WHITE PAPER

Real-Time File and Application Integrity Monitoring for the Modern Enterprise

Serpentua Security Agent · 2026

Deploy a lightweight agent on any platform, monitor critical files and application binaries in real time, and detect unauthorized changes before they become incidents.

Executive Summary

Unauthorized file modifications, tampered application binaries, and altered configuration files are among the most dangerous and difficult-to-detect security threats facing organizations today. Whether the result of a supply chain compromise, insider threat, or external attacker with foothold access, changes to critical files often go unnoticed until significant damage has been done.

The Serpentua Security Agent is a lightweight, cross-platform add-on that provides continuous, real-time monitoring of files, application binaries, and system configurations. By computing and verifying cryptographic hashes of monitored assets, the agent detects unauthorized changes the moment they occur — triggering instant alerts and generating detailed audit trails for compliance and forensic use.

This white paper describes the Security Agent's architecture, capabilities, supported platforms, and the threat scenarios it is designed to address.

The Threat Landscape: Why File Integrity Monitoring Matters

Organizations invest heavily in perimeter security, endpoint detection, and network monitoring. Yet one of the most reliable indicators of compromise — changes to critical files and binaries — often goes unmonitored. File integrity monitoring (FIM) addresses this gap by providing a continuous, cryptographic record of the expected state of files and alerting when that state changes unexpectedly.

Supply Chain Attacks

High-profile supply chain attacks have demonstrated that even trusted software can be compromised at the source or during distribution. A Security Agent monitoring application binaries and shared libraries can detect when a file's cryptographic hash no longer matches its known-good baseline — a direct indicator of tampering, regardless of how it occurred.

Insider Threats

Malicious or negligent insiders with access to production systems may modify configuration files, scripts, or application components. Real-time FIM provides an immediate detection capability and a full audit trail linking changes to time and file identity — critical for investigations and compliance.

Post-Compromise Persistence

Attackers who have gained access to a system frequently modify files to establish persistence — installing backdoors, altering startup scripts, or replacing legitimate binaries with trojanized versions. File integrity monitoring is one of the most reliable methods for detecting these activities early.

Configuration Drift

Even without malicious intent, configuration files change over time through routine operations, updates, and human error. Unauthorized or undocumented configuration changes can introduce vulnerabilities, break compliance postures, and cause unpredictable system behavior. Continuous monitoring ensures that changes are always known, tracked, and auditable.

Agent Architecture

The Serpentua Security Agent is designed around three principles: minimal resource consumption, maximum detection reliability, and broad platform compatibility.

Lightweight Design

The agent is engineered to run alongside production workloads without impacting system performance. Low CPU utilization and efficient background operation mean the agent can be

deployed on production servers, endpoints, and embedded systems without performance trade-offs. It is built for always-on operation — continuous monitoring without scheduling gaps.

Cryptographic Hash Verification

The agent establishes a baseline of SHA-256 cryptographic hashes for all monitored files at deployment time. Continuous monitoring then compares live file hashes against this baseline. Any mismatch — whether caused by modification, replacement, or corruption — is immediately flagged. Because SHA-256 is cryptographically robust, even minor file changes produce a completely different hash, ensuring high detection sensitivity.

Real-Time Detection

Rather than relying solely on periodic scheduled scans, the Security Agent is designed for real-time detection of unauthorized changes. When a monitored file is modified, the change is detected and an alert is triggered immediately — minimizing the window between compromise and detection.

Centralized Dashboard

Agents across all monitored systems report to a centralized dashboard, providing unified visibility into the integrity status of the entire monitored estate. Security and operations teams can review active alerts, examine change histories, and track trends across systems from a single interface.

How It Works

The Security Agent is designed for rapid deployment. From installation to active monitoring typically takes minutes.

Step	Description
1. Install Agent	Deploy the lightweight agent on any supported platform — Linux, macOS, Windows, or BSD.
2. Monitor Files & Apps	Configure monitoring targets: application binaries, configuration files, scripts, shared libraries.
3. Detect Changes	The agent continuously verifies file hashes against the known-good baseline in real time.

4. Alert	Instant notifications are triggered on any integrity violation or unauthorized modification.
5. Report	Detailed audit trails and compliance reports are generated for every detected change.
6. Dashboard	Centralized visibility across all monitored systems via the Serpentua Cloud dashboard.

Application File Monitoring

The Security Agent extends file integrity monitoring beyond static data files to cover the full spectrum of application components. This is a critical distinction: many FIM solutions focus on configuration files and system directories but leave application binaries and shared libraries unmonitored — precisely the assets most valuable to an attacker.

