LIVE RESULTS IN UNDER 30 MINUTES

# Breach Minimisation

**Traditional cybersecurity protects systems.**
**Breach Minimisation secures sensitive data.**

Reduce the impact of sensitive data exposure with minimal disruption to users, workflows or business operations. Designed for organisations without dedicated security teams, specialist compliance expertise or enterprise budgets. **See for yourself — test it below.**

## Deploy in three steps

≈ 5 minutes of hands-on time · full walkthrough follows

### 1 Create your account

Sign up in seconds **(no credit card required)**. Choose the portal that matches how you'll deploy:

Customer portal →  MSP portal (multi-tenant) →

### 2 Download the Sentry Agent

Log in to my.actifile.com and go to **Deployment → Device Setup → Installation**. Download the agent and copy your **Agent Key**.

### 3 Install on a test device

Run the installer on a workstation or server — about **2 minutes**. Actifile immediately starts discovering, classifying and quantifying sensitive data. No further configuration required.

**BEFORE YOU INSTALL**

Add Actifile to your AV / EDR allow list first — this is a critical step. Allow-list guide →

**DURING EVALUATION**

Do **not** enable encryption yet. Run in monitoring mode first and talk to us before encrypting any data.

**Ready in minutes. Let's review your results together.**

Actifile (Australia & New Zealand) · (02) 9151 7313 · support@actifile.com

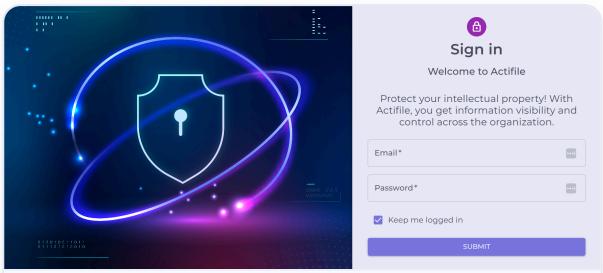
Book a results review →

THE FULL WALKTHROUGH

# Follow along, screen by screen

## 1 Log into your Actifile account

Sign in at **my.actifile.com** with your email and password.

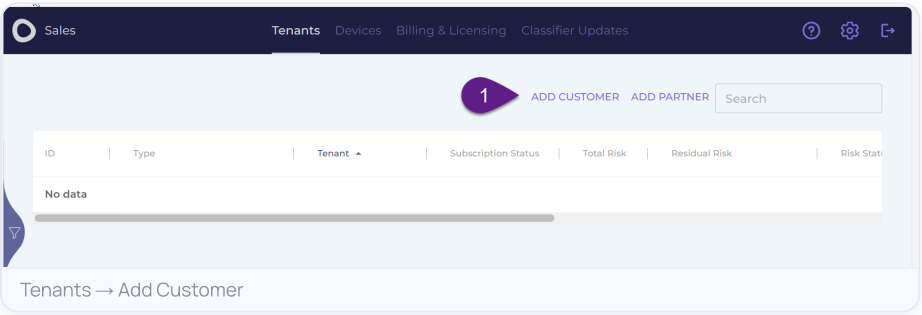



The Actifile sign-in screen

## 2 Add your company as the first customer

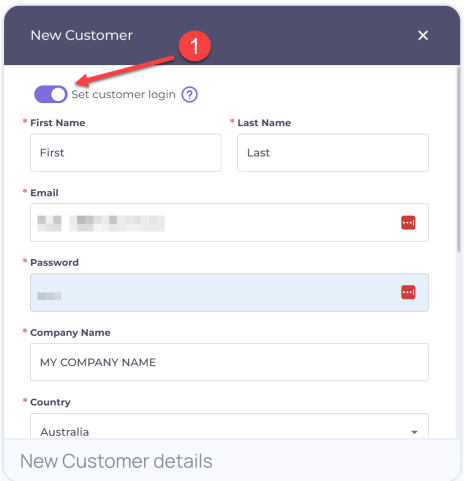
End clients log straight into their own account. MSPs create each client as a tenant. **Supported:** Windows, Mac and Linux PCs, laptops and servers — with options for SharePoint, OneDrive, M365 (beta), NAS and cloud (some may involve additional fees).

