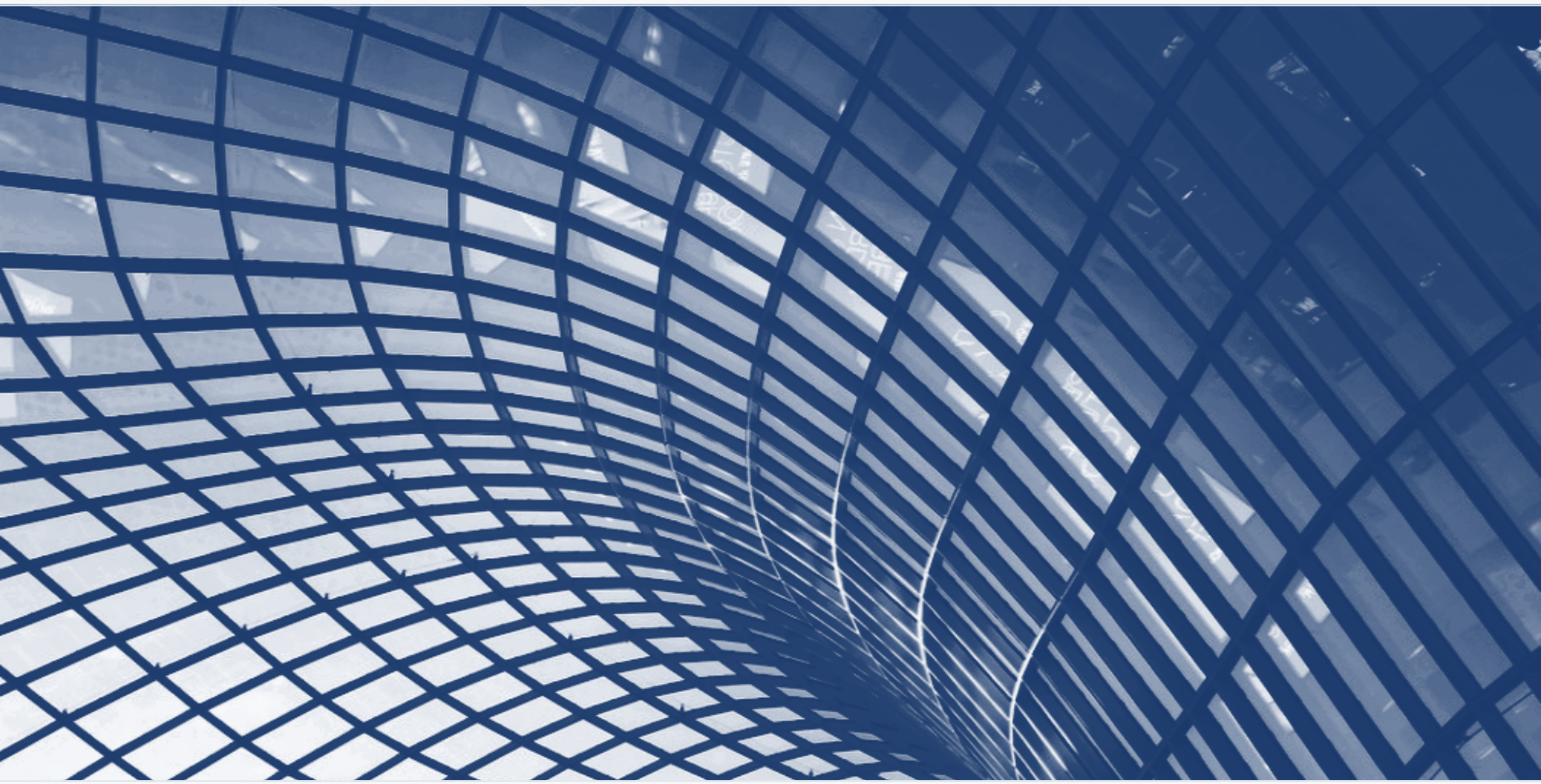
VYFORITY

Cyber security and business architecture advisory

The Microsoft Reset for Care Providers

What the 2025 nonprofit grant retirements and the July 2026 price event mean for your organisation, and the security you already own.

A plain-language guide for CEOs, CFOs and boards of not-for-profit care providers.



THE SHORT VERSION

Three things are true at once for most care providers: their Microsoft costs are rising, they are paying third parties for security tools their Microsoft entitlement already includes, and they are not using the security capability they are entitled to. Fixing the three together is the reset.

Dean Kastelic · Founder, Vyfority · former enterprise CISO

JULY 2026

INTRODUCTION

Why this guide exists

If your organisation is a not-for-profit care provider (palliative care, community health, aged care, disability, mental health or community services), your Microsoft licensing changed category in the last twelve months, or it will at your next renewal. Most providers found out from an invoice.

This guide explains what changed, why it is a security decision and not just a cost decision, and how providers are restructuring their licensing so the security uplift is funded by spend they recover rather than new budget. It ends with a twelve-point self-check you can complete in fifteen minutes with your IT manager or managed service provider.

It is written for the people who own the outcome: chief executives, finance leaders and boards. Plain language throughout. No product brochure, no jargon that needs an interpreter.

01

What changed, and when it hits you

Microsoft restructured its nonprofit program in 2025. Two long-standing free grants, Microsoft 365 Business Premium (the ten-seat grant) and Office 365 E1, were retired effective 1 July 2025. Because the change applies at each organisation's renewal date rather than all at once, providers have been hitting it progressively ever since, and many will feel it for the first time at their 2026 renewal.

