Actifile

ACTIFILE GUARDRAIL

SECURING DATA USAGE ON ZERO TRUST DEVICES

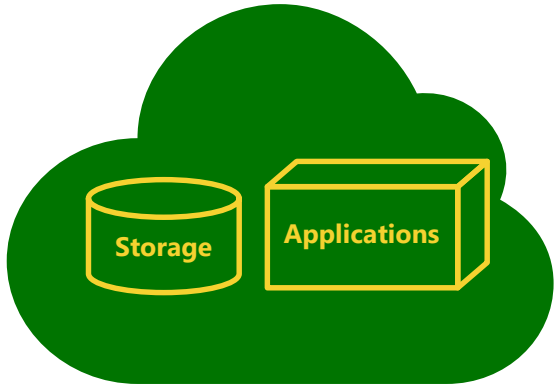
The challenge

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

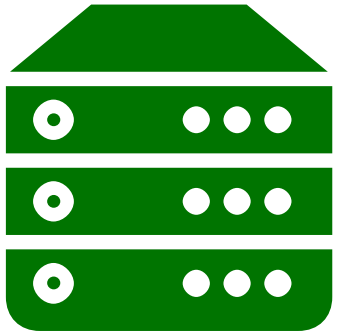
The solution

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.

Data is stored in secured data repositories

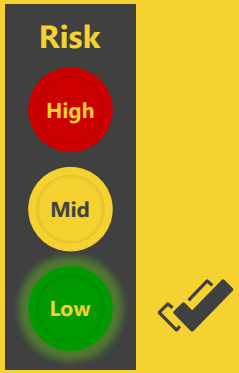


Trusted Cloud

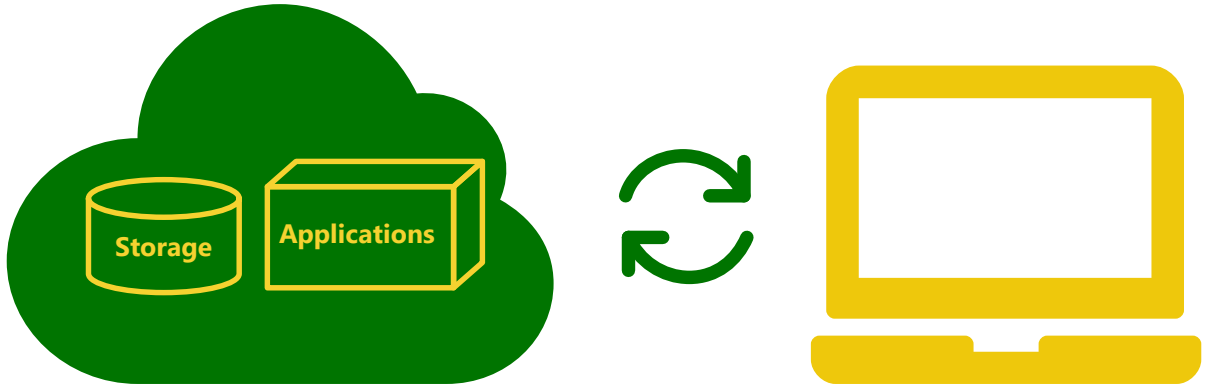


Local Data Store

- **Company stores data in cloud based repositories and applications, and on local servers.**
- **Visibility and organizational control over the data is high.**
- **Cloud vendors usually have best-in-breed data security solutions.**



