MSP SALES GUIDE

Australia and New Zealand
April 8, 2024

SELLING BREACH MINIMISATION in 2024

Cybersecurity is business critical in 2024

Today, seconds and minutes make the difference between a breach that steals your customers data, and one that is thwarted *before* it starts.

With the introduction of ChatGPT and generative AI, businesses and MSPs of all size must revisit how they deliver cybersecurity to their customers. 'Old-school' detection-based products such as AV, NGAV and EDR are no longer enough.

Modern cybersecurity solutions must enable you to transition to **Modern Breach Minimisation** cybersecurity solutions that move the focus from detecting malware to reducing the attack surface and minimizing the damage from a breach.

Ask **any** prospect these 3 questions...

- How much private and regulated data do you have in your business, where is located and which are the top 3 devices with the greatest data risk and, would you like to **make your data useless to a hacker if it is stolen**?
- How many vulnerabilities do you have in your network right now, today that a hacker can ***and will*** use to breach you? Do you know which ones are currently **actively being exploited** in the wild to remediate first?
- Does your current EDR, MDR or XDR vendor actually remediate attacks (or just alert) and if a breach occurs due to the failure of their product, will they provide **free** Incident Response - ***or do they charge you if their product fails***? Why?

ACAPacific

1 300 761 199
www.acapacific.com.au

up to:

$50m

penalty with the new Australian Data Privacy Act and Notifiable Data Breach Scheme

CYBERSECURITY IS BROKEN

- 67,000+ cyber-attacks reported to Australian government in 2022.
- 22 Australians hacked every 60 seconds in 2022.
- AI including ChatGPT, HackerGPT, and WormGPT increase threat landscape exponentially.

Why is cybersecurity STILL such as issue for all businesses

'Old School' detection-based cybersecurity products aren't enough.

- Almost every cybersecurity vendor is still focused on detecting malware and hackers.
- Detection based AV and NGAV can't stop unknown, never-before-seen, and AI generated malware.
- Most vendors are promoting EDR, MDR, XDR as an extension of traditional AV and NGAV.

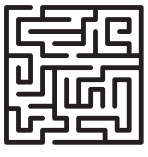
EDR, MDR, and XDR are also primarily DETECTION-based products.

- They are looking for Indicators of Compromise (IOCs) or Indicators of Attack (IOA), etc.
- The breach has potentially already occurred before they are able to identify the compromise.
- Almost all are focused on increasing the speed of discovery of the breach, alerting, remediation, or roll-back - but in most cases, you have been breached - potentially your data has already been stolen and your reputation may have been compromised and worst, you have put your customers at risk.

Dwell time is the hacker's best friend.

- The longer a hacker is in your systems, the more damage they can do - this is called dwell time. Historically dwell time as measured in weeks or months. Today, dwell time needs reduce to runtime (as a write occurs) - not in minutes or hours. 5 minutes dwell = 100,000 files encrypted - source.
- Endpoints are often the first breach point, and data is stolen so the hacker can prove they have breached your system, or potentially from that foothold, they can launch a ransomware attack.
- AI bots and skilled hackers can do enormous damage and steal lots of data in minutes, hours or days.

KEY OBJECTIVE: Hackers move to the next victim and miss your business



- **Close your doors and windows** - Make it very hard for a hacker to see you, and if they do, make it hard for them to move internally. Remediate critical external and internal vulnerabilities that are being currently being exploited first.
- **Zero Dwell Time** - You will never be able to stop all cyber-attacks, however, modern solutions reduce dwell time to ZERO so a hacker can't even get a foothold in your business. Isolate and contain all unknown objects trying to perform writes. Attackers are 24/7 & your cyber defenses need to be 24/7.
- **Secure your stale data** - if you look at most data breaches and how much old and stale data was stolen it is shocking that this stale data was not encrypted. All private data once it is no longer required should be automatically encrypted to make it useless to a hacker, and users can still access.

How much cybersecurity does a business need?

- You require enough for hacker to move to the next victim, and so that automated bots don't see you.
- A bank or Fortune 500 company will require substantially greater defenses than a business with 250, 100, 50, 25 or 2 PCs.
- **Budgets play a key role - however, it is actually RISK that should be the main criteria.**
  - What is the value of the private, sensitive, and regulated information in your business?
  - Where is it located? Which devices and users have the greatest/least risk exposure?
  - How many critical and exploitable vulnerabilities do you have right now, today in your business?
  - What is your total **DATA RISK VALUE** - this enables you make an informed decision about how much cybersecurity you require and justify the investment to secure your most important asset, your data.

Cybersecurity is similar to an insurance policy

The greater your risk, the more you should invest in a robust cybersecurity solution.

RED OCEAN Vs BLUE OCEAN

Concept from the Harvard Business Review: W. Chan Kim and Renée Mauborgne in their book, "Blue Ocean Strategy."

RED OCEAN

Highly Competitive Market

- Lots of similar competitors: AV, NGAV, EDR, MDR, XDR
- Marketing is often the biggest differentiator.
- No real major innovation = same, same, different.