**A** From the **Tenants** screen.



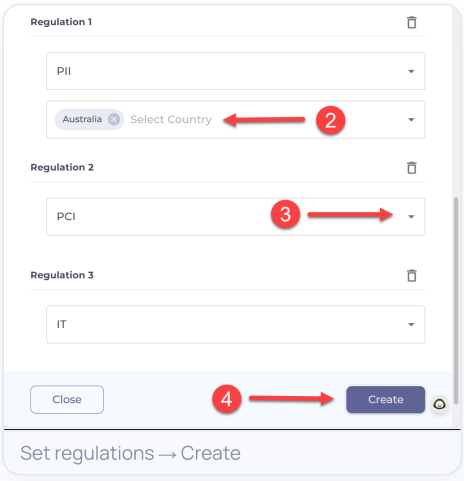

Tenants → Add Customer

**B** Turn on **Set customer login** — **no emails are sent**. Enter name, email, password, company and country.



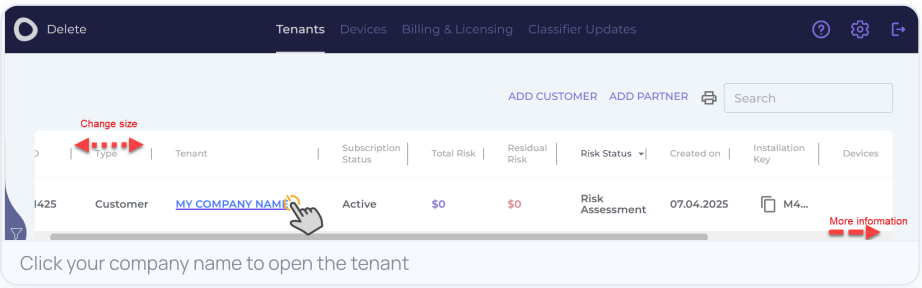

New Customer details

**C** Leave the default **regulated classifications** (changeable later). Click **Create**.




Set regulations → Create

**D** Your tenant now appears in the list. Click **your company name** to open it and begin deployment.

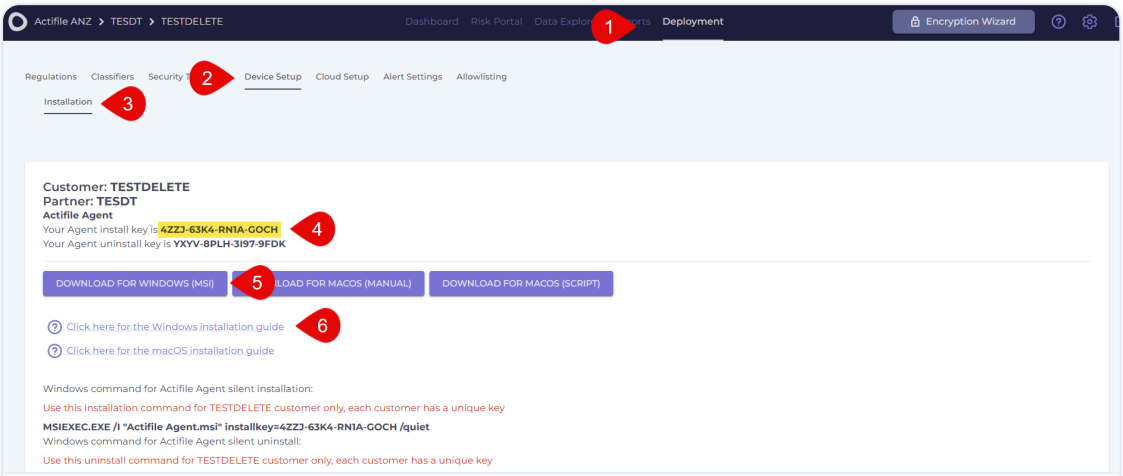



Click your company name to open the tenant

## 3 Deploy the Actifile Sentry Agent

**CRITICAL —** place Actifile in your AV / EDR / MDR / XDR allow list **before** installing. **Allow-list guide →**

Inside the tenant, go to **Deployment → Device Setup → Installation**. Copy the **Agent Key** and download the Sentry Agent — Windows (MSI), macOS (manual) or macOS (script).



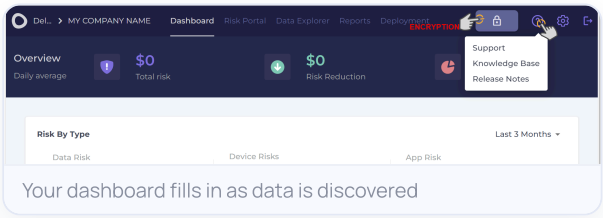
Copy the Agent Key and download the installer

Deploy across your endpoints and servers (up to **10 devices** on trial). For multi-machine rollouts, make sure the installer path uses the **Fully Qualified Domain Name (FQDN)** reachable by those machines. **Deployment options →**

### Now relax while it scans

Install takes ~2 minutes; the first audit completes in roughly **20–90 minutes**. Explore the dashboard, risk metrics, classifications and the in-product tutorials (bottom-right) while it runs.