Employees interact with the data



Trusted Cloud **Employees**

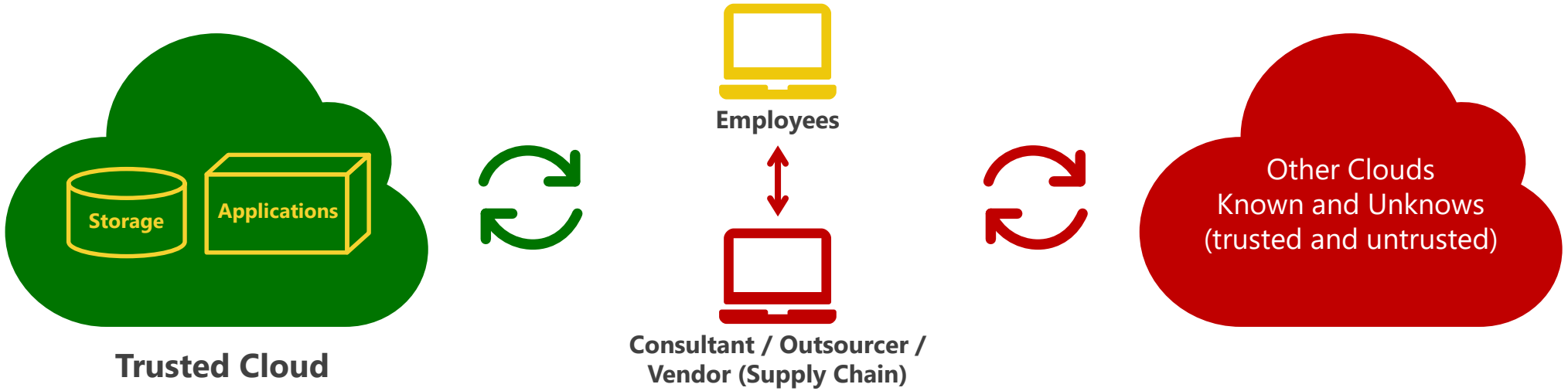
- **Employees access, download, process and upload/update data.**
- **Data accumulates on endpoint becoming an increasing liability over time.**
- **Visibility and control over the data is limited.**
- **As a result employee endpoints show up routinely on data breach “walls of shame”.**

Employees as a data “hub”

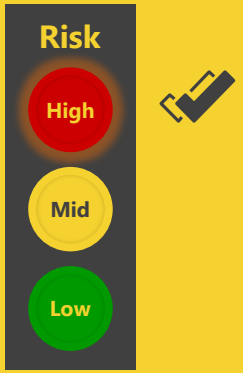
Trusted Cloud **Employees**

- **Employees routinely upload / download data from 3rd party cloud repositories and apps.**
- **As a result data liability accumulates at external clouds as well.**
- **Visibility and control over the data is limited.**
- **The liability due to a data breach increases as more data accumulates on the endpoint and clouds.**

The supply chain



- **Many companies give consultants, outsourcers and supply chain vendors access to sensitive information.**
- **Visibility is virtually non-existent for supply chain vendors.**
- **The liability due to a data breach increases as more data accumulates at the endpoints, clouds and external vendors.**



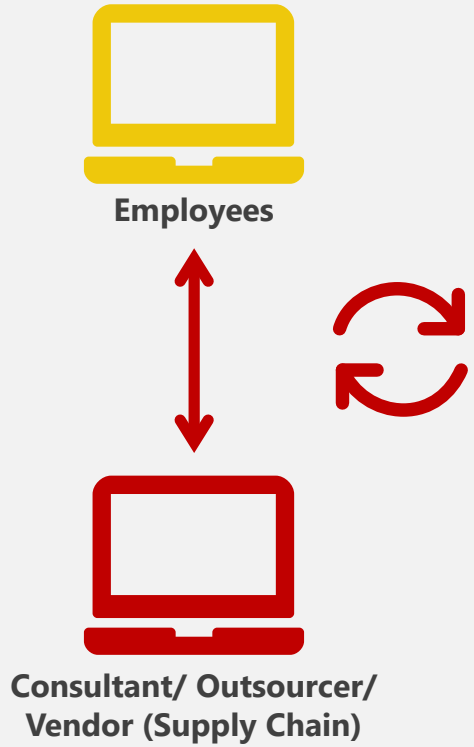
Data “hub” at the endpoint is **inevitable**

Driven by the need to process data for marketing, sales, regulatory filings, rendering of services, reporting, analysis.

