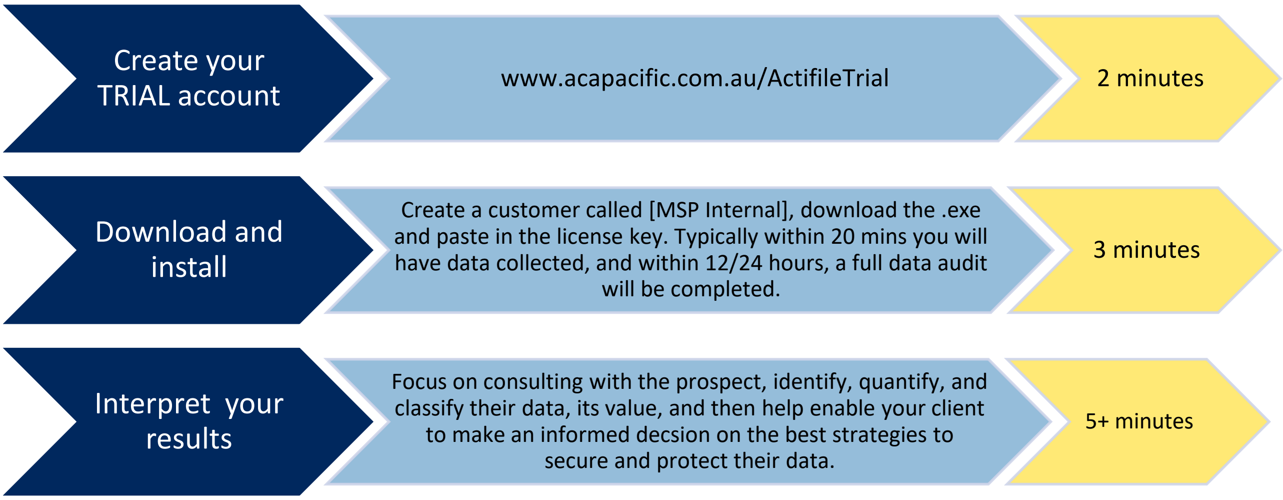
ACTIFILE (SaaS) QUICKSTART GUIDE FOR MSPs

Quick Links:

- Create an MSP account and TRIAL Actifile: www.acapacific.com.au/ActifileTrial
- 60 second demo of Actifile: https://vimeo.com/875873564/4aa1b2fa86
- 37 second – Intro video to Actifile: https://vimeo.com/1002347067
- Book a Live Demo: https://calendly.com/cyber-anz/30-min-sales-demo-to-actifile

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%?*



Create your TRIAL account

www.acapacific.com.au/ActifileTrial

2 minutes

Download and install

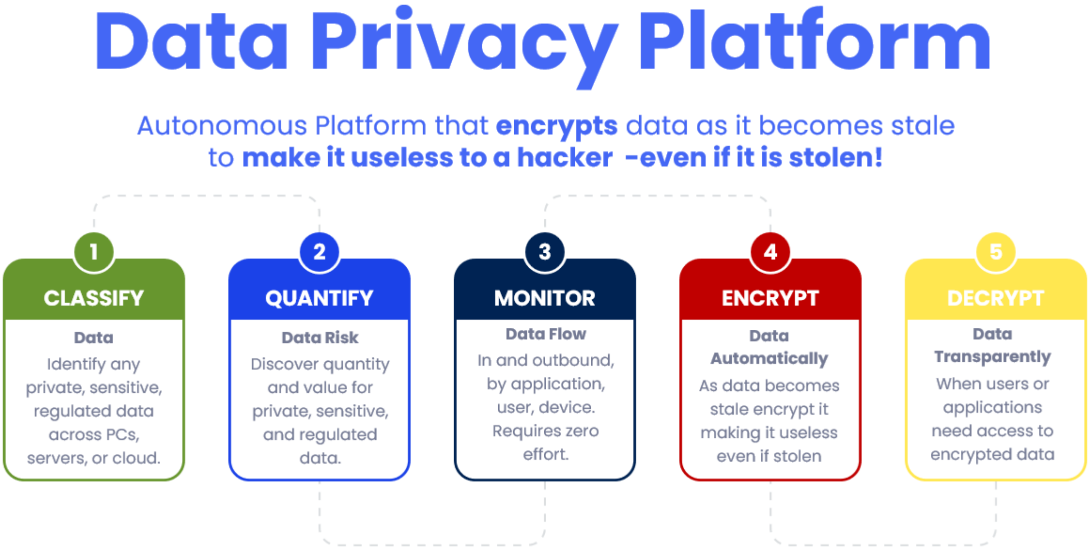
Create a customer called [MSP Internal], download the .exe and paste in the license key. Typically within 20 mins you will have data collected, and within 12/24 hours, a full data audit will be completed.

3 minutes

Interpret your results

Focus on consulting with the prospect, identify, quantify, and classify their data, its value, and then help enable your client to make an informed decsion on the best strategies to secure and protect their data.

5+ minutes



Data Privacy Platform

Autonomous Platform that **encrypts** data as it becomes stale to **make it useless to a hacker -even if it is stolen!**

1 CLASSIFY

Data

Identify any private, sensitive, regulated data across PCs, servers, or cloud.

