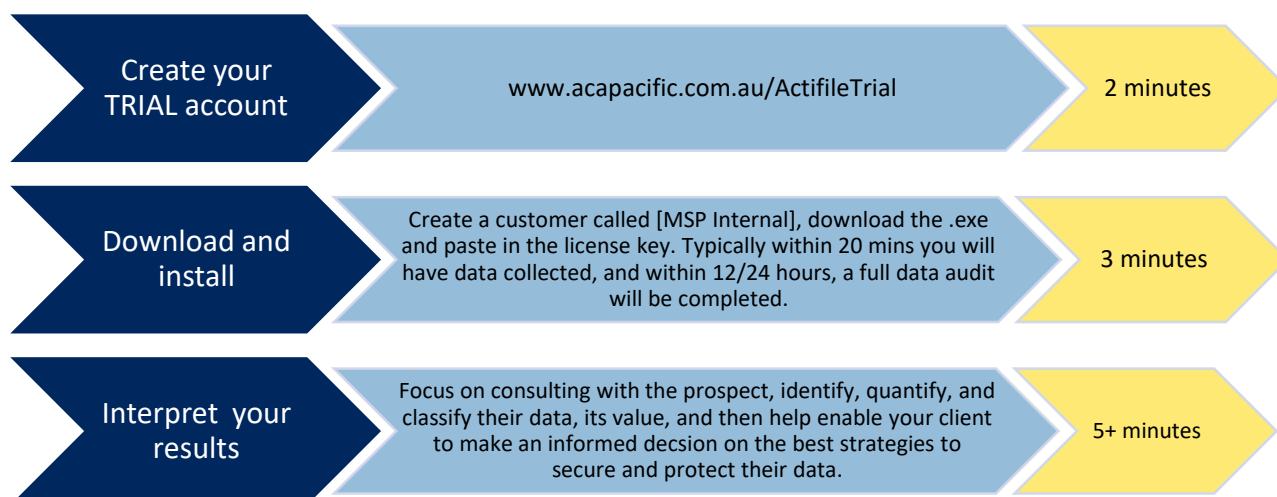


ACTIFILE (SaaS) QUICKSTART GUIDE FOR MSPs

Quick Links:

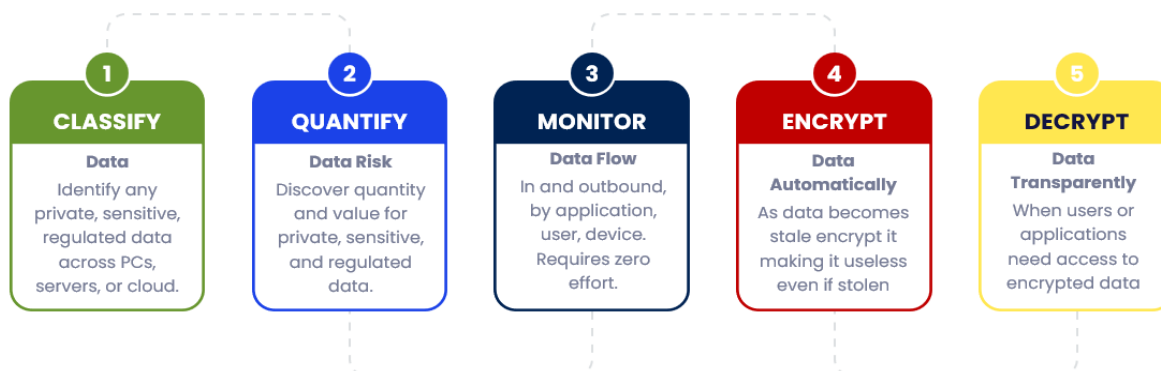
- 60 second demo of Actifile: <https://vimeo.com/875873564/4aa1b2fa86>
- 60 second video on how Actifile works: <https://youtu.be/Y4JPH2wWRXw>
- Book a Live Demo: <https://bit.ly/ActifileDemo>
- Create an MSP account and TRIAL Actifile: www.acapacific.com.au/ActifileTrial

Ask any prospect: *How much private data being stolen is acceptable to you, your customers, and the board? Do you know how much regulated data you have in your business, where it is located, who is at the biggest risk of it being stolen, and what is the total value of that data? Would you like to reduce your data risk by typically 60% to 90%?*



Data Privacy Platform

Autonomous AI driven platform that **encrypts** data as it becomes stale to **make it useless to a hacker**



Actifile makes the process of discovering, classifying, valuing, and securing (encrypting) private data trivial with near zero effort required. **Seeing is believing.**

Making sense of your clients private, sensitive, and regulated data

In today's fast-paced data-driven world, safeguarding private and regulated information is paramount. Actifile Data Discovery stands at the forefront, offering a comprehensive solution that meticulously uncovers, identifies, and secures sensitive datasets.