Healthcare exposure:

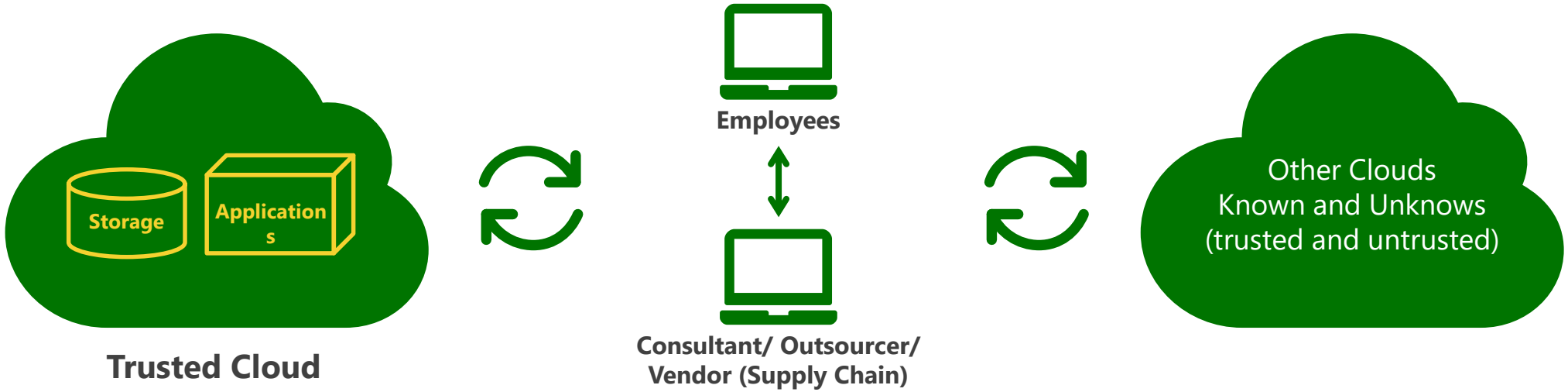
- **EMR, HIE, LIMS**
- **Payment systems, Medicare/Medicaid**
- **Government registries**
- **Doctors & nurses, consulting physicians**

Many systems a healthcare provider has to work with.

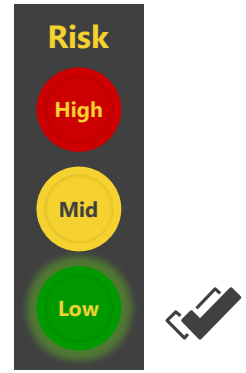


- Federal & State Regulators
- Suppliers
- Payment
- Medicare
- Consultants
- LIMS
- EMR
- Legal & Contracts
- Insurance
- Various Registries
- Accountant
- Pharma

What is needed?

