Actifile Data Security Platform Whitepaper

Email: info@actifile.com
Website: www.actifile.com
October 2022

WHITE PAPER: INTRODUCTION

The following document will describe Actifile security platform key principles, the platform operational model, and finally key capabilities

How are we different?

Actifile is a unique, comprehensive, and autonomous data security platform that is transforming how organizations secure their sensitive data. Unlike legacy DLP systems that are based on an event-driven approach and require extensive ongoing rules management built for LAN perimeters – Actifile is different. Actifile is based on analyzing data risks, and applying preemptive encryption that handles both external threats and insider carelessness, all in the world of no security perimeters. Moreover, Actifile's set and forget method, requires little to no maintenance, and can be up and running securing data, in less than 3 working days.

Key principles

Perimeter less world with hybrid cloud and on-prem usage

The local area networks and the notion of a security perimeter are no longer valid with the transition to hybrid cloud, work-from-home, and zero-trust architecture. In such a setup, sensitive files are spread across on-premise repositories (File Server, NAS) and different cloud-based repositories. These cloud-based repositories are divided between the ones that you manage (managed cloud, such as organizational OneDrive), shadow IT (such as communication apps like slack or WhatsApp), and 3rd party portals. Actifile provides an answer to this new data landscape with its cross-platform discovery functionality, coupled with the data flow monitoring capabilities.

Remediate Data Risk rather than handle files

Actifile provides a detailed breakdown of the data risk and leverages the data risk for data flow monitoring, auditing and remediation. This approach greatly simplifies the process.

actifile

Preemptive vs Reactive

Most DLP solutions try to prevent a data leakage event by blocking the exfiltration of the file. This approach has a couple of shortcomings:

- It does not help with an external threat, like ransomware stealing data;
- It requires an initial extensive effort of setting up all the blocking rules with ongoing maintenance.

Actifile's preemptive approach provides an answer for both shortcomings by encrypting files automatically.

How does it work?

Actifile is a cloud-based management platform coupled with a lean agent for workstations (both Windows and Mac), File Servers, NAS and Terminal Servers, and a sidecar docker instance for cloud-based file shares (. i.e., OneDrive).

Step 1: Data Risk Discovery and Quantification

Based on predefined privacy regulations and PII definitions, Actifile immediately starts scans for sensitive data using smart patterns. Actifile then quantifies data risk per PII type in local currencies (. i.e., US dollars).

Step 2: Data Risk Monitoring and Auditing

Tracks and audits data risk in real-time by continually monitoring incoming and outgoing sensitive data flows from and to the perimeter-less organization.

Step 3: Data Risk Remediation by Encryption

Our patented transparent encryption process automatically secures sensitive data across all endpoints, cloud apps, 3rd party portals, and shadow IT. The entire process, from initial deployment through data risk analysis to remediation by automatic encryption takes as little as 72 hours.

Actifile's solution not only preemptively encrypts sensitive private data in files, but it also transitions the data to safe harbor, per all privacy regulations requirements. Our solution helps organizations comply with all state, federal, and global data privacy regulations

actifile

What can Actifile do for you?

- **Sensitive File Discovery**

IT managers frequently have an incomplete picture of where sensitive data is dispersed - and who has access to it. Actifile locates and maps sensitive data across all your systems, devices, and the cloud.

- **Data Risk Quantification**

Actifile calculates the data risk per each and every PII type (such as SSN or PHI) by applying an algorithm that multiplies each and every PII record by its potential total damage, then aggregates that, across all the files and PII records of the organization. The aggregation is across file types, file locations, and different silos, to provide a complete data risk quantification. The quantification is always up to date, in real time.

- **Real-Time Data Flow Monitoring**

Actifile works silently in the background, monitoring real-time data flow across your entire IT ecosystem through user activities at the endpoints. This real-time monitoring shows how much data risk (presented in USD, alongside the number of the files and the records) is being exfiltrated outside the organization or imported into it. The monitoring capability does not require any type of integration to the sending or receiving application or website.

- **Full Audit and Indelible Log**

Actifile automatically logs all data-related events, including data ingress and egress and the creation of sensitive data. You can instantly audit back to specific dates, times, and locations. The log is never deleted, covering you in the event of a breach. You also have the option to generate alerts on specific events and to integrate the alerts to 3rd party systems, such as SOC or SIEM.

- **3rd Party Integration and Reporting**

3rd party event integration: Everything that Actifile captures can be seamlessly integrated into a third-party security central system (SOC or SIEM). Users can capture and correlate all events that happen within the organization.

- Online and offline reporting: Conveniently export system reports and analyses in PDF format and white label them as required.

- **Risk Remediation by Encryption**

- Automatic encryption is a fast and convenient remediation process that secures sensitive data across your entire IT ecosystem, including remote devices and the cloud. Even if data is stolen or misplaced, the AES 256 encryption mechanism Actifile uses prohibits bad actors from opening or using the file.

- **Invisible decryption** allows employees to automatically use encrypted files with no latency and without the need for a password. Your employees can work without disruption, but sensitive data remains useless to any hostile actor.

- Automatic decryption by channel enables users to automatically decrypt any encrypted file when it's attached to an application. Actifile easily meets the demands of modern high-tech working environments.

- **Delayed encryption** gives you the flexibility to balance security with the demands of daily workflows. You can create a pragmatic, tailored approach to the management of sensitive data.
-

ADVANTAGES OF ACTIFILE OVER OLD SCHOOL DLPs

Traditional DLPs (Data Loss Prevention) solutions are structured for the old web architecture and are essentially obsolete. Businesses that rely on high-maintenance DLPs are operating at a clear disadvantage. Companies are wasting valuable resources and risking financial penalties for data breaches with systems that are frequently doomed to failure. Old school DLPs are expensive, labor intensive, and require constant adaptation by data security experts.

Actifile offers the following key benefits over the current DLP systems:

1. Simple to use solution that requires no special expertise in data security or compliance. Every IT manager can quickly master Actifile.
2. Low maintenance cost: Actifile's preemptive approach, which leverages automatic encryption, is a set-and-forget solution that requires very low ongoing maintenance efforts.

3. Preemptive encryption versus an event-driven blocking approach results in more effective data security at a lower cost, while securing data against external threats and careless employees.
4. Business-oriented software design strikes a functional balance between usability and security in a risk-aware context. Users can focus on remediating the data risk based on actual financial liability and not focus on the number of files or records that are meaningless without the business context.
5. Transparent decryption: Encryption is the strongest security method to protect sensitive files. The challenge with encryption is striking a balance between security and usability: how do we encrypt files without changing how users work? Actifile transparent decryption enables users to open files in different locations without requiring a user/password for each action.
6. Patented delayed encryption gives organizations the flexibility to balance security and usability.
7. Unique monitoring tracks user-driven data flow activities at endpoints, to and from all destinations, and without integration. Actifile automatically calculates the potential data risk value in US dollars.