Often Actifile will discover large amounts of private data on endpoints that is unknown, forgotten about, or sometimes simply a false positive. Note: Actifile is searching for patterns of numbers and letters that conform to Australian Data Privacy requirements, in some cases, you may find records in for example an Excel spreadsheet may not actually be private data. Simply tag them as a false positive.

Comprehensive Data Privacy Platform for MSP and MSSP

	FEATURE LIST AND CAPABILITY (PARTIAL)	Actifile	Other product
1	Endpoint Edition - Windows, Mac, Linux, NAS: (base solution) identifies, monitors, and tracks private, sensitive, and regulated data across all endpoints without effort. Deploy and go and no/minimal configuration required.	✓	
2	Office365 Edition - SharePoint, OneDrive, Teams, Email (Google Workspaces is on Beta and due out shortly, other cloud shares planned on the roadmap).	✓	
3	No reboot, silent installation non disruptive to users.	✓	
4	Preconfigured and designed to automatically discover and classify all types of private, sensitive, and regulated data across most geographical regions including Australia and New Zealand without configuration or effort.	✓	
5	Fully autonomous AI driven data discovery, classification, quantification, value, encryption, and decryption on the fly - designed for MSPs and MSSPs.	✓	
6	Fully multi-tenant SaaS application that uses a lightweight agent for scanning, encrypting, decrypting data and a container app for Cloud Shares like Office365.	✓	
7	Different from the traditional DLP method which requires creating and maintaining a rule for each leakage event (up front work and a lot of maintenance), Actifile classifies, tracks, and encrypts pre-emptively groups of files, thus saving time and effort	✓	
8	Create a Rule to automatically encrypt your data by your own-defined classification type (e.g. TOP SECRET).	✓	
9	Make your stale private data useless and worthless to a hacker, even if stolen.	✓	
10	No private, sensitive, or regulated data is housed or stored in the Actifile cloud.	✓	
11	No user training required by users – seamless, invisible and near zero friction.	✓	
12	Don't rely on users to identify, move, tag, and encrypt data, fully automated process with near zero disruption.	✓	
13	Determines data risk value (in dollars) and quantify the risk – quantity and value of data by overall organisation, classification, and device. Note: this helps customers understand the value of their risk and often increases cybersecurity budgets as they now can see in black and white what their data is worth.	✓	
14	Who has the highest risk (they may require more cybersecurity), and what are the files that they have that contain that risk. Which users don't have private data on their devices.	✓	

15	Identify by device what and how much private data they have, and how it flows in and outbound.	✓	
16	Extensive search criteria help make data understandable and useable.	✓	
17	Automatically discover and classify data as it is newly created or moved into the environment.	✓	
18	Zero touch to users.	✓	
19	Create a 'person query' to identify a specific person across private data.	✓	
20	Monitor data movement to/from Applications / Web Applications and analytics.	✓	
21	Persistent file level encryption that makes data useless unless you have Actifile installed and working on that device.	✓	
22	Offline access to data enabled to minimise disruption.	✓	
23	Deactivate and reactivate users from management dashboard.	✓	
24	Comprehensive event audit and logging.	✓	
25	Automatically encrypt all stale private data without user intervention.	✓	
26	Encrypt all data by classification (e.g. Passport, Drivers licenses, Medicare, Centrelink, Credit Card, etc).	✓	
27	Encrypt groups of files (classifications) based on how much data risk they have in dollars, thus avoiding manual work to encrypt by file or folder	✓	
28	All private data automatically becomes encrypted depending upon your specific requirements of what is stale data down to each classification of data.	✓	
29	Instant decryption of encrypted files with a normal 'double click'. No user training is required. Just open the file as you would normally do - wherever they are: on endpoints, on file servers, on cloud shares.	✓	
30	Automatic re-encryption of data when decrypted data saved.	✓	
31	Create trusted applications that automatically decrypt data as requested.	✓	
32	When a user leaves your business, and accidentally takes private data with them, all encrypted files will be encrypted as soon as Actifile is disabled on their device. Click and de-activate one or multiple users.	✓	
33	FIPS-140-2 identification and encryption support	✓	
34	HIPPA, PCI-DOS, CMMC, PII, GDPR and more	✓	
35	Support for multiple countries drivers licenses, passport, Centrelink, Tax File Numbers, Medicare, HRIP, credit cards, date of birth, electronic funds transfers and wire information, NRIC numbers, SWIFT/BIC, ABN, BSB, GDPR Digital Identity, Medical records including for example Body temp, Blood pressure, Blood Panel, Body Mass index, ePHI, ICD-10, IME, ITAR, Social Security Numbers, UK VAT number, ACH Clearing Numbers and much more.	✓	
36	Over 40 included default file extensions and unlimited that you can simply create, to discover, classify, encrypt, search, and report on.	✓	
37	Create advanced Rules and Channels to perform almost any decryption process.	✓	
38	Automatically decrypt data sent as email (leverage email encryption-in-transit).	✓	
39	De-crypt all data in specific locations / repositories (e.g. public shared locations).	✓	