BLUE OCEAN

Few Competitors: innovation

- **Breach Minimisation** solutions that focus on solving the fundamental issues at the heart of the problems with innovative technologies.
- Win new clients, grow existing customers.
- **Deliver VALUE** to your clients and prospects.
- Drive **profitable** business.

Fundamentals of Blue Ocean Selling

People need a problem to fix <u>before</u> they invest in a solution

HIGH PROBABILITY with **low** IMPACT = minimal investment

Low PROBABILITY with **HIGH** IMPACT = minimal investment

HIGH PROBABILITY of a breach + **HIGH IMPACT** of a breach = **INVESTMENT & URGENCY**

Identifying and Validating a New Client's Critical Risks

During the initial discussions with a new client, it is essential to identify and validate if they have multiple areas of critical risk. This step is crucial as it helps in determining the **probability** of a breach occurring and the potential **impact** it could have on their business. This is where you perform a **Data Privacy and Security Risk Assessment**.

By highlighting problems such as the quantity and value private data stored on devices, who has the most exposed risk, what vulnerabilities a hacker can use to breach and move internally, and even if they have potentially malicious programs hidden within their network. This helps to validate why investing in your additional security services is essential.

As a cybersecurity provider, conducting **Data Privacy and Security Risk Assessments** for your clients allows you to tailor your services to address their specific vulnerabilities and risks. By doing so, you are not only providing essential protection for their business but also positioning yourself as a trusted expert in the field.

Breach Minimisation Checklist (2024)

It can be really hard to know what to do and how much to invest when it comes to cybersecurity.

You don't want to spend too much money on something you might not need, but you also don't want your business to be the next one in the headlines. The challenge is discovering what investment makes sense for your business - ***this is where you fit in***.

You can offer enterprise grade **Modern Breach Minimisation** cybersecurity at SMB price points, so that you can help protect your clients against the latest and most damaging known and unknown AI bots, cyber threats and attacks. You are now able to help close your clients' doors and windows and help secure their private data to make it useless to a hacker, in the event that it is stolen.

Do your cybersecurity products deliver the following capabilities:

YES	NO	REDUCE YOUR DATA RISK VALUE BY OFTEN UP TO 96%
		Automatically **encrypt stale** regulated data at the **FILE LEVEL** to make that data useless to a hacker even after a breach and the data is stolen. You can reduce your data risk by typically 90% to 96%.
		Discover old and new (as it created) private, sensitive, and regulated data across **endpoints** including PC's, servers and **cloud** environments including SharePoint, OneDrive, and Network Attached Storage.
		Classify data by category (e.g., PII, PHI, PCI, Passport, Drivers License, Medicare, TFN, etc.)
		Quantify how many files by each classification and monitor how data flows in and outbound.
		Provide a **DATA RISK VALUE** by file, classification, and user to help determine your risk profile.
		Identify the most exposed users with the highest risk if they were breached.
		Users can automatically decrypt files with a normal 'double click' to reduce user friction.
		Create rules to automatically decrypt data as it flows to an application/cloud without manual intervention.
		VULNERABILITY MANAGEMENT - CLOSE YOUR DOORS AND WINDOWS
		Perform daily **external** vulnerability scans to identify exploitable holes in your perimeter defenses.
		Perform continuous or near continuous **internal** vulnerability scans looking for newly discovered vulnerabilities across Windows, Mac's, IOT devices, Active Directory, firewalls, and applications.
		Build remediation plans for vulnerabilities to enable your IT team to remediate as quickly as possible.
		Discover newly added devices to the network and determine if and what vulnerabilities they have.
		Map/track vulnerabilities over time.
		Determine patch status of operating systems and applications on a daily, weekly, and monthly basis.
		Produce compliance reports including PCI, CIS, NIST, HIPPA, ESSENTIAL 8, and ISO 27002.
		DELIVER ZERO DWELL TIME TO PREVENT DAMAGE FROM HACKERS
		Reduce dwell time of unknown objects to zero and help prevent unknown objects (including .exe, PDF, Word, Excel, JSON, Python, PowerShell scripts, etc.) from writing to the disk, COM interface & Registry until they are **KNOWN SAFE.**
		Examine unknown payloads in real-time (24/7) with humans (as required) and determine if SAFE or MALICIOUS.
		In most cases allow the user to safely interact with contained payloads without risk of infecting of that endpoint or the network.
		24/7 THREAT HUNTING WITH REMEDIATION FROM GLOBAL SOC
		24/7 threat hunting across endpoints (MDR) by a global SOC (Security Operations Centre) team of security experts. includes remediation (where possible).
		Optional XDR (including SIEM) with Remediation of threats across **network** (where possible) by the 24/7 security experts at the SOC centre.
		Incident Response is included with MDR and XDR solutions to highlight the confidence in stopping damaging malware.

CURRENT AV COST PER ENDPOINT: $_____ **QTY CRITICAL / TOTAL VULNERABILITIES: ____/_____**

CURRENT DATA RISK VALUE: $_____ **MOST EXPOSED DEVICE: _____ with $_____ RISK**

POSITIONING SOLUTIONS

Even though you are selling the same solutions to new clients and existing customers, it is important to understand the subtle differences in positioning them. For new clients it is about highlighting the failings of their existing supplier and with existing customers, it is showing them how you have matured into a security specialist, and you can continue to protect them against even the latest AI driven cyber threats.