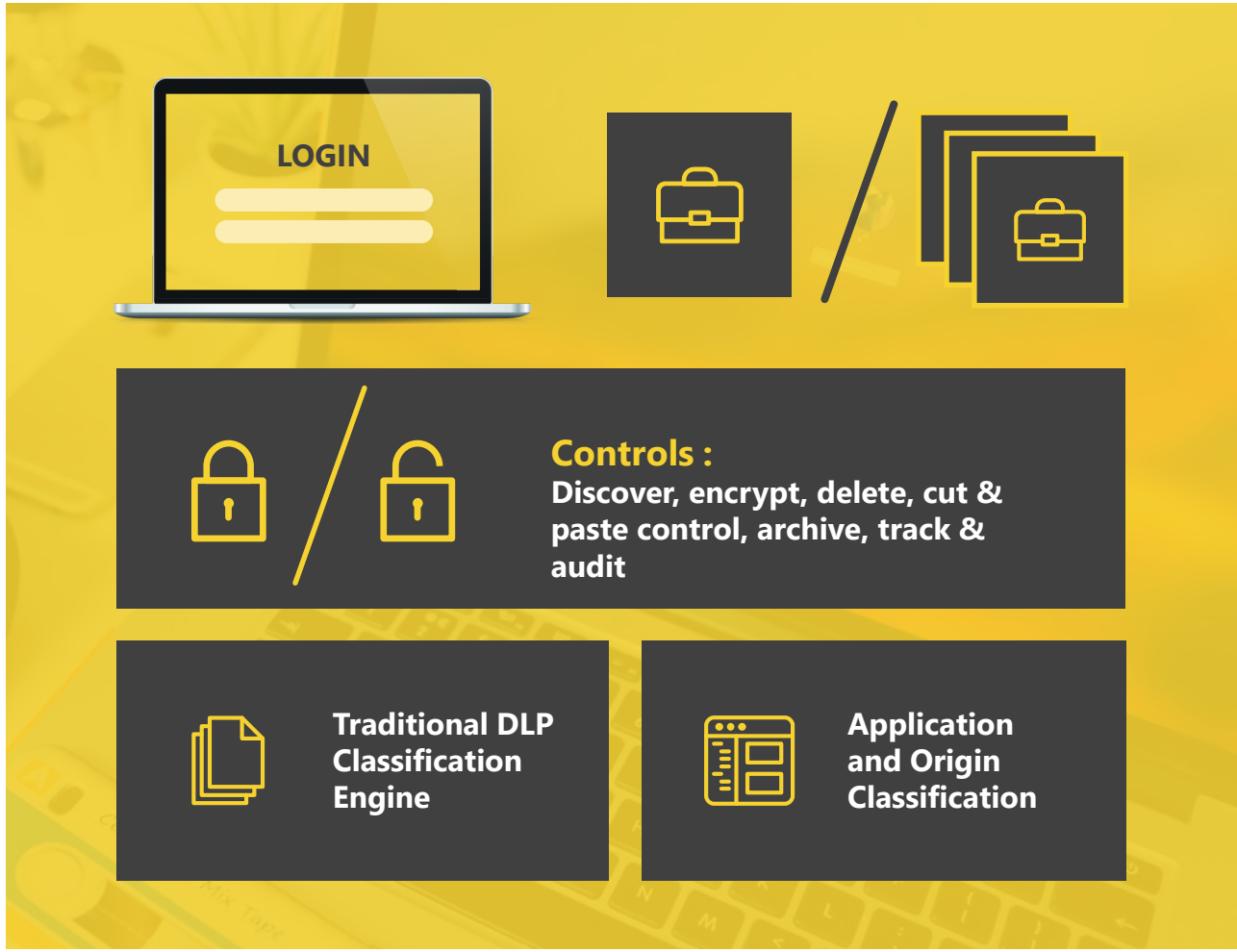


A solution that will (i) lower the risk of data breach occurring & (ii) **lower the liability** if a data breach occurs across **all** endpoints and clouds