40	Define a Rule to prevent data from being deleted.	✓	
41	Define a public classification by content.	✓	
42	Define a public classification by folder. PLS EXPLAIN WHY IMPORTANT	✓	
43	Define a public classification by extension.	✓	
44	Define a public classification by channel.	✓	
45	Create a Rule to track and notify the change of a file extension.	✓	
46	Create a Rule to prevent copying of data from a removable drive to fixed drives.	✓	
47	Define a classification rule by removable device.	✓	

KISS (Keep It Simple) principle for clients to understand the importance of Data Privacy

- When you buy or rent a house you typically invest in home and/or contents insurance.
- How do you determine the value of your insurance policy?
- You (and your insurer) perform a 'risk assessment' – what is the value of your contents, your house, where is it located, is it in a high crime area or susceptible to bush fires or flooding?
- The insurance company will provide you with the premium that you need to pay.
- The higher the value of your contents, in high-risk area means you will pay a higher premium.

With malicious AI BOTS attacking 24/7, every business regardless of size now lives in a high crime area.

Hackers want to cause disruption and pain – stealing or encrypting private data is their main goal.

When it comes to cybersecurity, endpoints are like the gates to your digital fortress — and they're often left inadequately guarded. The result? Easy pickings for hackers. These opportunistic infiltrators and their AI BOTS will grab a file here, a folder there, perhaps even just a sliver of your data, just in case they're quickly caught. Then they'll issue a bold-faced threat: Pay up, or we'll unleash the entirety of what we've taken. The catch? The value of the seized data might be peanuts; the real gain is in the potential payoff, not the information itself.

Enter Actifile, your personal data guardian. Actifile automatically encrypts your data on a granular level, rendering it utterly worthless to any would-be data bandits. As the data ages and becomes stale, its encrypted state ensures that even if it's stolen, it's effectively a dead end. No more nail-biting over stale data that could turn into a headline-grabbing data breach.



And all of this is done at a scale and an investment that make cybersecurity not just palatable but practical. Actifile's Data Privacy Platform offers peace of mind for companies of all sizes, helping to secure your customer's sensitive information from the evil of identity theft. Time to level up your data security game with Actifile.

Once you have run an Actifile discovery across a machine or multiple devices (silent instal and no reboot required) – it is time to help the customer understand their data and their potential risk.

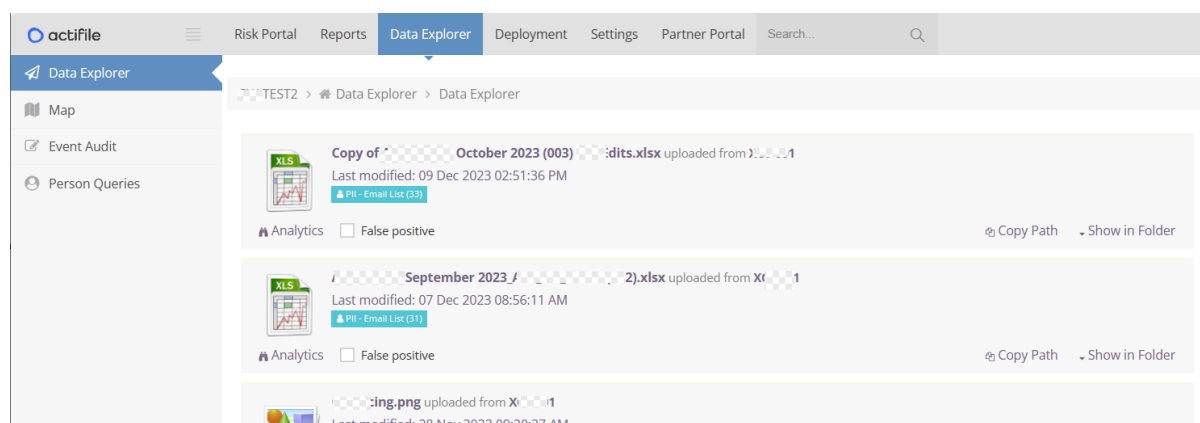
Interpreting the data discovered by Actifile.