NEW CUSTOMER

VS

EXISTING CUSTOMER

Identify Data RISK

Our first step is to understand your private, sensitive, and regulated data. How much you have (it is always more than people think).

We then classify it and then we put a value on your data. We tell you who has the most risk exposure if they are breached.

Then we can encrypt the stale data so if a hacker steals it, it is useless and worthless to them.

DATA PRIVACY

- Discover private data.
- Quantify the risk and its value.
- Monitor in/outbound data.
- Encrypt (secure) stale data.
- Decrypt as required.

Make stale data useless to a hacker, even after it is stolen.

New Revenue Stream

Deploy Actifile to all endpoints in all your clients. Start with the three clients with the largest risk values, the next 3 and so on until you include in all client QBRs.

"We are providing a new service that helps to reduce our customers risk by typically up to 96% by using autonomous AI technology to automatically encrypt your private data as it becomes stale to make it useless and worthless to a hacker - even if it is stolen!"

Easy to Breach?

Vulnerabilities are essentially holes in applications.

86% of cybercrime is bot driven. 60% of breaches exploit known vulnerabilities - most of which have available fixes or patches. With an average of 72 new vulnerabilities per day - that is over 2100 per month, it is crucial to provide daily or at least weekly vulnerability remediation.

*How many vulnerabilities do you have in your network right now that a hacker can **and will** use to breach you?*

VULNERABILITITY

- Discover all devices added to the network.
- Identify new vulnerabilities continuously.
- Prioritise which are being exploited.
- Remediate these ASAP.
- Validate that remediation has worked.

Close your doors and windows to make it hard for a hacker to even see you or move internally.

New Revenue Stream

*Included in our standard MSP package is **OS** vulnerability remediation every [month /quarter].*

With AI driven bots attacking 24/7 and accounting for 86% cybercrime and 72 new vulnerabilities per day, and malicious AI increasing we now STRONGLY recommend daily or at least weekly remediation across applications and operating systems...

Our daily remediation service is only an extra [$x.xx] or weekly only [$x.xx] pm per endpoint.

Zero Dwell Time

One key metric that is used by modern cybersecurity is to measure the effectiveness of cybersecurity is dwell time – the amount of time that a hacker or malware remains undetected within a system. The longer the dwell time, the greater the potential for damage and data breaches.

Our goal is zero dwell time so malware can't even get a foothold into your business.

ZERO DWELL

Reduce dwell time to ZERO at runtime:

- isolate unknown objects.
- Examine safely with AI, ML & humans
- User can (normally) interact during examination process.

Does your current cybersecurity vendor include FREE Incident Response if you are breached because their product failed?

New Revenue Stream

*In order to reduce the damage that new AI based malware can do, we now have the ability to deploy 24/7 MDR that includes ZERO DWELL CONTAINMENT technology that helps to stop the damage caused by traditional and **unknown, never-before-seen** malware.*

This is a critical upgrade and needs to be deployed urgently - the additional fee is [$X.XX] per month per endpoint - we have scheduled in deployment for next Tuesday at 10:30am - is that OK with you?

Affordable SOC / SIEM

Automated BOTS and hackers are 24/7, and all businesses, regardless of size need affordable 24/7 threat hunting to keep you safe. If a hacker breached you at 1am, they could steal all your data by 8am - we help prevent this!

24/7 THREAT HUNTING

- Real-time, always-on EDR and MDR SOC.
- 24/7 hunting for hackers and malicious code.
- Optional **network** threat hunting upgrade.
- Remediate in realtime, even at 1am
- Includes FREE Incident Response (IR)

New Revenue Stream

*86% of cybercrime is now bot driven and bots are relentless and 24/7, and we now **need** to deliver 24/7 threat hunting to keep you safe. If a malware breached you at 1am, it could steal all your data by 8am.*

We now have a global SOC that delivers 24/7 threat hunting to keep eyes on your businesses, even whilst we are sleeping it is only an extra [$xx] pm/endpoint.

SIMPLIFIED sales process

1. **IDENTIFY** their **Data RISK Value**, and which devices are most exposed = **IMPACT**
2. **PROVE** the quantity of **vulnerabilities** that they have that hackers can use = **PROBABILITY**
3. **EDUCATE Dwell time** and attacks are now 24/7 and always-on **threat hunting** is critical = **URGENCY**

COLD CALL A NEW PROSPECT

Use the cold calling scripts as templates

Success is typically based upon the prospect agreeing to an assessment so that you can show them in black and white:

- Actifile: How much private & regulated data they have, where it is located, its value and who is at the highest risk.
- ConnectSecure: Run a full scan to identify key issues and quantity vulnerabilities that a hacker can and will use.
- Xcitium: Leverage the Unknown File Hunter tool to scan and identify any unknown files, including malicious ones.

HIGHLIGHT THE CYBERSECURITY ISSUES THEY HAVE RIGHT NOW AND EASE OF A BREACH

Perform a Data Privacy, Security and Risk Assessment

Use the tools in the Sales Guide to help illustrate and show the client the risk they have right now, today:

- Actifile: (impact) - identify, classify and quantify the amount and value of private and regulated data on selected endpoints.
- ConnectSecure: (probability) Qualify how easy they are to breach by discovering vulnerabilities and gaps in their network.
- Xcitium: (urgency) discover any unknown files (and malware) lying in wait across their network.