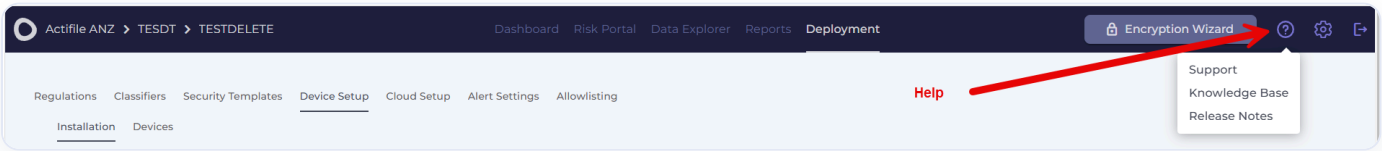
**Do NOT turn on encryption.** Run in monitoring mode for 1–3 months first (can be days if needed) and **talk to us** before encrypting any data.



Your dashboard fills in as data is discovered

### Need a hand?

The **?** menu (top-right) has **Support**, the **Knowledge Base** and **Release Notes**. Browse the portal sections to see how your data is monitored — just avoid saving changes unless you understand the impact.

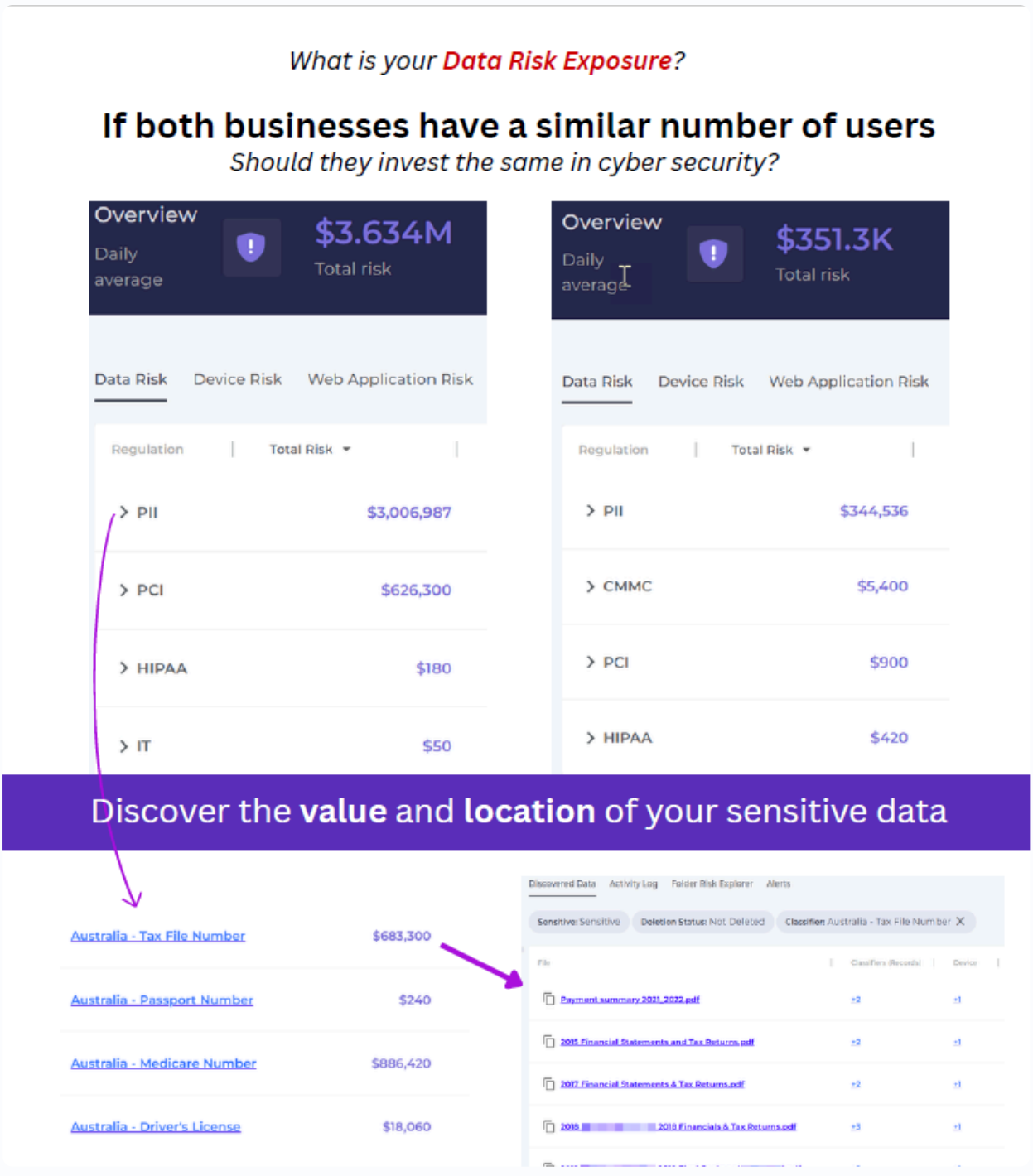



### Within minutes, Actifile begins working

- **Discovers** sensitive & regulated data, including stale files
- **Quantifies** your data-risk exposure
- **Values** the real financial impact of exposed data
- **Highlights** your highest-risk endpoints

## A quick walk-through of the data

Two businesses with a **similar number of users** can hold **vastly different** amounts of valuable data. Actifile puts a dollar value on it — then lets you **drill down** from a regulation like PII, to a data type such as Tax File Numbers, right down to the **individual files** holding it. No projects, no policies — just click.




**Ready in minutes. Let's review your results together.**

Reach our local Australian team for sales, a demo or deployment help.

**Actifile (Australia & New Zealand)** · **(02) 9151 7313**
**support@actifile.com** · **Knowledge Base**

**Book a results review →**

# Why it's critical to every size of business today

Once a breach occurs, the first objective for many attackers is not necessarily to disrupt systems, but to steal data. Why? Because stolen data provides immediate leverage. Even if an attack is detected and contained, the attacker can simply claim, "We have your data," placing the burden on the organisation to determine what was accessed, what was exfiltrated and what obligations it now has to customers, regulators and stakeholders.

Historically, protecting data at the file level has been difficult. Traditional Data Loss Prevention (DLP) solutions are often complex to deploy, expensive to maintain and can create enough disruption to users and business processes that they never achieve full adoption.