GO TO: Actfile > Data Risk

- At the top are the classifications by highest value, start here and work down to lowest value to confirm the risk value of these files with your client.
- In many cases the customer will say “Oh, I didn’t realise I still had those files, I thought I deleted them...” or similar.

Sensitive Files						
Classification	Actions	Sensitive	Files	Records	Residual Risk in USD	Risk in USD
Credit Card - MasterCard(New)	 	<input checked="" type="checkbox"/>	6	131519	\$ 39,200	\$ 13,151,900

In the case above example, click the ‘hotlink’ for [Credit card – MasterCard], and this show you the data files that correspond to that Classification of data. **NOTE:** To protect data confidentiality, there is no direct access to the file, just the name and its path.



As part of the consulting project with your client:

- Identify the highest value files first and quickly determine if they are real or a false positive.
 - In most cases, there will be less than a dozen or so files per classification that contain the bulk of the private data making analysis very simple – use this as a CONSULTATION with your customer or prospect to help them better understand their business and the value of their data – which in turn creates a powerful foundation for selling risk reduction.
 - What would it mean if these ‘12,437’ records were stolen by a hacker and released?
 - Can any of this data be used by a hacker to threaten the person with exposing that data so the individual pays the hacker money not to release it and naming you as the source?
 - Example 1: we have seen a case where product SKUs in a price list was interpreted as Credit Card numbers and it was easy to identify and mark as a false positive.
 - Example 2: a customer identified a file called “Customer List” (which contained private data) from an employee who was just about to leave the organisation.
 - If data has been encrypted by Actifile, and a user steals it, once Actifile is turned off on their device – or data is moved to another device, the file will be encrypted and useless to them.
 - If you do not to report on a data classification type (eg BSB, ABN, etc) simply untick.
- Where the data is located – endpoints, OneDrive, SharePoint, Teams, NAS?
 - Actifile’s Endpoint Edition (base solution) delivers endpoint risk analysis with an optional VM for SharePoint, OneDrive, Teams, and NAS data.

3. Which users have the highest risk value? Which have the lowest risk? Note: it is equally important to know if users don't have any regulated data on their endpoint, as if they are breached, the risk is minimal of a data exposure.
4. Do some users require a 'higher level' of security due the quantity of private data they have (e.g. CEO, CFO, HR, etc)
5. For each classification type of data, how long is that file in use and after how long does it take to become typically stale?
 - a. What is the IMPACT if that data is stolen?
6. What additional data does the client have that they consider to be confidential, and would they like to automatically encrypt it? You are able to create your own classifications for documents or files.
7. How many instances of critical files?
8. Which applications access which files and need automatic decryption rules created for them?
9. How does data flow in and out of the business? What web applications do they use – a good example is the MoveIT breach. These are discovered and monitored by Actifile.
10. Educate your customers about what constitutes private, sensitive, and regulated data and why it is important to protect and secure it.
 - a. Email addresses.
 - b. Turn off classifications (e.g. BSB) with a simple 'click' if you no longer wish to track it.
 - c. Passport, Drivers licenses, Medicare numbers and so forth
 - d. Do they have any industry unique data that needs to be classified?

Data insights – why understanding your client's data is critical in 2024.

Do you remember when the first MSP concept came out, and only a few resellers adopted it initially, and these often rapidly became leaders by offering monthly subscription instead of traditional break-fix? **Now almost every reseller is an MSP.**

Data Privacy, and modern **prevention-based** cybersecurity **MSSP** (Managed Security Solution Providers) will be the next major transition for MSPs. ACA Pacific have put together a trio of valuable and cost-effective solutions (Actifile, ConnectSecure and Xcitium) that enable most MSPs to within days become an MSSP.

In an era when data privacy is no longer a luxury but an expectation and, in many countries, a legal requirement, we understand how critical it is to arm Managed Service Providers (MSPs) with the right tools to not just survive, but to thrive in a rapidly evolving industry and **create completely new revenue streams.**

Data Insights Demystified: Actifile provides a comprehensive analysis of the data insights offered and their direct relevance to the MSP-to-MSSP transition. Data insights are a strategic edge for MSPs, leading to more informed business decisions, enhanced customer relations, and, crucially, a smoother transition to the intricate world of Managed Security Solution Providers.

Valuable and Cost-Effective: The MSSP Advantage: Discover the cost savings and efficiency boosts Actifile will bring to your business. By leveraging data insights, MSPs can seamlessly upscale and become an MSSP, unlocking new revenue streams while maintaining a competitive edge.

Elevating Your Business in 2024: By becoming an early adopter of our cutting-edge solutions, you can redefine what security means for your customers and differentiate yourself from the traditional MSP.

Conclusion: Actifile is an onramp to a whole new world of opportunities for your business. Prepare to be impressed by the transformative power of data insights and the role they will play in shaping the future of MSPs and MSSPs. Welcome to the next level of service provision.