BUILD THE JUSTIFICATION / PROPOSAL

Highlight the urgency to remediate ASAP

Scaring people is not a good sales strategy. Educate your client about the new era of threats post ChatGPT and AI and help them understand that old school AV, NGAV and EDR is not enough. Show them in printed form just how at risk the actually are. **WATCH THIS 15 MINUTE VIDEO** (https://vimeo.com/894405252). **KISS** - keep your data simple and easy to understand - forget jargon - use plain English (Insurance is a great analogy for all three solutions)**.**

LAND AND EXPAND

Cybersecurity is a journey, not a destination

During your conversations discuss the Australian Government **Essential 8** prevention-based suggestions to improve cyber defenses. Depending upon the data risk discovered, and the critical vulnerabilities leaving the doors and windows wide open today for a hacker to walk through, this should be a simple upsell opportunity. Education in plain English is critical.

Other key information to identify to help justify the new budget:

- What is their turnover, and what would 10 days downtime cost them in real dollars (salaries, downtime, customers, etc.)?
  - - If their turnover is greater than $3m - it is **mandatory** to comply with the new Data Privacy Act & NDBS.
- When did they last do a **FULL DR** test of servers and **endpoints** to see how quickly they could recover from a ransomware attack or if they had a catastrophic disk failure on a production server?
- If customers private data was leaked on the dark web, and breaches occurred because of them, what impact would that have on the customer (financial and reputational)?
- What is the Average Customer Value ($/annum/customer), and how many customers would they lose after a major breach? How easy is to replace those customers lost?
- What about the reputational damage - in certain industries they are substantial.
- Do they fall under any compliance regulations, for example HIPPA,

For critical infrastructure, regulated industries and larger organizations, also consider advanced solutions such as 24/7 XDR, network segmentation, supply chain analysis and more.

If an MSSP approached your customers and ran through this process -
HOW WOULD YOUR CUSTOMERS REACT?

CONCEPTUAL ONE PAGE OVERVIEW

1. **IDENTIFY** their **Data RISK Value**, and which devices are most exposed = **IMPACT**
2. **PROVE** the quantity of **vulnerabilities** that they have that hackers can use = **PROBABILITY**
3. **EDUCATE Dwell time** and attacks are now 24/7 and always-on **threat hunting** is critical = **URGENCY**

Note: the following image was created from powerpoint is is not a standard report available

$225k
REGULATED DATA

Sample size: 5 devices:

- 82,312 files
- 53,373 PII files
- 315 VISA Credit Cards
- 442 Medicare records
- 4 Passport numbers

Device Name	Risk Valuation	Files	Sensitive files
IANASUSLAPTOP	$189,260	8274	3827
ANDRIA-YOGA	$32,410	17068	540
SKYNET-LAP-T470	$3,602	577	29

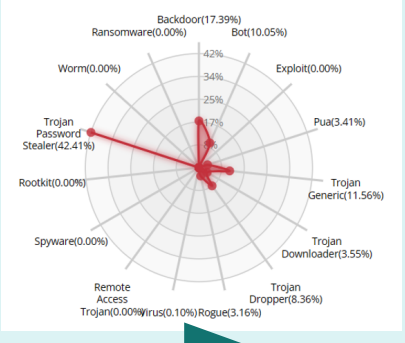
184
VULNERABILITIES

Sample size: 26 IP Devices

- 17 Critical (3 urgent)
- 37 High Importance
- 130 Medium/Low
- 3 ports open

2
HIDDEN MALWARE

- 1 x Remote Access
- 1 x Password Stealer



Which problem would you like us to fix first?

Suggestions

- Perform daily tracking and monitoring of private data.
- Monthly reports on changes.
- Encrypt files as they become stale to reduce your data risk value and to help make them worthless to a hacker.

Suggestions

- Perform daily or at least weekly vulnerability assessments.
- Remediate ones being exploited in the wild within a max of 3 days.
- Resolve critical in 7 days.

Suggestions

- Deploy a Zero Dwell solution.
- implement 24/7 threat hunting urgently.
- Put in place an Incident Response process.

If an MSSP approached your customers and ran through this process
HOW WOULD YOUR CUSTOMERS REACT?

Calling existing customers

Objectives:

- **PROBABILITY**: AI has changed the threat landscape and automated bots are the major cybersecurity threat to SMBs.
- **IMPACT**: You can deploy a Data Risk Platform to help them make an informed decision of how much security they require which is typically only 1% to 3% of their data risk value (Run Actifile across the client).
- **URGENCY**: You have invested in building modern solutions to fight these new and critical threats, and it is urgent to deploy ASAP to help keep them safe.

Hi [First Name],

Globally AI (e.g. ChatGPT) has transformed how hackers attack and breach. 86% of cybercrime is bot driven and these attacks are now as sophisticated as human led attacks - that means traditional, or 'old school' detection-based AV, NGAV and EDR products simply can no longer stop these ever-increasing sophisticated attacks. In order to help keep you secure; we have put in place a 3-stage process to modernise your cybersecurity defenses and deliver **Breach Minimisation** solutions.

