Actifile

SECURING DATA USAGE ON ZERO TRUST DEVICES

Enabling employees, contractors and business partners,
to securely use corporate data taken from any application,
in a perimeter-less world

Challenge

In the age of cloud applications, no-perimeter security and zero-trust endpoints, users continue to take data out of applications you manage, like CRM or ERP, or applications that you do not manage such as government repositories. In both cases, the organization that is responsible for the data, lacks data visibility and control.

Solution

From securing any data taken from any application, to protecting any usage type like processing, storing and distributing the data from the endpoint, Actifile Guardrail delivers non-stop data protection at the endpoint and beyond.

Benefits

- Reducing liabilities outside your trusted apps
- Enabling secure and productive way of work for employees, subcontractors and business partners
- Does not require data security expertise to configure and maintain
- Can complement other solutions like DLP or RMS
-

As organizations move more applications to the cloud and employ remote workers and 3rd parties using zero trust devices, they lose data visibility and control outside the applications.
Actifile's unique low footprint technology enables employees, contractors and business partners, to securely use corporate data taken from any application or data source, whether or not the organization manages these applications.

The Challenge

The move to cloud applications and services has eliminated perimeter security that helped organizations control data. In addition, the explosive growth of the Gig Economy (the use of contingent workforce, 3rd parties and subcontractors) and the increase in remote work, have created more and more zero trust devices and BYOD, which are blind spots to current data control solutions. To secure data stored in the cloud, new products like CASB (Cloud Access Secure Broker) have been developed to enable control over application access and protect sensitive data when stored in the cloud. These products do not, however, cover users' growing need to retrieve, process, store locally and distribute data pulled out of cloud applications, as part of their normal work routines. Once data is retrieved, the cloud controls are not effective anymore, which in turn creates a gap in data governance. The challenge is even bigger when data is pulled from applications that are not managed by the organizations (such as government and service provider repositories). Organizations may remain fully liable for information extracted from some of these repositories.
Additional challenge stems from the need to strike the right balance between users' productivity and data privacy: corporate and zero trust devices contain a mixture of personal and organizational data that are hard to distinguish.

Actifile Guardrail Solution

Effective Approach to Protecting Data Outside Applications

Actifile addresses the challenge of securing data usage on zero trust devices by:

1. Measuring the liability associated with company data stored locally or transferred to external clouds or other users.
2. Transparently securing the company data when stored locally (for both transient or longer-term storage) or when transferred to untrusted clouds and/or recipients.
3. Providing liability reducing controls such as remote wipe to address excessive risk, lost endpoints and/or employee turnover.

Actifile's approach to securing data outside trusted applications has three pillars: Data Sources/Targets, Devices and Usage.

Source & Target Centric: The easiest way to protect data retrieved from applications, is to define the applications as the data sources and apply the appropriate controls *by default* to any retrieved data. In similar fashion, by defining the target applications as data targets, Actifile can control data flow to any target. Actifile supports both cloud-based and local applications and can protect data retrieved from sources such as: business apps, web portals, local apps, databases, code repositories and more. Actifile is focused on the data source, and is agnostic to the tool used to retrieve the data, for instance using Excel to retrieve customer data from Salesforce. Actifile does not require configuration on the application side and can thus support applications outside of the organization's control.

Given a user has access to an application, Actifile will handle any data retrieved from that app.

Usage Centric: to properly control data pulled from applications, requires supporting all potential user actions. Actions include data retrieval, with download, extract and copy & paste, data processing with merge or save as, data storage locally and data distribution (beyond the endpoint) to external repositories. Actifile's solution is file agnostic, and protects any files types, such as: standard office 365 and G Suite, all pictures format like PNG and JPEG, Drawings like Visio and Autodesk, etc.

Device Centric: The organizational supply chain today combines full time and part time employees, subcontractors and business partners. When coupled with the increase in remote work, and the desire to balance work and life, has resulted in the proliferation of mixed-use endpoints, with a mix of personal and corporate data. Actifile patented container-less data separation method, insures that your organizational data is protected on one hand, and users and other organizations privacy is not tempered.