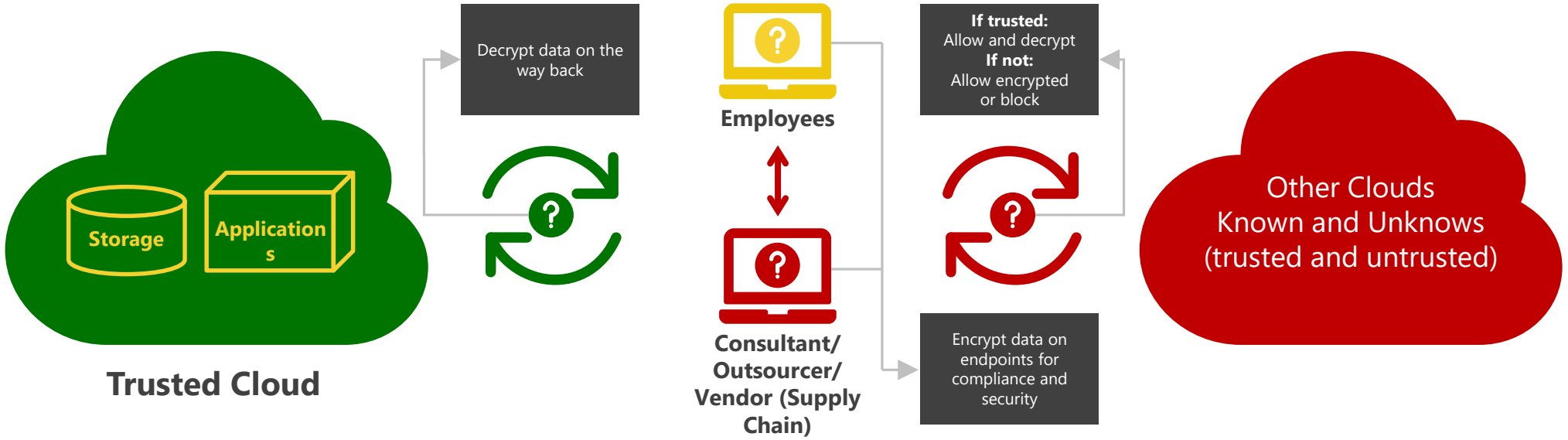


Actifile solution overview

- Leveraging 14 MB app for Container-less data separation and isolation
- Key data security capabilities: DLP, Transparent Encryption, Archiving and Discovery
- Central, Cloud based management, with one pane of glass
- For a mix of BYOD, CYOD, COPE & COBO across OS, and for any data source, any application and any file type
- User continuous and session based modes, for BYOD and COPE EP types