2 QUANTIFY

Data Risk

Discover quantity and value for private, sensitive, and regulated data.

3 MONITOR

Data Flow

In and outbound, by application, user, device. Requires zero effort.

4 ENCRYPT

Data Automatically

As data becomes stale encrypt it making it useless even if stolen

5 DECRYPT

Data Transparently

When users or applications need access to encrypted data

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/)
   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** – we suggest the following:

   a. Customer name: **[INTERNAL + DEMO**], 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 own environment.
      ii. If you allow them to access to their portal instance – you will need to Enter [**EMAIL**] and [**PASSWORD**] – NOTE: no emails will be sent to this email address; it is to verify that it is unique.
   c. Primary Regulation Country Select [**AUSTRALIA**]
   d. Turn [**ON** or **OFF**] each Compliance Profile as required – typically change CMMC and IT to [**ON**]
   e. Save Changes.
   f. Congratulations you have created your 1st customer (**INTERNAL DEMO**).
   g. NOTE: when you login to your account – check if you are logging into your main MSP account, or the "Internal Demo" you just created.

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

a. Click on Customer Name [**INTERNAL DEMO**], 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.** To set up exclusions in your AV product – you will probably need to put 3 .exe in your AV/EDR allow list:
      AFAgentService.exe
      AFUpdaterService.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 20 minutes data will start appearing in the [**INTERNAL DEMO** 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. **ZERO EFFORT IS REQUIRED** until you start encrypting stale data.
   iv. **NOTE**: We strongly recommend that Actifile is run in (normal) monitoring mode for 3 to 6 months before encrypting data so all applications and websites are identified that may need access to encrypted data.
   v. **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 [**Agent Deployment**]
   c. Search [**SharePoint, OneDrive, or NAS**] – additional chargeable option per TB per month
   d. Search [**Channels**] – these are essentially pre-designed 'rules' that you can implement as you become more experienced with Actifile – scroll down the list.

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 DEMO**], 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.

   b. By Classification, quantify how many files and records, Risk value, Encryption (should be $0)
   c. We will explain the [**PADLOCKS**] in Stage 6 – Encryption
   d. [**APPLICATION RISK**] – over time (we normally recommend at least 3 to 6 months monitoring), 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.
   e. 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. IMPORTANT: 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. We normally recommend monitoring for 3 to 6 months BEFORE implementing encryption to ensure we have fully tracked all apps that require access to encrypted data.

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 [**25**] days, Explore Channels dropdown – we will explain this in a later training course.

h. If you click [SAVE CHANGES] – all files of that Classification will automatically become encrypted 25 days after the last access date, so if that data is stolen, it is useless to a hacker.
   a. Internal (licensed)users will 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.

i. 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!

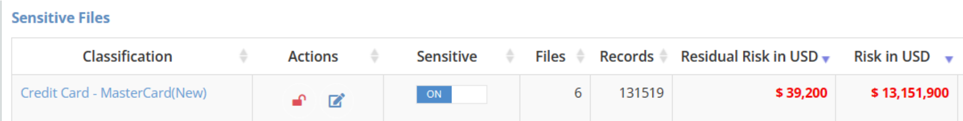
…….

We will 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.

Interpreting the data discovered by Actifile.

GO TO: Actfile > Data Risk

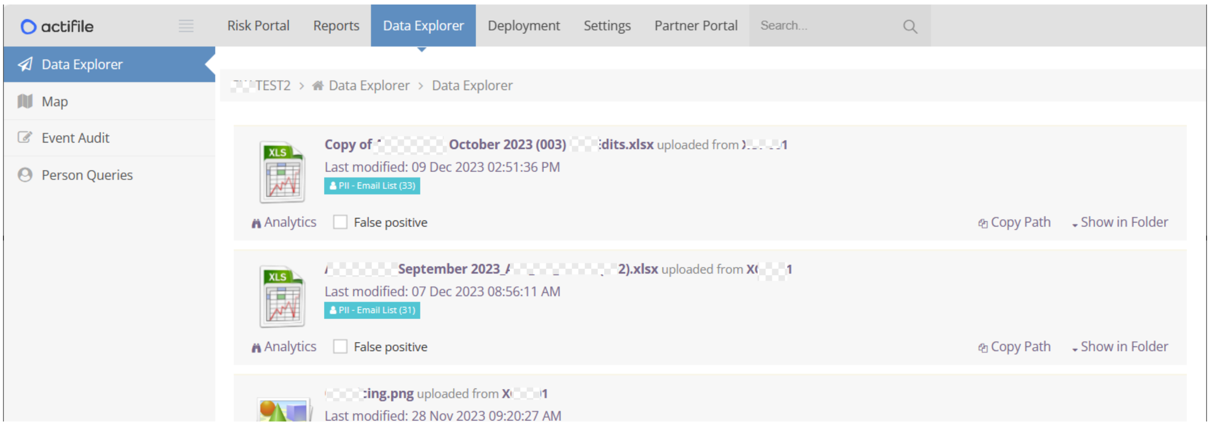
- At the top are the classifications by highest value, start here and work down to lowest value to confirm the risk value of these files with your client.
- In many cases the customer will say "Oh, I didn't realise I still had those files, I thought I deleted them…" or similar.