Suggestions:

1. When talking to a new prospect, focus on cybersecurity and helping them understand the value of their data, the **IMPACT** if that data is stolen and the high **PROBABILITY** of a breach due to automated AI driven bots that are relentlessly attacking 24/7, looking for weaknesses that they can exploit mean all companies of all sizes urgently need to transition to prevention-based cybersecurity.
 - a. **Reduce your Attack surface** – Close your doors and windows – remediate critical vulnerabilities urgently – Considering using the exceptionally cost effective and powerful ConnectSecure (www.acapacific.com.au/ConnectSecureTrial) MSP vulnerability Platform.
 - b. **Understand the value your data and secure it** with **FILE** level encryption as it becomes stale (Actifile).
 - c. **Deliver 24/7 threat hunting with remediation** (Xcitiium MDR/XDR) – not just alerting - who in your business is going to be the person who every night gets woken up at 1am with a security alert, then again at 2:30am, then at 2:45 with a number of potential false alarms – or even worse an active breach at one of your clients – do they have the actual expertise to investigate the attack chain, make the determination and stop the damage from the breach?
 - d. Included **Incident Response** (Xcitiium MDR/XDR) at no additional charge to the MSP.
 - e. If your cybersecurity vendor offers incident response, we believe it should be included (free) in their security services. Why? If the cybersecurity vendor is confident, they will stop all the damage from breaches, why would they charge you extra to fix a breach that they failed to detect?
 - f. Ask them why they charge extra for failing to protect you?

Hackers and automated bots are 24/7 – the threats are real and immediate:

Russian, Iranian, or Chinese hacker groups will probably not target your customers with 2 to 250 PC's, however, automated BOTS **will** - and these attacks are 24x7x365. They are relentless and AV, NGAV, EDR is no longer enough.

- 72 **new** application vulnerabilities per day in 2023 (2100 pm and 6300 per quarter) – and vulnerabilities are like a house that has a broken lock on the front door, or even worse, the front door is left wide open. Most prospects will have tens, hundreds, or even thousands of application vulnerabilities that a hacker can and will leverage to breach and move internally.
- 67,000+ cyber-attacks were reported to Australian government in 2022.
- 22 Australians were [hacked](#) every 60 seconds in 2022.
- Traditional AV, NGAV, and EDR are typically detection-based products and quite simply, they are not enough today to prevent the new generation of AI and automated bots.
- **Modern cybersecurity solutions** have transitioned into **prevention-based solutions** focused on reducing the attack surface and making it harder for a hacker to see and breach your business – these complement and improve 'old school' detection-based products.

Positioning cybersecurity in 2024 – Data Privacy is a critical foundation to helping your customers.

Scaring clients is not a good sales strategy. Educating them as to why 'old school' AV and EDR products are not enough and how you can help to deploy cost effective prevention-based solutions to help keep hackers where they belong – outside their network. Using Actifile, you can almost instantly differentiate yourself from the incumbent MSP or even internal IT team.

- **Discover** and explain to the customer what data they have, where it is located and its value. Typically, a tiny percent of small businesses or MSP's help customers understand this major issue

which impacts almost every small business – they just don't know it – you can help them understand the issues and this will help demonstrate why you are an expert that should be trusted.

- Build a **simple justification** to increase expenditure in cybersecurity to protect that private data, highlighting the risks of data being stolen. Don't over complicate the issue – use layman's language and tell the story by referencing back to home security (watch this [15-minute presentation](#))
- Help your customers **reduce their attack surface** making it exceptionally hard for a hacker to breach them and automatically encrypt stale data, so even if it is stolen, it is useless to the hacker.

SHOW THEM THE EVIDENCE IN BLACK AND WHITE

- Perform a data risk assessment to show them the problem (how much private data they have): www.acapacific.com.au/ActifileTrial
- Show them their vulnerabilities (ease of a hacker breaching): www.acapacific.com.au/ConnectSecureTrial
- Discover if they have any unknown malware lurking in their environment with Xcitium.