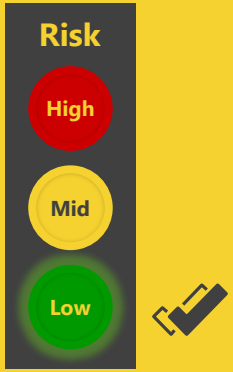


Actifile's solution

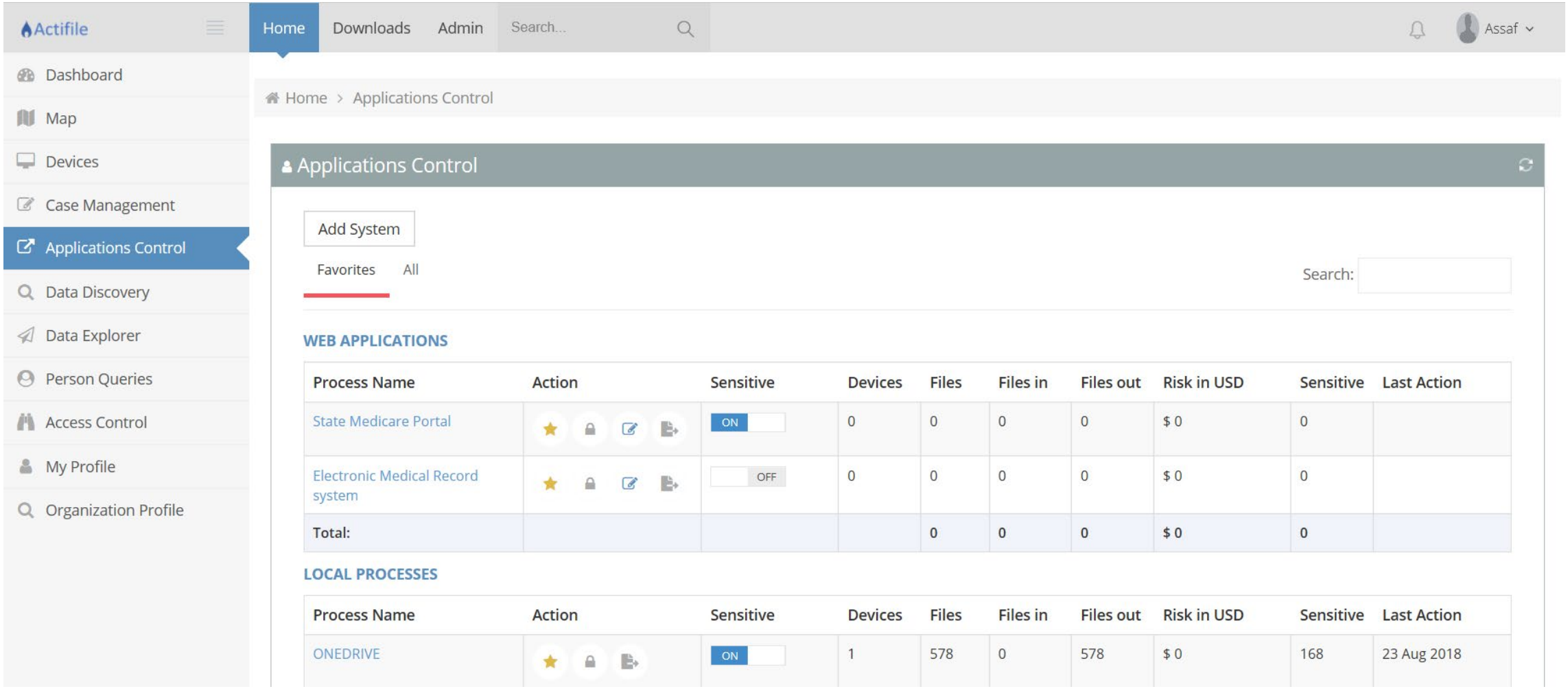


Actifile's app ensures that the liability is kept in check by:

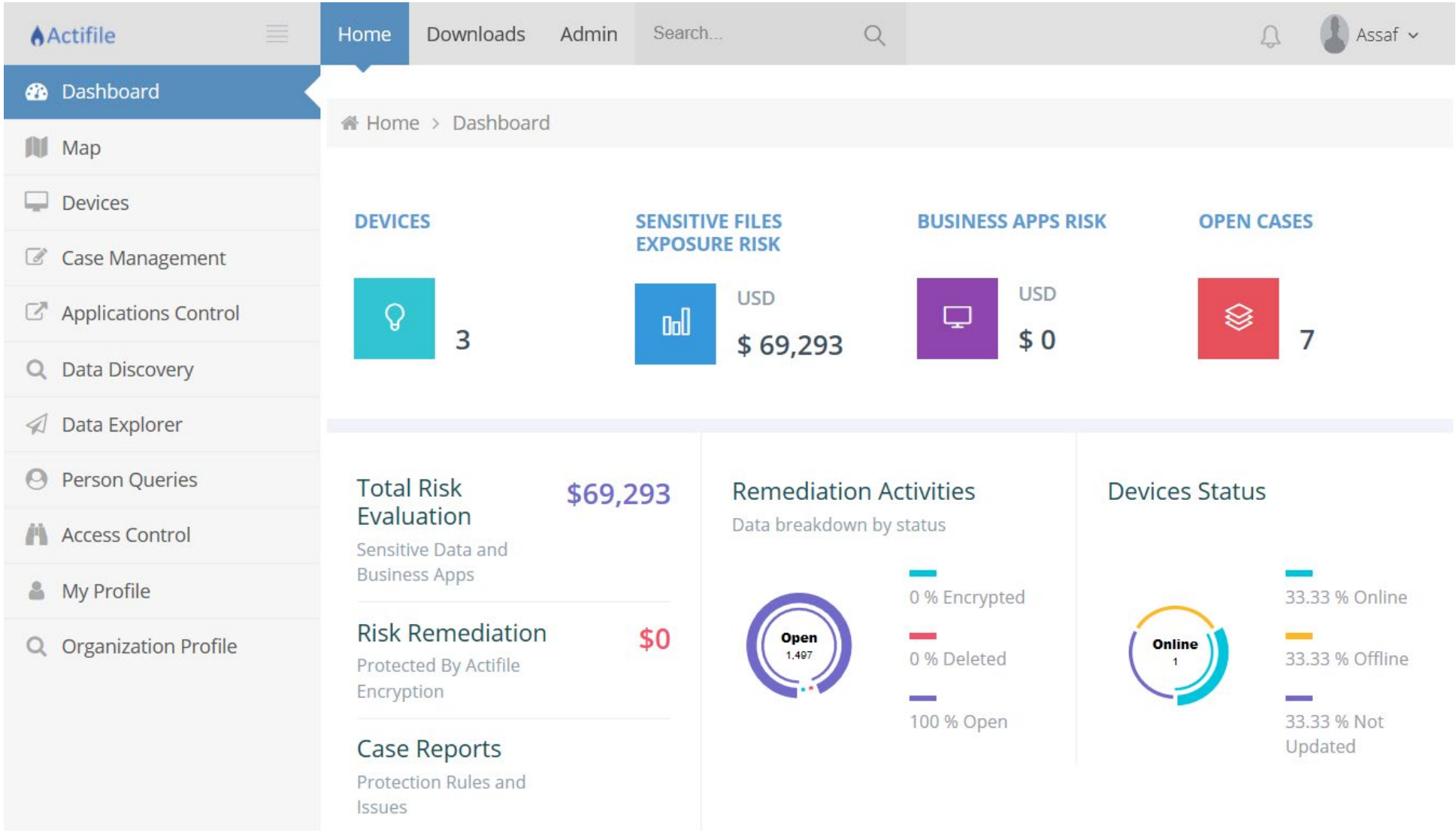
1. **That the sensitive data is audited at all times**
2. **… and kept encrypted when at risk ("outside" the trusted cloud)**
3. **… and can block data from being sent to untrusted channels**
4. **All by point-and-click on the trusted data sources – no policy editing needed**