Sensitive Files

Classification	Actions	Sensitive	Files	Records	Residual Risk in USD	Risk in USD
Credit Card - MasterCard(New)		ON	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 – this also helps to ensure that local Data Sovereignty laws are upheld.



[redacted]TEST2 > Data Explorer > Data Explorer

Copy of [redacted] October 2023 (003) [redacted]dits.xlsx uploaded from [redacted]1
Last modified: 09 Dec 2023 02:51:36 PM
PII - Email List (33)
Analytics □ False positive Copy Path Show in Folder

[redacted]September 2023_[redacted]2).xlsx uploaded from X[redacted]1
Last modified: 07 Dec 2023 08:56:11 AM
PII - Email List (31)
Analytics □ False positive Copy Path Show in Folder

[redacted]ing.png uploaded from X[redacted]1
Last modified: 28 Nov 2023 09:20:27 AM

As part of the consulting project with your client:

1. Identify the highest value files first and quickly determine if they are real or a false positive.
   a. 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 exercise with your customer or prospect to help them better understand the value of their data – which in turn creates a powerful foundation for selling risk reduction.
      i. What would it mean if these '12,437' records were stolen by a hacker and released?
      ii. 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?
   b. 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.
   c. 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.
   d. 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.
   e. If you do not want to report on a data classification type (eg BSB, ABN, etc) simply untick.
2. Where the data is located – endpoints, OneDrive, SharePoint, Teams, NAS?

   a. Actifile’s Endpoint Edition (base solution) delivers endpoint risk analysis with an optional (chargeable) Microsoft 365 edition 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 from that machine – unless they use that machine to move laterally within the network.
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?

Overcoming Objections

We don’t have any private data!

We don't have any private data! 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.

This will be reassuring to confirm that your business does not have any regulated or sensitive data on endpoints – as often endpoints are the first breach point and where initial data is stolen from-

and with government legislation rapidly changing, it is critical to know where you stand with regards to regulated data.

Additionally, we can identify any devices with high data risk values so that your IT team or service provider can address them promptly.

In most cases, delivering Breach Minimisation technology is often between 1% to 3% of your data risk value – making it exceptionally affordable for you – should we discover any private or regulated data.

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?

ACTIFILE COMPETITIVE OVERVIEW:

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 and Mac (base solution) identify, monitor, and track private, sensitive, and regulated data across all endpoints without effort. Deploy and go and no/minimal configuration required.	✓	
2	**Office365 Upgrade** - SharePoint, OneDrive, Teams, NAS, Email (Google Workspaces is on Beta and due out shortly, other cloud shares planned on the roadmap).	✓	
3	No reboot, silent installation and non-disruptive to users	✓	
4	ZERO EFFORT Discovery, Classification, and Monitoring of data. 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.	✓	
5	Fully autonomous 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 – using globally accepted values) 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. You can change the value if required.		
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	Create a 'person query' to identify a specific person across private data.	✓	
19	Monitor data movement to/from Applications / Web Applications and analytics.	✓	
20	Persistent file level encryption that makes data useless unless you have Actifile installed and working on that device.	✓	
21	Offline access to data enabled to minimise disruption.	✓	
22	Deactivate and reactivate users from management dashboard.	✓	
23	Comprehensive event audit and logging.	✓	
24	Automatically encrypt all stale private data without user intervention.	✓	
25	Encrypt all data by classification (e.g. Passport, Drivers licenses, Medicare, Centrelink, Credit Card, etc).	✓	
26	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	✓	
27	All private data automatically becomes encrypted depending upon your specific requirements of what is stale data down to each classification of data.	✓	
28	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.	✓	
29	Automatic re-encryption of data when decrypted data saved.	✓	
30	Create trusted applications that automatically decrypt data as requested.	✓	
31	When a user leaves your business, and accidently 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.	✓	
32	FIPS-140-2 identification and encryption support	✓	
33	HIPPA, PCI-DOS, CMMC, PII, GDPR and more	✓	
34	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.	✓	
35	Over 40 included default file extensions and unlimited that you can simply create, to discover, classify, encrypt, search, and report on.	✓	
36	Create advanced Rules and Channels to perform almost any decryption process.	✓	

37	Automatically decrypt data sent as email option.	✓	
38	De-crypt all data in specific locations / repositories (e.g. public shared locations).	✓	
39	Define a Rule to prevent data from being deleted.	✓	
40	Define a public classification by content.	✓	
41	Define a public classification by folder.	✓	
42	Define a public classification by extension.	✓	
43	Define a public classification by channel.	✓	
44	Create a Rule to track and notify the change of a file extension.	✓	
45	Create a Rule to prevent copying of data from a removable drive to fixed drives.	✓	
46	Define a classification rule by removable device.	✓	

BONUS

- Check out www.BreachMinimisation.com for a new look at how to sell cybersecurity. All content on this website is able to be branded as your MSP organisation.