FILE INTEGRITY ASSURANCE

SOLUTION BRIEF

virsec®

Application File Systems Are Under Siege

Virsec Security Platform (VSP) detects changes to application file systems and libraries to ensure the integrity of your most valued applications. VSP delivers unique capabilities that protect the full application stack at the web, memory, and host layers, detecting and stopping exploits at the first step before damage is done.

File integrity assurance is essential for complete application security. With ransomware, remote code execution and other advanced attacks continuing to grow, security teams must be proactive in curtailing malicious efforts to highjack, encrypt or leverage critical system files. Without Virsec protection, these assets can be commandeered or rendered useless when not continuously monitored during runtime.

Attackers accessing your application environment can take unnoticed steps to corrupt critical resources, tamper with application binaries, change configuration files, inject libraries, or change data files, all while maintaining anonymity by editing or deleting logs. The faster you can detect unauthorized attacks affecting files and file systems, the faster you can take action to prevent critical assets from being altered, seized, replaced or erased.

Virsec Guards Critical File Systems

VSP File System Monitoring capabilities help maintain the veracity of critical applications at the file level. VSP profiles and creates an AppMap™ of the entire application file system, capturing information about each relevant file, library and process, and then continuously monitors whether any files have been tampered with or corrupted during runtime.

VSP tracks all activity on critical files including directories, executables, scripts, configuration files, content files, and logs used within the application instance. When unauthorized changes to any file attribute occurs, VSP generates alerts and takes protection actions within milliseconds, such as quarantining suspicious files and restoring originals.

VSP Profiles and Monitors Critical Files Including

- Core Attributes
- Credentials
- Privileges & Security Settings
- Content
- Hash Values
- Configuration Values
- File Size
- Directory Structure
- Meta Data
- Libraries
- OS and File System Type

Stops Library Injections

VSP knows ahead of time which libraries should get loaded whenever the protected application spawns a process. It effectively detects library injections or code not part of either an executable or any of its dependent libraries, in process memory at runtime. Upon detection of such an attack method, VSP can instantly execute protective actions such as un-injecting the illicit library.

Deterministic Approach

VSP operates at the OS kernel level to identify illicit modifications as they occur. The AppMap baselines the file system and individual file components when applications are provisioned by VSP. Details of the AppMap are stored in the VSP database as cryptographic hashes that cannot be edited, deleted, or altered. If a difference is detected between the current state and baseline, predefined response actions can automatically execute in milliseconds. Monitoring can be performed continuously in real-time or at pre-defined polling intervals.

Virsec delivers unrivaled visibility and accuracy, with extensive, actionable forensics including the precise time, threat ID, affected files & resources, victim & attackers IP addresses, as well as the complete attack payload to prevent future attacks.