

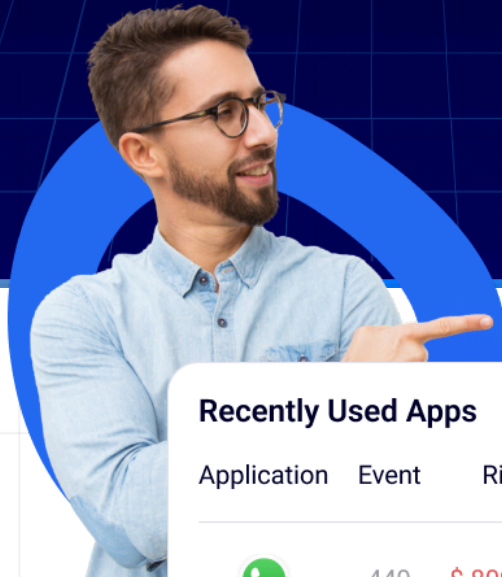


White Paper

Data Security Platform

Guy Bavly, CEO

August 2024



Recently Used Apps

Application	Event	Risk	Access to Encrypted Files
	449	\$ 809,143	Disable ☒ Enable



Executive Summary:

Why is Actifile the best security platform for the modern enterprise?

Organizations, as with anything else, are presented with new and evolving challenges with the passing of time. The latest challenge they face within a cloud based, post-COVID reality is how to protect their data when it is no longer kept within a perimeter and their employees are using and sharing data through hundreds of apps and platforms from as many locations.

Actifile was developed for this modern perimeter less workspace as a means to seamlessly encrypt and decrypt data based on value and risk, without interrupting workflow.

Why should you be worried about how you protect your and your clients' data?

There are two main reasons you should be worried: It comes down to cost of breaches and the inefficacy of legacy security solutions.

The average cost of a data breach to an organization is between \$4 million and \$9 million. The majority of organizations that experience a breach shutdown soon thereafter.

Additionally, legacy security solutions such as DLPs are not protecting the modern workspace. Rather, they merely attempt to chase down breaches for months after they occur.

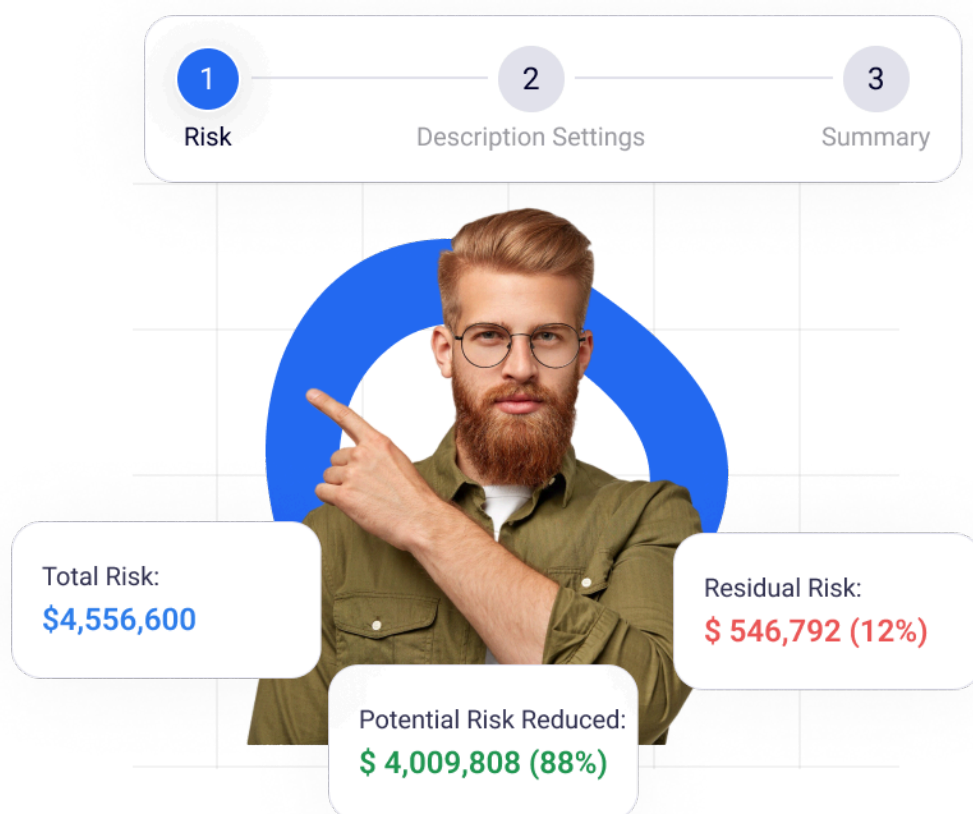
Actifile uniquely protects your data and ensures that even if a breach were to occur, the data is unreadable to the thief.



Why is knowing the data risk in \$ dollars the key to keeping your company safe?

One shocking aspect of modern data management is the lack of control organizations have over where their data is and who has access to it. Sensitive files, private customer information and trade secrets often float into and out of the organization with no controls placed on them.

Actifile not only locates all of this data, but its proprietary algorithm is able to classify it based on its value and sensitivity, then with one click allows the MSP or IT team to seal that data so that it is only accessible to those who need it. The dollar value our software places on data is directly tied to the value of stolen data as reported in thousands of historical breaches. Assessing a value is the surest way to identify where an organization is most vulnerable and protect it instantly on the spot.



The Actifile Difference

How are we different?

Actifile's patent-protected architecture allows Actifile to effectively mitigate risk by automatically cross-referencing data, events, and monetary risk, avoiding the need for heavy duty DLP implementation that requires extensive professional teams or, alternatively, cumbersome manual encryption/decryption mechanisms burdening workflow procedures.

By flipping the problem from event-driven workflow control to focusing on risk reduction (merging the data, the events, and risk to one easy-to-manage number) Actifile was able to remove the main obstacles that hinder other data security approaches:



1. Actifile's stated target is to reduce risk.

This allows Actifile to focus on the Top risks (80-90%) and either delay or avoid the hard-to-solve workflow data (the 10-20%). This approach is the exact opposite of DLP and Rights management which focus on the 10% of the data that is in the workflow.

2. Actifile focuses on keeping data in-house.

Thus, we are able to use a simple organization-wide key to encrypt data.

3. Actifile embraces simple controls and easy exception handling.

No control is perfect - and traditional handling of exceptions at SOC's costs resources. Actifile allows end users to control the data. The main control is Transparent Decryption using allowed whitelisted applications, and exceptions are handled using right-click decrypt (which decrypts for a set time, and then re-encrypts the data, and is limited in number of files per day). All usage and exceptions are logged.

4. Actifile avoids alerts and work by quantifying and prioritizing the risks (per time period) so that users (even MSP operators) can focus on quick ROI.

As an MSP put it - we converted the "alert monster" DLP approach to a "vulnerability assessment" style approach. Where the MSP/MSSP can review the system on a monthly/quarterly basis.

5. Actifile has built in classification.

It is lightweight enough to work on underpowered nodes. It is accurate so that false-positive and false-negative rates are low. Easy exception handling (see 3 above) means that occasional false-positive and false-negative aren't an issue.

6. Actifile supports multi-tenant and multi-tiered – modern IT which may include a mix of internal, MSP and MSSP service providers

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.

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.



Actifile at Work 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.

Actifile at Work for You

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.