In 2022, 22 Australians were getting hacked every 60 seconds. Can you believe that? Then in 2023, there were over 76,000 attacks **reported** to the Australian government, and with more than 26,447 new security vulnerabilities discovered - that is 72 per day, we need to dramatically change how and what we are doing to help keep you safe and secure.

But here's the thing - we're not here to scare you. We're here to help. We understand the importance of protecting your business, which is why we've developed a multi-stage methodology to help ensure your security while keeping costs low.

The single biggest challenge is that hackers - well actually automated bots, are now 24/7 and we have invested in Modern Breach Minimisation technologies that reduce the risk of a hacker breaching your business.

First, we'll start by identifying the value and location of your private and sensitive data. This will help us provide us with a benchmark of how much security we need. Then, we'll "close your doors and windows" to make it very difficult for hackers to get in. Finally, as hackers are now 24/7, we'll provide you with round-the-clock 24/7 security platforms (if needed), including data encryption, so even if hackers do manage to get in, they won't be able to use your stale private data.

Now, typically, the investment for these three stages falls within 1% to 3% of the value of your data. We want to start implementing the first two stages as soon as possible. The first stage, called the Data Discovery layer, is foundational to all the other measures we'll take. It is only [$X.XX] per endpoint per month for the Data Privacy Platform software license. Plus, we can perform a Vulnerability and Security Assessment for just an extra [$1.50] per IP device per month, so we can then determine the investment for remediating the vulnerabilities and the frequency required.

We're aiming to start the deployment and assessment next Tuesday or Wednesday - would you like us to do just the data discovery, or include the vulnerability platform as well?

Once we have these initial stages in place, we can make further decisions on what other actions we need to take. This could include zero dwell containment, encryption, vulnerability management, security training, anti-phishing measures as other solutions as recommended by the Australian Government's Essential 8. But let's discuss these in more detail during our next QBR, once we have more data to work with. Are we good to schedule your deployment for next week?

TYPICAL OBJECTION: *I thought you were already protecting us*!

Yes, absolutely we are - which is why you haven't had any breaches so far. The landscape is rapidly changing with government regulations, insurance requirements and quite simply the fact that hackers, AI and bots are far more skilled and focused on small business than ever before. It is critical to improve cyber defenses to help ensure we continue protecting you, which is why I am calling you. We now have tools that historically have only been available to large organizations - our goal is to continue to deliver high value and low-cost solutions to secure you - Lets first start with a Security and Risk Assessment to get a baseline - that is [$XX / EP].

Cold calling (new) prospects...

Objective:

- **PROBABILITY**: Prove to the client they are 'easy' to breach due to exposed external ports and internal vulnerabilities - perform a ConnectSecure Risk Assessment.
- **IMPACT**: Demonstrate to the client the value, quantity and location of private, sensitive, and regulated data they have in their business. Download the Actifile QuickStart Guide and set up your Actifile MSP account today.

High Value, low cost

Suggested call script

Good morning/afternoon, my name is [Your name] from [your company], we are a cybersecurity specialist that is focused on cost-effectively making it very hard for a hacker to see and breach your business using the latest modern **Breach Minimisation** solutions.

We see most small businesses believe they are too small to be targeted, and this is correct. You probably will not be **targeted** as they would target a bank.

However, 86% of cybercrime is now bot driven thanks to generative AI. The attacks are global, relentless and non-stop. The challenge is that small business typically doesn't have the same resources as large enterprises, hence they are 'low hanging fruit' for hackers and their automated AI driven bots. AV, NGAV and EDR products quite simply are not enough anymore.

They don't care if you have 2 or 250 PC's. All they want is to cause disruption, so you pay a ransom demand.

As a **security** specialist to small businesses, our goal is simple, we help you to identify if you have risks, and then cost-effectively provide modern **Breach Minimisation** cybersecurity solutions for typically only 1% to 3% of your Data Risk value.

We have a powerful 3 step process:

- **First**, Let's discover your vulnerabilities - which are basically holes in applications that a hacker can **and will** use to breach your business and steal your data. If your existing IT team is doing a great job, it is a great endorsement for their skills, however, if like many businesses, you have your doors wide open, so that a hacker can walk right in, you need to be aware of that before the automated bots discover you. Think of this as a broken lock on your front door, or even worse, you leave your front door wide open when you go out.
  - **Question for them to ask internal IT**: *How many critical vulnerabilities do we have in our network right now, today?*

- **Second**, we perform a Data Risk Assessment that looks at how much regulated, private, and sensitive data you have on either a handful of devices, or we can perform a complete scan across all devices, SharePoint, OneDrive and network attached storage. This is similar to your home insurance - how much are your contents worth, are you in a flood or bush fire risky area, or perhaps you live in a high crime area - all these will impact the cost of your insurance premium.
  - **Question for them to ask internal IT:** *What is the value of our private data, and who are the top 3 people with the greatest data risk exposure if we are breached?*

- **Third**, we then make recommendations for your IT team, or existing MSP to close your doors and windows to make it exceptionally hard for a hacker to breach you, so they simply move to the next victim – this is normally 1% to 3% of your Data Risk Value (discovered in phase 2). If required, we can also assist with or even a quote on remediating the issues that have been identified if your team needs a helping hand.
  - **Question for them to ask internal IT:** *If you get breached at 1am, how do you stop a hacker stealing all your data by 8am?*

How much do you charge?

