WHITE PAPER

Enterprise-Grade Data Validationfor the Modern Organization

Enterprise-Grade Data Validation for the Modern Organization

The Serpentua Cloud Platform · 2026

Serpentua combines lightweight local agents with powerful cloud analytics to deliver comprehensive data validation — without compromising security or performance.

Executive Summary

Organizations face mounting pressure to ensure the integrity, authenticity, and long-term preservation of their digital assets. Whether managing sensitive records, regulated data, or critical infrastructure files, the consequences of undetected data corruption or tampering can be severe.

The Serpentua Cloud Platform addresses this challenge with a hybrid architecture that keeps all file processing on-premise while delivering enterprise-grade analytics, monitoring, and reporting through a secure cloud layer. This white paper outlines the platform's architecture, key capabilities, security model, and deployment approach.

The Challenge: Data Integrity at Scale

Modern enterprises accumulate data at unprecedented rates across distributed systems, cloud environments, and edge infrastructure. Ensuring the integrity of this data — detecting corruption, unauthorized modification, or silent data rot — is a critical but often underserved operational need.

Traditional approaches to file validation are manual, fragmented, and difficult to scale. They typically require significant administrative overhead and offer little visibility into the health of data at rest across an organization's full infrastructure.

What organizations need is a solution that is:

- Automated — running continuously without manual intervention
- Privacy-preserving — ensuring sensitive files never leave the organization's infrastructure
- Cross-platform — deployable across heterogeneous operating systems and environments
- Centrally observable — providing a unified view across all nodes and systems

Platform Architecture

The Serpentua Cloud Platform is built on a two-tier hybrid model that separates sensitive data processing from cloud-based analytics and reporting.

Tier 1: Local Agent / Script

A lightweight agent or script is deployed directly on each system requiring validation. The agent is designed for minimal resource consumption — under 200MB installed size — and operates quietly in the background with a minimal footprint.

All file processing happens locally. Validation scans run on a configurable schedule, performing file integrity checks using cryptographic methods. Crucially, your files never leave your infrastructure. Only the validation results — checksums, status codes, and metadata — are transmitted to the Serpentua API.

Tier 2: Cloud Analytics & Reporting

Validation results are securely transmitted to Serpentua's cloud layer, where they are processed, analyzed, and made available through a real-time dashboard. The cloud layer provides historical analytics, trend reporting, anomaly detection, and automated alerting — all without ever receiving or storing your actual file contents.

How It Works: From Installation to Insights

Serpentua is designed for rapid deployment. The typical path from installation to actionable insights takes minutes, not days.

Step	Description
1. Install Agent	Deploy the lightweight Serpentua agent or script on any target system.
2. Validation Scans	Automated file integrity checks run on schedule — no manual triggering required.
3. Send to API	Validation results are securely transmitted to the Serpentua API using TLS 1.3.
4. Processing	Cloud-based analysis verifies results, identifies anomalies, and applies retention policies.
5. Reporting	Comprehensive reports are generated, with alerts triggered for detected issues.
6. Dashboard	Real-time monitoring and historical insights are available through the cloud dashboard.

Security Model

Security is foundational to the Serpentua platform, not an afterthought. The platform is built around three core security principles:

Privacy by Design

Files are never transmitted to Serpentua's infrastructure. The local agent performs all file-level operations on-premise, ensuring that sensitive or regulated data remains under the organization's complete control. Only validation results — cryptographic hashes and status metadata — are sent to the API.

Encrypted Communications

All communications between local agents and the Serpentua cloud API use TLS 1.3 encryption with certificate pinning, ensuring protection against interception and man-in-the-middle attacks. API key authentication provides an additional layer of access control.

Minimal Attack Surface

The agent's small footprint (under 200MB installed, under 100MB memory usage) reduces the potential attack surface. Background operation with minimal system interaction limits exposure to host-level risks.

Cross-Platform Support

Serpentua is built for the reality of enterprise infrastructure — heterogeneous, distributed, and constantly evolving. The platform supports all major operating systems:

Platform	Support Details
Ubuntu / Linux	Full agent and script support across all major distributions.
macOS	Native support for Apple Silicon and Intel architectures.
Windows	Compatible with Windows 10, Windows 11, and Server editions.
BSD	FreeBSD, OpenBSD, and NetBSD supported via script (agent coming soon).

Technical Specifications

Specification	Value
Agent Installed Size	< 300 MB
Memory Usage	< 500 MB
API Uptime SLA	99.99%
Supported File Formats	All file types

Concurrent Agents	Unlimited
Data Retention	Up to indefinite
Encryption	TLS 1.3 with certificate pinning
Authentication	API key authentication

Key Use Cases

Digital Records & Archive Integrity

Organizations managing large volumes of records — legal, financial, medical, or archival — can use Serpentua to continuously verify that stored files remain unaltered over time, meeting compliance and audit requirements.

Infrastructure & Configuration File Monitoring

IT and security teams can monitor the integrity of critical configuration files, scripts, and system artifacts across server infrastructure, receiving instant alerts if unexpected modifications are detected.

Regulated Industry Compliance

Industries subject to data integrity regulations — including healthcare, finance, and government — can leverage Serpentua's audit trail and reporting capabilities to demonstrate ongoing compliance with minimal operational overhead.

Digital Preservation

Libraries, museums, research institutions, and enterprises with long-horizon data preservation mandates can use Serpentua to detect and respond to data degradation, storage medium failures, and silent corruption before data is permanently lost.

Getting Started

Serpentua is available for deployment today. The platform is designed for rapid onboarding, with support available from Serpentua's team throughout the deployment process.

Ready to protect your data? View pricing at serpentua.com/pricing/cloudpricing or contact the Serpentua team to request a demonstration at serpentua.com.

About Serpentua

Serpentua is an enterprise data validation and digital preservation company. The Serpentua Cloud Platform is purpose-built to help organizations protect the integrity of their digital assets at scale — combining on-premise privacy with cloud-native observability.

For more information, visit serpentua.com or contact the Serpentua team directly.