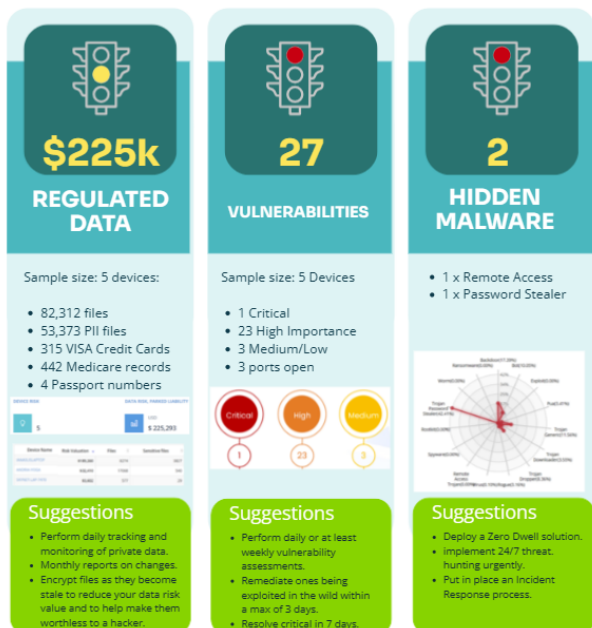
Advanced Demonstration of Actifile – in minutes deliver a powerful demonstration.

1. Stop sensitive files from being deleted:
 - a. Deployment > Policies > Rules > ADD > Create or Edit Rule with Name [Stop Deleting Sensitive Data] > Rule Status [ON] > When User [Protect Folder Content from Deletion] > Apply [All] Channels > Apply [All] Tags > Apply [All] Devices > Prevent [ON] > Create Case [ON] > Colour [Purple] > Icon [Flash] **SAVE.**
 - i. **To turn OFF:** > Rule Status [OFF]
2. Encrypt data by your own user-defined classification (e.g. A TOP SECRET)
 - a. Deployment > Policies > Classifiers > Add > Enable Policy. [ON] > Classification Type [By Content] > Caption [Top] > Rule 1 [Contains Exact Phrase] = A TOP SECRET (by putting A, it will at the front of searches for demo purposes) > Optional [Add Rule]
 - i. **NOTE:** If you use a single word, for example confidential – every occurrence of confidential will be encrypted, including non-confidential. Always use a phrase (e.g. TOP SECRET)
 - ii. **NOTE:** Run rule to identify data BEFORE you enable encryption.
 - b. Now create a file and include TOP SECRET in the footer, save file – the file will be automatically identified by Actifile.
 - c. Email file to prospect – they won't be able to open the file.

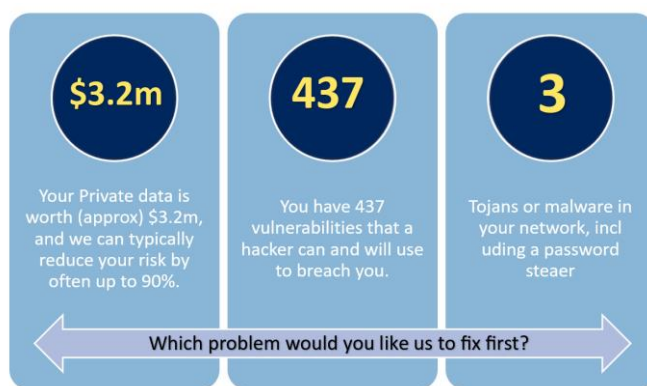
1+1+1 = Compelling competitive advantage and a new customer!

Reverse the roles, if another MSP approached one of your customers, and did the same, and provided them a simple one- or two-page document that clearly outlines the issues and areas of concern that they discovered during the risk assessment (using Actifile, ConnectSecure and Xcitium) – what would your customer do?

Note: the image below is not a standard report, we used PowerPoint to present the consolidated data.



Or, an even simpler presentation of the data using Microsoft WordArt



Data is the most important asset at ALL your customers – yet few understand its real value or the risk – as historically data privacy products have been too complex, too expensive, and quite simply too difficult to understand. Welcome to Actifile – the Data Privacy Platform designed for MSPs and MSSPs.

Back to basics: People only invest when they need to solve a problem:

WHY PEOPLE BUY...

Probability and Impact

Low probability with high impact = minimal investment

High probability with low impact = minimal investment

HIGH PROBABILITY with **HIGH IMPACT** = **URGENCY & INVESTMENT**

High **PROBABILITY**

- Breach = not IF, **WHEN**
- Automated** Vs Targeted
- Endpoints often 1st breach point

+

High **IMPACT**

- Always worse than expected
- Loss of customers/reputation
- Fines, penalties, compliance

=

URGENCY & BUDGET

- Identify quantity of data = risk
- Identify value of data = budget
- How exposed they are – TODAY!

Overcoming Objections

We don't have any private data!

We don't have any private data... or do we? Many of our customers were surprised to find out that they actually had a lot more private, sensitive, and regulated data than they thought. It's not until you conduct a Data Risk Assessment that you truly discover the extent of your data. Something as simple as downloading a report from your CRM system or viewing resumes in HR could potentially expose regulated data.

To help you gain clarity, we are offering a complimentary Data Risk Assessment. This assessment will uncover whether you have any data, where it's located, who poses the highest risk, and what the overall value of your data is across your organization. Don't wait until it's too late - take advantage of this opportunity now.