Our goal is to identify if you have a problem, the extent of the problem and make recommendations to fix the problems. We normally charge 1% to 3% of the Data Risk value. In fact, we are so confident that we can help you - will conduct the initial Data Risk and Security Risk assessments free of charge. If you are secure, it is a great peace of mind, if you have gaps, we would like the opportunity to quote on working with you as a security expert, focused on helping you to reduce the risk of a breach.

helping to 'hide' you from hackers

So the hacker simply move to the next victim, not yours

Of course, you don't actually become invisible, however, as we close your doors and windows it becomes very difficult for a hacker to even see you.

OVERCOMING OBJECTIONS

Put yourself in your prospects shoes:

We are too small, no one is going to target us!

Correct - as an SMB/SME it is automated bots that are the greatest threat. In fact 86% of cybercrime is bot driven and 60% of breaches use known vulnerabilities to infect and steal data.

Businesses must move beyond traditional 'old school' AV, NGAV and EDR products to low cost-high value modern Breach Minimisation solutions that are designed to exponentially reduce the risk of a breach and its damage.

We don't have any regulated data!

That is what most of our customers thought until we performed a data risk audit. They were shocked to find that users had substantial data on their devices!

In fact, in minutes we could show them who is at most risk, the quantity and even the value of regulated data. It is a painless process, and no reboot is required.

We also identify how many critical vulnerabilities you have, because that is how a hacker or automated bot is going to breach you and steal your data.

We already have an IT Team or MSP!

Our Data and Secuirty Risk Assessment will help to give you complete peace of mind knowing that they are doing an outstanding job.

In fact, feel free to ask them just 3 questions:

- How many vulnerabilities do we have right now, that a hacker can use to breach us?
- Which PC's have private and sensitive data on them, and what is our total Data Risk Value?
- If we are successfully breached at 1am tonight, does your current cybersecurity vendor provide FREE Incident Response (repair)? Why not, if the breach is due to a failure in their product, shouldn't they help fix it?

What does it cost - we dont have any budget!

It's difficult to know exactly how much cybersecurity is enough. You don’t want to be the next victim in the news, but you don’t want to spend money unnecessarily either.

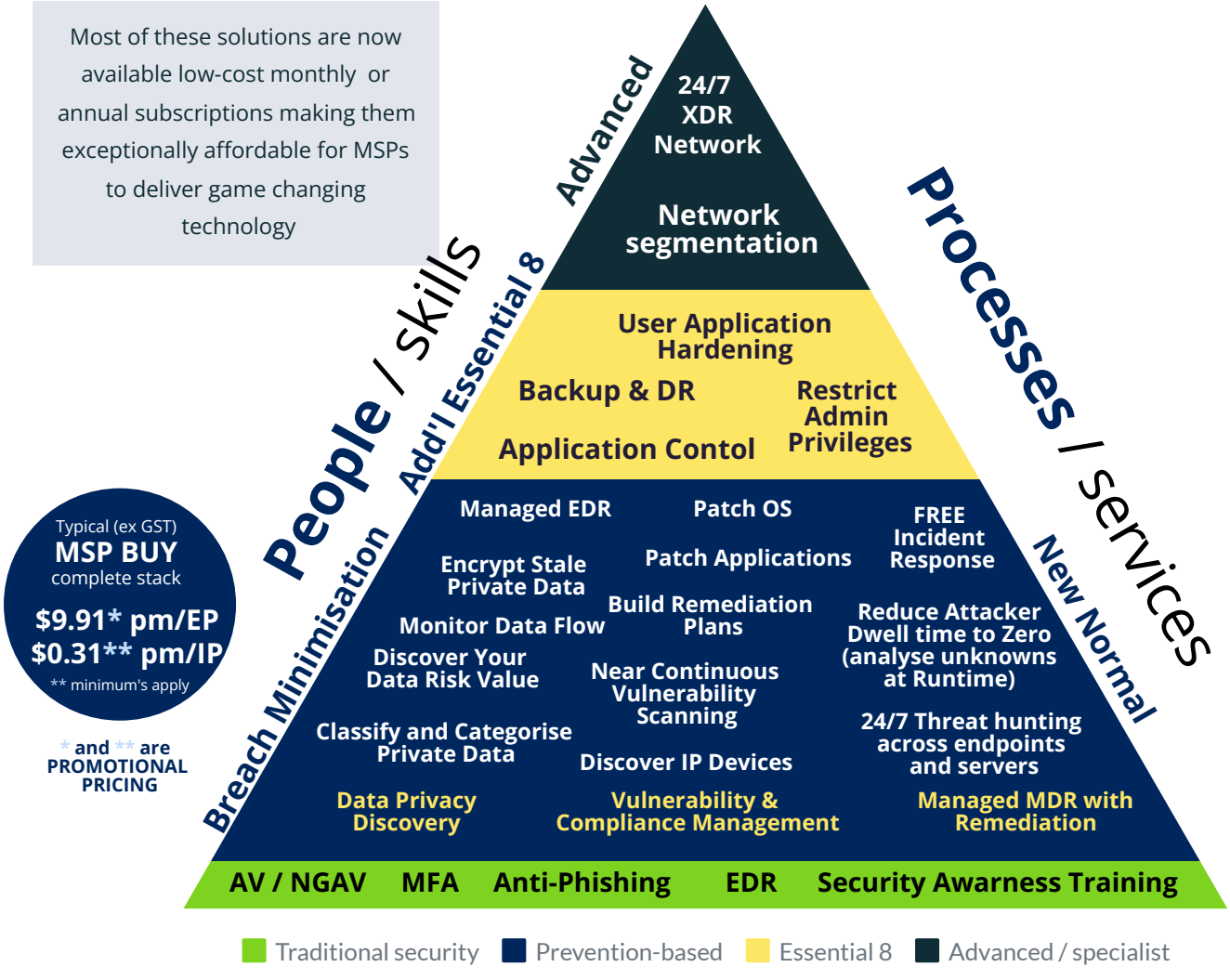
Our Data Privacy and Risk Assessment evaluates your network's security posture to determine how much regulated data you have and the likelihood of a cybersecurity breach.