Actifile Guardrail Solution Benefits

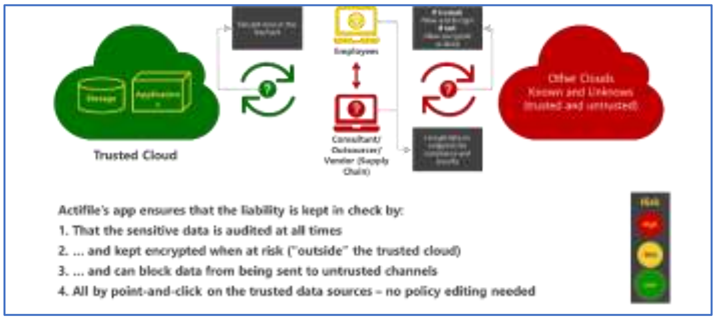
1. Reduces liability: Addresses the liabilities created by data that is outside trusted applications, in all transient states.
2. Helps leverage the gig-economy: Work securely and productively with all types of employees including those who work outside of the organization
3. Helps addresses the insider threats: Solve the problem of employee hoarding and carelessness.
4. Gain visibility: of your sensitive data, outside applications.

Actifile Guardrail Advantages

1. Zero Trust: Work in unmanaged endpoints outside your secured perimeter
2. Zero configuration: Just and click on data sources to discover and protect
3. Non-intrusive: Actifile has no effect on the corporate and users' way-of-doing-business. Users continue working with their favorite application, while Actifile Guardrail transparently works in the background.
4. Data and Application Agnostic: Works with any data taken from any application, cloud, on premise or local one.
5. Ownership requirements: Protects also data you are liable for but do not technically manage, such as government repositories or online financial services.
6. Easy to deploy and use: Does not require data security expertise to configure and maintain.
7. Independent of network services: Active Directory not required.
8. Supports offline mode: protection rules are persistent, even if the connection to the management module is disconnected.

How Actifile Guardrail Works

Actifile Guardrail is a lightweight application (<15 MB), is installed locally on the device (can be installed using automatic deployment tools) and managed using a cloud SaaS based module. Small footprint policies allow tether-less functionality (does not require directory integration), and SSO integration alleviates the need for policy writing. Actifile differentiates corporate data from other data, monitors select corporate data sources (cloud, intranet and applications) for sensitive data, tracks the sensitive data as it is used by different applications, uses an inheritance function to persist even when data is shared out-of-band. In addition, Actifile Guardrail uses transparent encryption, to secure the data without changing the way the users work with the data.



Actifile's app ensures that the liability is kept in check by:
1. That the sensitive data is audited at all times
2. ... and kept encrypted when at risk ("outside" the trusted cloud)
3. ... and can block data from being sent to untrusted channels
4. All by point-and-click on the trusted data sources – no policy editing needed

Figure 1 - Actifile Guardrail Data Protection Approach

Figure 2: Actifile in use: Point Actifile at the Trusted Sources and Applications

Figure 3 - Actifile Guardrail shows per device and cloud liability and whether it was remediated

Data Protection Methods Compared

	Actifile	RMS	DLP
Approach	• User retrieves any data • Actifile then transparently tracks and protects the data • Users continue to work as is	• Publishers must set file protection rules • Data user actions limited to pre–defined rules	• Organizations must pre-define permissible workflows • User may only work within these workflows
Security focus	Any transient phase between protected repositories	Sensitive assets that require distribution beyond the organization	Organizational workflows between predefined sources and targets
Addressing liability (due to corporate data at the EP)	Directly measures and remediates liability	Cannot measure the liability – only published files can protect their content	Can measure the liability at the endpoint and can be integrated with other solutions to provide remediation
Employee flexibility	High – any source, any use and any user, including 3rd parties	Low - restricted to the published files and their pre-defined limitations (hinders collaboration)	Low - Restricted to the workflows allowed by the DLP endpoint
Complexity	Simple deployment and automated source configuration	Simplest deployment, however requires complex policy maintenance by the publisher	Complex GRC process to measure and define the predefined workflows
External sources & Mixed-use	Supports both external sources of data (e.g. govt sites) as well as mixed use devices	External sources not supported (cannot wrap the download in RMS). Does support mixed use.	Does not support mixed-use scenarios.
Remediation persistency	Yes, files are encrypted at all times	Yes, files are encrypted at all times	Depends on the DLP configuration and its integrations

Table 1 - Actifile Approach vs. DLP and RMS Approaches

Actifile Guardrail is the Future of Data Protection

In the post perimeter security era, we are witnessing spectacular growth in the number zero trust devices on one hand, and in the variety and number of applications and data sources employees use. Current approaches, like DLP or RMS are not suitable for protecting data on zero trust devices and beyond, while balancing user productivity and data security.

Next Steps

Additional information can be found at www.actifile.com, or by emailing to info@actifile.com

About Actifile

Actifile is a data security innovative company, leading the category of data protection in a world of zero trust devices, no perimeter security and Gig Economy employees. Founded by group of industry veterans in the areas of GRC and DLP, Actifile believes that today's solution are not built for the next era of open, digital world. The company serves customers and partners worldwide.