We only use cloud applications – we don't have data on our laptops!

In today's digital era, many businesses pride themselves on operating solely through cloud applications, eliminating the need for local data storage on devices like laptops.

However, this approach can present hidden risks when seemingly innocuous activities—such as downloading spreadsheets, emailing lists, or taking credit card details over the phone—can lead to sensitive data unknowingly residing on endpoints.

These devices, often the target of the initial breach by hackers or automated bots, may inadvertently expose private and regulated information. To understand if there is a risk and the magnitude of data risk within your organisation, we can conduct a comprehensive analysis which is painless and invisible to users.

By examining either a select number of devices or the entire infrastructure, we can swiftly gauge the potential exposure and even put a dollar value on it.

Additionally, it may be prudent to undertake a vulnerability assessment to evaluate how susceptible the company's defences are to intrusion efforts. This dual approach not only reveals the current state of data risk but also the likelihood of a successful cyber-attack on your business. Would you be interested in finding out just how secure your data really is with our quick and thorough assessment?

We don't have any budget!

We have great news! The initial data risk assessment can be performed free of charge. We utilize a industry-leading Data Privacy Platform and, as a strategic partner in [region], we offer a limited number of no-cost assessments per quarter.

It would be reassuring to confirm that your business does not have any regulated or sensitive data on endpoints. Additionally, we can identify devices with high data risk values so that your IT team or service provider can address them promptly. We can also conduct a vulnerability assessment to determine the ease with which a hacker or automated bot could breach your business. Would you like us to proceed with the Data Risk Assessment, the vulnerability assessment, or both?

START A TRIAL OF ACTIFILE:

Step 1 – Create your Actifile Account and create your 1st customer (about 2-minutes)

- a. Create your Actifile MSP account:
<https://app.actifile.com/Account/SignUpPartner?partnerkey=BV4X-C9CC-IICW-OWV8>
- b. You will be requested to verify the email address used (it must be unique and never before used in the Actifile system).
- c. If the confirmation email doesn't arrive in a few minutes, click **[RESEND]** and check JUNK MAIL please.
- d. Logon to your account
[Actifile](https://app.actifile.com/account/login/) (<https://app.actifile.com/account/login/>)
 - a. Username [your email address]
 - b. Password [You just created]
- e. Click **[CUSTOMERS]**, then **[ADD CUSTOMER]**, then create your 1st customer - **watch a [2-minute video](#) MSP deployment and a [1-minute](#) end user deployment video** – we suggest the following:
 - a. Customer name: **[INTERNAL - MSP NAME]**, include First Name, Last Name.
 - b. Click **[Set customer login]** (if disabled, your customers will not have access. Access is only via the partner through the partner portal).
 - i. This will allow the customer to manage their own environment if you want them to have access to their environment.
 - c. Enter **[EMAIL]** and **[PASSWORD]** – NOTE: no emails will be sent to this email address; it is to verify that it is unique.
 - d. Primary Regulation Country Select **[AUSTRALIA]**
 - e. Turn **[ON or OFF]** each Compliance Profile as required – typically change CMMC and IT to **[ON]**
 - f. Save Changes.
 - g. Congratulations you have created your 1st customer (**INTERNAL MSP**).

Step 2 – Download & Install the Actifile Agent on to your device (about 3-minutes).

- a. Click on Customer Name **[INTERNAL MSP]**, it will be blank until you deploy your 1st agent.
 - a. TOP tab – 4th along **[DEPLOYMENT]**.
 - b. **CRITICAL**: this will be the unique key for **all endpoints at this customer**. Every new **[Customer Name]** **MUST have a unique key**, or it become unmanageable if the same key is used across multiple customers.
 - c. At the bottom of page, follow the **[Click Here]** links to learn more about **Downloads, Installation Guide** and **Important AV/EDR information** (set up exclusions in your AV product – you will probably need to put 3 .exe in your AV/EDR allow list:
 - i. **AFAgentService.exe**
AFUdaterService.exe
AFAgentServiceManager.exe

Step 2

Exclude the folder + sub folders from scanning:

C:\Program Files (x86)\Actifile Agent

Step 3 (optional – for Intrusion Prevention Systems – IPS):

URLs for whitelisting (all HTTPS port 443):