The good news is that a full Breach Minimisation Platform is typically between on 1% to 3% of your data risk value - as the more private data you have, typically the more comprehensive the solutions you require - but let's first see the value of your data and if you are wide open and exposed to hackers and automated bots breaching you.

Breach Minimisation Stack (2024)

Traditional core products - typically detection-based are fundamental to basic security
Breach Minimisation - these are now considered CRITICAL and **MUST HAVE in 2024**
Essential 8 stack - these are important (some overlap) and highly recommended
Advanced / specialist - typically more expensive technologies for mid to large businesses

Most of these solutions are now available low-cost monthly or annual subscriptions making them exceptionally affordable for MSPs to deliver game changing technology



Technology / software

Once you discover a client's risk exposure (Actifile) and the fact that they have lots of vulnerabilities (ConnectSecure), it is relatively straight forward to build a **Breach Minimisation** plan that reduces their risk and their attack surface with 24/7 threat hunting to reduce dwell time to zero (Xcitium) and do it for typically 1% to 3% of their data risk exposure.

Your goal is to 'hide them from hackers' so a hacker moves on to the next (easier to infect) victim. These solutions help to make it very hard for a hacker to see them, identify how to breach them, and steal their data. This dramatically reduces their risk of a breach and the negative impact of a ransomware attack or stolen private and sensitive data on them and their customers.

No one can guarantee you will never be breached; your goal is making it so hard the hacker that they simply move to the next victim as your customers are too hard to breach - this is called **Modern Breach Minimisation** technology.

A complete Breach Minimisation cybersecurity solution set for typically only 1% to 3% of Data Risk Value

ASD ESSENTIAL 8

a very basic overview

The Australian Government recognises that cybersecurity is a major threat to all Australians and have developed the ESSENTIAL 8 - a guideline for prevention-based security to reduce the risk of a breach.
Each of the 8 controls has 4 levels of maturity (0 = minimal to 3 = very secure)

01 Application Control

Xcitium blocks unknown objects and payloads from being able to write to the disk. **ConnectSecure** tracks all applications installed, removed and can create an Application Baseline of mandatory and denied applications.

02 Patch Applications

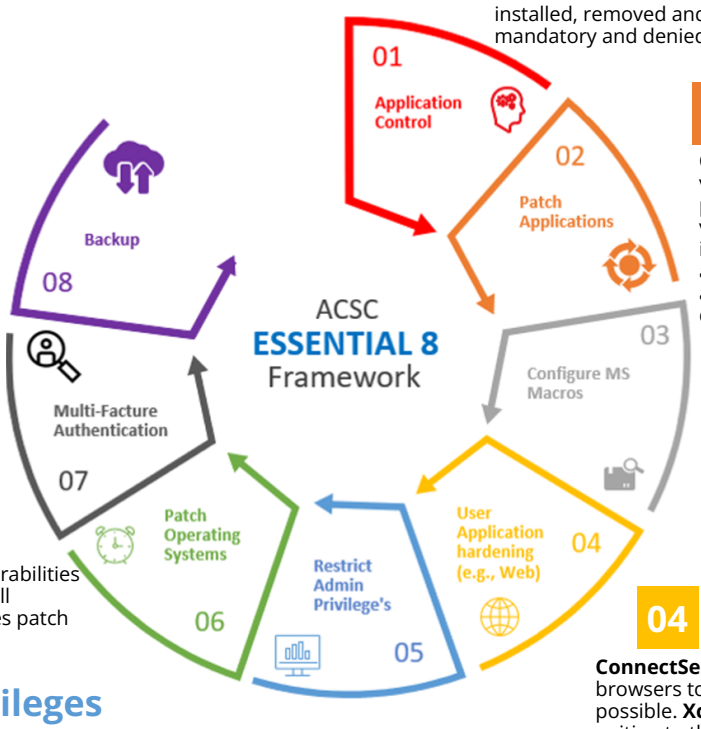
ConnectSecure is a near continuous vulnerability management platform that performs a multitude of comprehensive vulnerability scans including external, internal, AD, Azure, Network, application and devices. It now also includes application security patching. **Xcitium** also delivers application patching.

