A file integrity scanner, also known as a File Integrity Monitoring (FIM) tool, verifies the integrity of files by comparing them against a known baseline or previously stored checksum. This process helps detect unauthorized modifications or tampering with files, which could indicate malware or other malicious activity.

How it works:

1. **1. Baseline Creation:**

A file integrity scanner first creates a baseline, which is a record of the initial state of the files being monitored. This baseline typically includes checksums (like SHA-256 hashes) of the files.

2. **2. Monitoring:**

The scanner periodically or continuously monitors the files, calculating new checksums for each file.

3. **3. Comparison:**

The current checksums are compared against the baseline checksums. If any discrepancies are found, it indicates a change in the file's content, permissions, or other attributes.

4. **4. Alerting:**

Upon detecting a change, the scanner generates an alert to notify administrators or security teams about the potential security breach or unauthorized activity.

Key features and benefits of file integrity monitoring:

- **Detects unauthorized changes:**

FIM is crucial for identifying malware, ransomware, and other malicious software that modifies system or application files.

- **Ensures data integrity:**

By verifying file integrity, FIM helps maintain the accuracy and reliability of critical data and system files.

- **Enables rapid response:**

Early detection of file modifications allows for prompt investigation and mitigation of potential threats, minimizing damage.

- **Supports compliance requirements:**

Many regulatory frameworks, such as PCI DSS, mandate file integrity monitoring for sensitive data.

Examples of FIM tools:

- **Achiefs/fim:** A file integrity monitoring tool built with Rust.
- **SolarWinds Security Event Manager:** A comprehensive solution for file integrity monitoring and security information and event management (SIEM).
- **Windows System File Checker (SFC):** A built-in tool for verifying and repairing critical Windows system files.

In essence, file integrity scanners are a vital component of a robust security strategy, helping to protect systems and data from unauthorized modifications and potential security breaches.