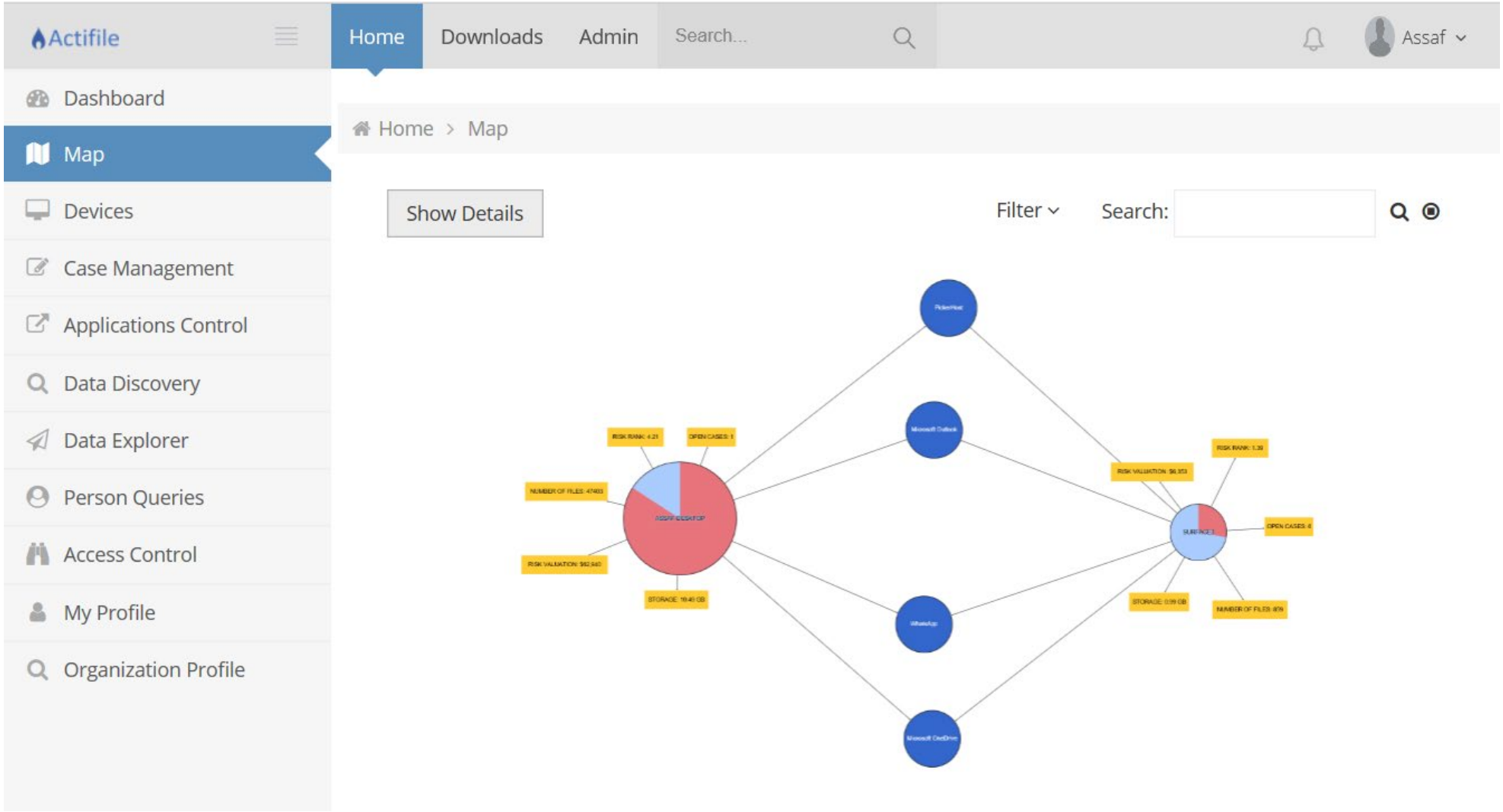
Actifile in use: Point Actifile at the Trusted Sources and Applications……