03 Configure Macros

Xcitium blocks unknown and malicious executables running from macros and writing to the disk. All unknown writes occur to a secure virtual environment that normally allows users to interact with the macro in complete safety while the file is being examined by AI, ML or hurmans.

04 User App Hardening

ConnectSecure will identify in real-time vulnerabilities in browsers to enable IT teams to remediate as quickly as possible. **Xcitium** blocks unknown executables from writing to the disk and Microsoft can be configured to further harden browsers.



08 Backup

or, more importantly, **RECOVERABILITY** of servers and desktops. Recoverability must be tested on a regular basis and they must be **AIR-GAPPED.**

07 MFA

There are multiple MFA products available, including from **Microsoft**. For network, system administrators and 'high value targets', you should strongly consider hardware MFA such as **Yubikeys**.

06 Patch OS

ConnectSecure continuously discovers vulnerabilities on all major OS's and now the PRO version will remediate OS vulnerabilities. **Xcitium** includes patch management across Operating Systems.

05 Restrict Admin Privileges

Microsoft can be configured to help reduce the risk.

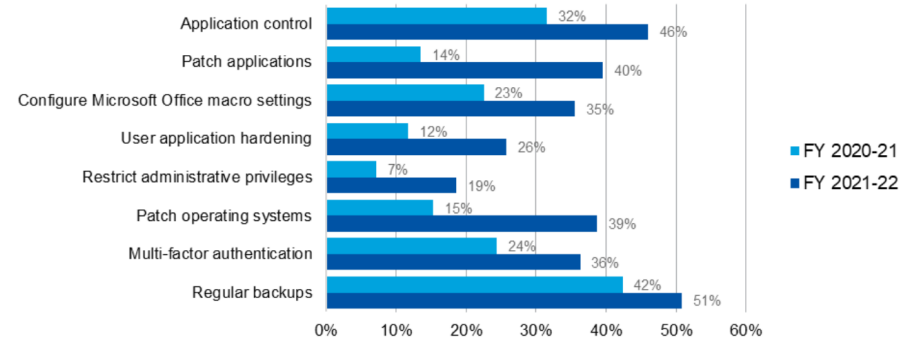
The Essential 8 are not mandatory for most businesses, but they are **strongly recommended** to help prevent breaches and data theft.

Most of these are able to be configured within Microsoft. The tools listed above (plus other tools) complement the capabilities and make deployment and management much less expensive.

.

How do you compare?

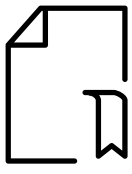
Figure 1: Percentage of entities with Essential Eight Maturity Level 2 or higher (Essential Eight strategies only)



https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2022

Breach Minimisation solutions are required to help fight the onslaught of automated cyber-attacks. Allocate a budget of typically between 1% to 3% of data risk value (www.actifile.com)

TRIO OF POWER SOLUTIONS



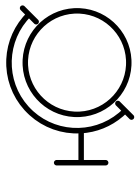
DATA PRIVACY PLATFORM

If a hacker breached you right now, what private and sensitive data could they steal from your executives' laptops or your servers?

Discover data
Monitor movement
Auto encrypt when stale

CLICK for 60-sec DEMO

actifile



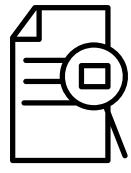
VULNERABILITY PLATFORM

How many vulnerabilities do you have in your network right now, today that a hacker can and will to breach your business and steal your data?

Discover vulnerabilities
Prioritise remediation
Remediate rapidly

CLICK for 60-sec DEMO

CONNECTSECURE



24/7 THREAT HUNTING

If a hacker successfully breached you at 1am tonight, how much data could they steal by 8am?

ZERO DWELL TIME
Global SOC
EDR/MDR/XDR

CLICK for 60-sec DEMO

xcitium

Build Your own **Breach Minimisation Plaform**

Next steps?

actifile

www.**Actifile**.com

then, download the QuickStart Guide including set up free trial:
www.acapacific.com.au/Actifile QuickStart

To benefit from special A/NZ 100 IP pack
Create your FREE TRIAL Account:

- **https://acapacific.com.au/ConnectSecureTrial**

CONNECTSECURE

www.connectsecure.com

xcitium

www.**Xcitium**.com

To benefit from special A/NZ pricing for Xcitium please:

Signup for a free trial of Xcitium:

- https://platform.xcitium.com/signup/?af=18152&fr=1&pa=1
- (Select Region: **US** and then **MSP**)

Then email **Sales@Xcitium.com.au** with your **Account Admin email address**
(Go To: MANAGEMENT > Staff> Account Admin)

ACAPacific

www.acapacific.com.au

Distributor for Australia and New Zealand

- ConnectSecure - Vulnerability
- Actifile - Data Privacy
- Xcitium - Cybersecurity
- Entrust - Identity & Certs
- Redstor - Backup
- ArcServe - Backup
- SonicWall - Firewall