Binary Monitoring

Application executables and binaries are primary targets for tampering. An attacker who replaces a legitimate binary with a trojanized version gains persistent, privileged access that survives reboots and updates. The Security Agent monitors application binaries continuously, alerting immediately if a binary's hash changes unexpectedly.

Configuration Tracking

Configuration files govern application behavior, access controls, network settings, and security policies. Unauthorized changes to these files can silently undermine security postures or introduce exploitable misconfigurations. The Security Agent tracks configuration files alongside binaries, providing a comprehensive integrity record.

Shared Library Monitoring

Shared libraries (.so, .dll, .dylib) are frequently targeted in sophisticated attacks because they are loaded by multiple processes and often have elevated trust. Monitoring shared libraries alongside the applications that depend on them closes a critical visibility gap in traditional FIM deployments.

Script and Cron Job Monitoring

Scheduled scripts and cron jobs represent another common persistence mechanism for attackers. The Security Agent monitors script files for modifications, ensuring that automated tasks run only the code that was authorized.

Cross-Platform Support

The Security Agent is built for the reality of heterogeneous enterprise infrastructure. A single, consistent monitoring capability is available across all major operating systems.

Platform	Support Details
Linux	Ubuntu, RHEL, CentOS, Debian, and all major distributions. Full agent support.
macOS	Native support for Apple Silicon and Intel architectures.
Windows	Windows 10, Windows 11, and Windows Server editions.
BSD	FreeBSD, OpenBSD, and NetBSD. Full agent support.

Cross-platform consistency means that security teams can apply uniform monitoring policies and reporting standards across the entire infrastructure, regardless of the operating systems in use.

Platform Features Summary

Feature	Description
Lightweight Agent	Low CPU and memory footprint; designed for always-on production deployment.
Real-Time FIM	Continuous hash verification with immediate detection of unauthorized changes.
Application Security	Monitors binaries, configs, shared libraries, and scripts — not just data files.

Change Audit Trail	Full audit history of every detected change for compliance and forensic use.
Instant Alerting	Notifications triggered immediately on integrity violations.
Centralized Dashboard	Unified visibility across all monitored systems via the Serpentua Cloud platform.
Compliance Reporting	Detailed reports suitable for audit, regulatory review, and incident response.
Cross-Platform	Linux, macOS, Windows, and BSD — consistent behavior across all platforms.

Key Use Cases

Production Server Hardening

Security teams can deploy the Security Agent on production servers to continuously monitor critical system files, application binaries, and configurations. Any unauthorized change — whether from an external attacker, an insider, or an unintended software update — is detected and alerted immediately.

Compliance and Regulatory Requirements

Many regulatory frameworks — including PCI DSS, HIPAA, SOC 2, and ISO 27001 — explicitly require file integrity monitoring as a security control. The Security Agent's continuous monitoring and detailed audit trails provide the evidence needed to demonstrate compliance with these requirements.

Supply Chain Integrity Verification

Organizations that distribute or deploy software can use the Security Agent to verify that deployed binaries match their expected cryptographic hashes — providing assurance that software has not been tampered with between build and deployment.

Incident Response and Forensics

When a security incident occurs, the Security Agent's change audit trail provides a chronological record of file modifications — a critical input for incident response teams investigating the scope, timeline, and mechanism of a compromise.

Development and CI/CD Pipeline Security

Development teams can use the Security Agent to monitor build artifacts, deployment packages, and pipeline configuration files, detecting unexpected modifications that could indicate a compromised build environment or supply chain injection.

Integration with the Serpentua Cloud Platform

The Security Agent is an add-on to the Serpentua Cloud Platform, extending its data validation capabilities into the domain of real-time security monitoring. Organizations already using the Serpentua Cloud Platform for scheduled file validation can add the Security Agent to gain continuous, real-time detection alongside their existing reporting and analytics infrastructure.

> *The Security Agent and Serpentua Cloud Platform share a unified dashboard, giving security and operations teams a single pane of glass for both scheduled validation and real-time integrity monitoring.*

Getting Started

The Serpentua Security Agent is available as an add-on to the Serpentua Cloud Platform. Contact the Serpentua team to discuss deployment options, licensing, and how the Security Agent fits into your existing security infrastructure.

> *Contact the Serpentua sales team at serpentua.com or view platform pricing at serpentua.com/products/cloud to get started.*

About Serpentua

Serpentua is an enterprise data validation and digital preservation company. Its product portfolio spans real-time security monitoring, scheduled cloud-based validation, and fully air-gapped

on-premises deployment — enabling organizations of all types to protect the integrity of their digital assets.

For more information, visit serpentua.com.