data all over again?

They were right. Modern attacks often include timebombs, multiple back doors, poison pills and other malware welded into the software infrastructure, prior to the primary attack. If they only restored their data they would still be exposed to a secondary attack.

Enter MainTegrity FIM+. This product augments the world's best access control and data recovery processes by allowing a selective recovery of infrastructure components that have been compromised. By using the mainframe's onboard hashing facilities, FIM+ could detect components that were changed in unexpected and unauthorized ways. Because perpetrators are now patient and knowledgeable, they frequently make malicious changes for weeks before the real attack.



To combat persistent threats FIM+ provides both a list of the components affected and when they were known to be correct. Armed with this tampering insight, FIM+ builds the required restore steps to get the infrastructure back to its trusted state and focus the data restore on an immutable backup that is recent AND uncompromised.

1. Recover data from immutable backup
2. Selective infrastructure restores from conventional backup

The Result: Now the customer has real resiliency from ransomware and other malicious attacks. They are able to overcome the root cause, malware in the infrastructure, and can restore their data concurrently, to get back on the air quickly.

Advanced Detection: Most security tools look for suspicious activity so require manual effort to confirm whether the alert is real or false. FIM+ detects only actual content changes, learns about expected changes automatically so is then not subject to false positives. This means when there is an alert it is a real problem. Further the FIM+ forensics browser fetches relevant information from other sources to automate the investigative process, saving precious time during a crisis. Combined with advanced early warning FIM+ may prevent the ransomware attack.

Compliance: The customer also found that FIM+ could help with PCI/DSS compliance. Sections 10.5 (integrity monitoring) and 11.5 (log verification) were met with existing FIM+ services. By using the advanced reporting effort could be reduced substantially. The same applies to SOX, NIST, cyber resiliency and other standards.

With FIM+ in place this financial giant can focus on the business not fighting cyber fires.