… and Actifile clearly shows overall organizational liability and remediation …



… and shows per device and cloud liability and whether it was remediated



Customers Sample Use Cases

- ✓ I would like to asses the level of liability/risk I have on my endpoints
- ✓ If one of my laptops is stolen, I need to know what data was on the laptop and make sure it is protected
- ✓ Can I make sure we only track and protect my organizational data and not employee / 3rd party data ?
- ✓ I need to make sure that the sensitive data at the endpoint is audited at all times, for compliance reasons
- ✓ I need to make sure that a terminated employee / discontinued 3rd party, has no longer my company's data on his endpoint

- ✓ I have 3rd party physicians downloading PHI data on their BYOD laptops
  - ✓ ..How do I know from which data sources?
  - ✓ How do I make sure the data on their laptops is monitored and archived?
  - ✓ How do I make sure they do not transfer it to non authorized targets?
  - ✓ Can I enable my 3rd parties to to transfer only to authorized targets?

Reduce liability w/data protection capabilities

- ✓ Protect by file types, such as: XLS, PPT, TXT, PNG, etc.
- ✓ Protect by local file shares: for instance, my documents
- ✓ Protect by remote file share on a windows file server
- ✓ Protect by cloud based file share, such as : Dropbox, Box, OneDrive, etc.
- ✓ Protect by web based application which is a data source
- ✓ Protect by locally installed application, such as: EMR, EHR
- ✓ Protect files by target: anything transferred to external repositories such as Dropbox or any web based portal
- ✓ Protect files with certain content, such as: social security number, passport number,
- ✓ Protect everything created while in login to the customers domain
- ✓ Share with externals in a secure way, leveraging any cloud based file share such as Box

Summary: Benefits

Reduces liability: Addresses the liabilities created by data that is outside your trusted apps

Helps leverage the gig-economy: Work securely and productively with users working outside of the organization

Helps address the insider threat: Helps address the issue of employee data hoarding and carelessness

Complements existing systems: Can complement other InfoSec systems, such as DLP

Summary: Advantages

Zero configuration: Just and click on data sources to discover and protect

Zero trust: Works in unmanaged endpoints outside your secured perimeter

Non-intrusive: Actifile has no effect on the corporate and users' way-of-doing-business

Data and application agnostic: Works with any data taken from any application

Easy to deploy and use: Does not require data security expertise to configure and maintain

Works independently of the network:No dependency on network services, such as Active Directory

Thank You

info@actifile.com

Actifile