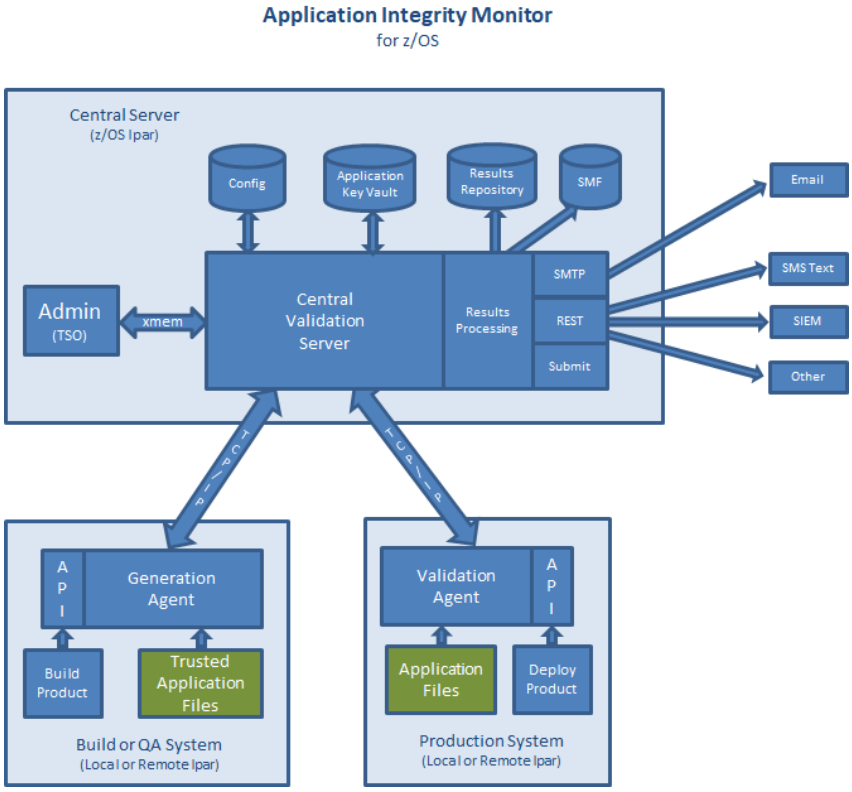
How it Works

The MainTegrity software product provides File Integrity Monitoring (FIM) and extended integrity monitoring (FIM+) for mainframe computers. By creating and matching secure keys for individual and groups of components such as executables, scripts, control members and other data MainTegrity can determine if critical information has been altered.



How it works: MainTegrity generates a unique TrustKey for each component (executables, html, panels, scripts, JCL, control members, log files, etc.), as well as creating a TrustKey for the entire group of components called an application. These keys are stored securely in a Vault. Later, using the same algorithms, production environments can be scanned at will and a new key built. By comparing the key stored in the vault with the new key MainTegrity can see if anything has been changed.

Creating a TrustKey: MainTegrity provides a generation process that creates a new TrustKey at a suitable control point in your application development process (for instance after QA testing has been completed and the application is at a trusted level) but before they are rolled out into production.

Validations: Performed on demand, on a schedule, or randomly, validations can be performed in seconds according to their policy. Results of each scan are then compared with known releases (past, present and sometimes future). If the keys match the desired release an all clear is logged. If not an alarm status is raised. All alerts can be delivered directly via email or SMS text to specific staff. In addition, MainTegrity log records can be sent to an SIEM console (such as Splunk). In this manner both all clear and alarm records can be correlated with other event other data to provide valuable insight into when a problem was introduced.

Authorized Changes: Your deploy process or approval tool (such as ServiceNow) can be queried by MainTegrity to see if the identified change is authorized. In this way MainTegrity can provide varying levels of alert on planned vs un-authorized changes. This makes MainTegrity is far less susceptible to false positives that plague conventional file integrity monitoring tools.

With the deployment of each new release, an immediate verification can be run to ensure that all elements arrived successfully. If MainTegrity detects a problem, a failure analysis will report the details and allow a quick response to any deployment issue. Since MainTegrity maintains a record of all software releases it can easily distinguish if an exception appears to be malicious (red flag) or simply an update in error (yellow flag) where the components are recognized but at the wrong level. As a vital part of your deployment process, MainTegrity can validate a successful implementation rather than conventional FIM which only identifies if something has changed.

FIM+: By managing entire application groups instead of just individual files MainTegrity can be used to identify missing files, additional components, prior releases or modified files. Typically, all components are scanned using a quick comparison process, ensuring that overhead is minimized and allowing scans with far greater frequency. If a key mismatch is detected, the keys at the individual component level can be interrogated, quickly identifying the compromised component. If further analysis is desired, a full scan examining the components bit by bit can be automatically invoked. In this way, MainTegrity provides the optimal blend of performance and granular analysis while delivering complete application scrutiny.

MainTegrity gives you a black and white yes/no answer to the question “Are we exposed?” in a way other tools simply cannot. Ultimately customers get “right now” peace of mind and improved incident response. Coupled with reliable compliance information MainTegrity provides a new level of security, faster recovery times and simplified system audits.