The result is that many organisations focus heavily on preventing attackers from getting in, but far fewer have an effective strategy for reducing the risk of data loss and protecting the data itself when a breach inevitably occurs. This is where Actifile takes a fundamentally different approach—by making sensitive data unusable to attackers, even if they manage to access or steal it.

A good analogy is a traditional DLP deployment in a legal firm. The organisation/MSP spends months building policies, exceptions and workflows. The solution is enabled on Monday morning. By 9:30am a senior partner cannot access a document and calls IT. The exception is granted. Later that morning another file is blocked and another call is made. Before lunch, the product is disabled.

Today, most organisations have very little tolerance for workflow disruption, which is one of the reasons many traditional DLP deployments never reach full operational maturity. An additional benefit is that Actifile intentionally errs on the side of caution. We will often over-classify data to ensure potentially sensitive information is identified and protected. While this may introduce some false positives, the patented delayed transparent decryption model helps to ensure there is little to no impact on users.

**"We have your data."**

That single claim is enough to trigger the regulatory, financial and reputational fallout of a breach. **Actifile helps to reduce the leverage** by rendering the vast majority of sensitive data useless — so a stolen file is worth nothing to an attacker.

## Frequently asked questions

### "We don't have sensitive data — why use Actifile?"

You'd be surprised. Most organisations store more regulated data than they realise — exports from ERP, CRM and finance systems, email attachments, and files of passwords. Actifile helps to uncover and secure it. Ask about a complimentary **Data Risk Assessment**.

### "We only use cloud apps — do we still need it?"

Yes. Endpoints like laptops quietly store sensitive data from downloads, attachments and offline work — and they're prime targets. Actifile finds and secures these hidden risks. Cloud security alone isn't enough if endpoints and networks aren't covered.

### "We don't have budget for another tool."

Actifile offers a **free initial data-risk assessment** showing whether your endpoints hold regulated data and which carry the highest dollar exposure. Breach-minimisation typically costs just **1–3%** of your estimated data-risk value.