<https://app.actifile.com>

<https://actifileapp1.azurewebsites.net>

- d. Click **[DOWNLOAD FOR WINDOWS]** to install to your device.
 - i. No reboot is required.
 - ii. Within about 15 minutes data will start appearing in the **[INTERNAL CUSTOMER]** portal. Normally a full audit has been completed with 6 or so hours.
 - iii. From now on, it is all automated and all private, sensitive, and regulated data is being monitored and tracked in real-time.
 - iv. **Note:** When deploying to multiple machines, the “path” must be the FQDN to the installer package accessible from the installed machine.
- b. While waiting for the audit to populate with your data, let’s do a quick walk through of some of the capabilities of Actifile.
- c. Click top left **[ACTIFILE LOGO]**, **TOP** Horizontal Tab, click **[PARTNER PORTAL]**, Click 2nd from the bottom **LEFT** Vertical tab **[SUPPORT]**, create a new Login – this is the best way to ask technical questions to the Actifile team. Note: *this needs to be a different email address than the Actifile Account created.*
- d. Go back to your original browser tab (clicking Support will automatically open a new tab), **LEFT** Vertical Tab, click **[KNOWLEDGEBASE]**
 - a. Explore the Actifile Knowledgebase, some examples of searches include:
 - b. Search **[Channels]** – these are essentially pre-designed ‘rules’ that you can implement as you become more experienced with Actifile – scroll down the list.
 - c. Search **[SharePoint, OneDrive, or NAS]** – additional chargeable option per TB per month
 - d. Search **[Agent Deployment]**
- e. Click TOP Left Vertical Tab **[Actifile logo]**, then **LEFT** Vertical Tab (8th down) **[PARTNER SETTINGS]**, then Turn **[ON]** 2 Step Verification, then upload your logo (Actifile is currently a co-branded solution)

Step 3 – Discover your private, sensitive, and regulated data. (About 5 minutes) Watch a [4-minute demo](#) of Actifile.

- a. By now, the audit should be producing some results, so let’s look at the results.
- b. Click TOP Left Vertical Tab **[Actifile logo]**, then **[CUSTOMER]**, then **[INTERNAL MSP]**, the Dashboard will now show how many devices are connected and the total **Data Risk Value**.
 - a. TOP Left Vertical Tab **[DATA RISK]**, all the different classifications will start appearing here, and immediately you can see what you have.
 - i. By Classification, Quantify how many files and records, Risk value, Encryption (should be \$0)
 - ii. We will explain the **[PADLOCKS]** in Stage 6 – Encryption

- iii. **[APPLICATION RISK]** – over time, this will track the flow of all data inbound and outbound to this customer. You are able to change the date range and **[DETECTED]** and **[TRUSTED]** – this is for advanced users and when you turn on encryption and start using Channels / Rules.
 - iv. On the **LEFT** Vertical Tab, Click **[MAP]**, then **[EVENT AUDIT]**, and keep clicking the options to drill further into the data analysis.
- c. Top LEFT Vertical tab, click **[DEVICE]**, This will give you a view by individual device – click the links and explore.
- d. Top LEFT Vertical tab, click **[ACTIVITY LOG]**, click the options and explore.
- e. **Understanding the BASICS of Encryption - we will work with you BEFORE you start encrypting your or your customers data – (About 1-minute). Watch a [2.4-minute video](#) on Actifile Encryption**
- f. Encryption is very simple, to get a quick understanding – follow these steps **[DO NOT CLICK SAVE]**
- g. Click Top Left **[Actifile logo]**, LEFT Vertical Tab **[DATA RISK]**, Click the **[RED PADLOCK]**, Click Encryption Status **[ON]**, Select **[91]** days, Explore Channels dropdown – we will explain this in a later training course. If you click **[SAVE CHANGES]** – all files of that Classification will automatically become encrypted 91 days after the last access date, so if that data is stolen, it is useless to a hacker.
 - a. Internal users can automatically decrypt the encrypted files by a simple double click of the encrypted file = zero friction to users
 - b. You can also set up Allow listing of Applications to automatically decrypt encrypted files using Channels.
- h. DO NOT CLICK SAVE UNTIL YOU ARE READY AND FULLY UNDERSTAND THE ENCRYPTION PROCESS IN DETAIL BEFORE YOU START ENCRYPTING DATA.**

Note: you will have different options depending on if you are in the 'Global' view or the individual 'customer' view

If you have any questions, first look at the Knowledgebase, then create a ticket for the Actifile support team [Actifile Support Site | Data Privacy and Security](#). You will need to create a support login – this must be different from any other emails used (so perhaps support@YOURMSP.com.au or Tickets@YOURMSP.com.au – or any email that your technical team monitor. Normal response is typically about 12-24 hours due to time differences. Also, please feel free to send me a text to my mobile and I will see if I can help you!

.....

We have set you up with a **15-day trial key for 3 devices**, that we can **convert into an NFR key** once you are satisfied with Actifile. Please email ACA Pacific the email address that you used to create your Actifile account so we can ensure we process the special promotion pricing for you.