What remains is still substantial: eligible nonprofits keep access to up to 300 free Microsoft 365 Business Basic licences, and discounts of up to 75 per cent on paid plans, including Business Premium and the enterprise E3 and E5 suites.

Two further events are now in view. Microsoft has flagged suite packaging changes from June 2026 and global pricing updates from July 2026. The nonprofit discount percentage continues, but it applies to the updated base price, so the dollar cost moves even where the discount does not.

WHEN	WHAT HAPPENS
1 July 2025	Free Business Premium and Office 365 E1 grants retired. Applies at each organisation's next renewal after this date.
Through 2025–26	Providers hit the change renewal by renewal. Licences that do not renew must be transitioned manually; organisations that did nothing saw users lose access.
June 2026	Microsoft suite packaging changes begin rolling out.
July 2026	Global pricing updates take effect. Nonprofit discounts remain but apply to the new base prices.
Still available	Up to 300 free Business Basic licences; discounts of up to 75% on Business Premium, E3, E5 and other paid plans (eligibility verified by Microsoft).

The reflex response, downgrading everyone to the free Basic tier, is where the security problem starts. That is the subject of the next section.

02

Why this is a security decision, not a licensing chore

Business Basic is free, and for some roles it is exactly right. But it does not include the device management, endpoint protection, conditional access or data-loss-prevention capability that sits in Business Premium and the E suites. An organisation that downgrades its workforce wholesale to save money has quietly removed the controls that stood between a stolen password and its client records.

For a care provider, the stakes are higher than for a typical small business of the same size, for four reasons.

The Privacy Act applies to you at any size. The small-business exemption does not apply to health service providers. A provider holding health information carries the full Australian Privacy Principles obligations regardless of turnover: the same core obligations as a hospital.

Your data is as sensitive as data gets. Clinical notes, care plans, family circumstances, financial hardship: the records of people at their most vulnerable. The reputational consequence of a breach is existential for an organisation that runs on community trust and government funding.

Ransomware reporting is now law for many providers. Organisations with $3 million or more in annual turnover that make a ransomware payment must report it within 72 hours under the Cyber Security Act 2024. It is a civil penalty regime, and a question your board should be able to answer before an incident, not during one.

Your board carries the duty. ACNC Governance Standard 5 places duties of care and diligence on responsible persons. Information and cyber risk sit inside that duty, and volunteer directors are rarely briefed on it until something goes wrong.

> THE GOOD NEWS
>
> None of the above requires new spending to address in most providers. The capability usually already exists inside the licensing you hold or are about to pay for. What is missing is architecture: deciding who needs what, switching the controls on, and retiring the duplicates.

03

The security stack you already own

The discounted Microsoft plans are not just email and Office applications. Business Premium and the E suites include a genuine enterprise security stack (the same product families used by banks and hospitals) that most providers have switched on only partially, if at all.

CAPABILITY (INCLUDED)	WHAT IT DOES IN PLAIN TERMS
Entra ID: MFA and conditional access	Multi-factor authentication for every account, and rules like "clinical records only from managed devices" or "block sign-ins from overseas". The single highest-value control against account takeover.
Microsoft Defender	Endpoint and email protection: antivirus, phishing and malicious-link defence, attack detection. The category most providers also buy separately from a third party.

CAPABILITY (INCLUDED)	WHAT IT DOES IN PLAIN TERMS
Intune	Device management. Requires a PIN, encryption and up-to-date protection before a laptop or phone can touch client data; remotely wipes lost devices. Essential for mobile and community-based workforces.
Purview	Data loss prevention and retention: rules that stop client health information leaving by email or Teams, and records retention aligned to your funding and clinical obligations.
Privileged access (E5 / add-on)	Time-limited administrator rights, so a compromised IT account is not the keys to everything. Relevant for the small number of privileged and clinical-systems roles.

A capability you are entitled to but have not configured protects nothing. That is why the reset is an architecture exercise, not a procurement one: the licence is the raw material, not the outcome.

04
Right-sizing: the three-tier model

Microsoft allows organisations to mix licence types across their users, and this is where both the savings and the security live. The wrong models are the two extremes: everyone on the free tier (cheap, exposed) and everyone on a premium tier (secure on paper, and paying for capability half the workforce never touches). The pattern that works for care providers is three tiers matched to role risk.

TIER	WHO	WHAT
Foundation (free)	Volunteers, casual and short-tenure roles with no access to client records or finance systems	Business Basic: email, Teams and web Office at no cost, inside the 300-licence grant
Core (discounted)	The general workforce: care coordinators, administration, rostering, most clinical support	Business Premium: the full security stack in Section 03, at nonprofit pricing
Privileged (discounted)	IT administrators, executives, finance, clinical-systems owners: the small group whose accounts unlock everything	E5, or E3 with security add-ons, adding advanced identity protection, privileged access management and deeper audit

Getting the tiering right typically moves a meaningful share of seats down a tier while moving a small number up, and the licences it frees usually fund the difference. The exact split is discovered, not assumed: it comes from an entitlement-versus-usage audit, which is a two-day exercise, not a project.

05
The overlap list: what you may be paying for twice

Almost every provider we look at is paying at least one third party for a capability their Microsoft entitlement already includes. These tools usually arrived one at a time over years, each solving a real problem at the time. Nobody is at fault, but nobody has mapped them against the entitlement either. Common overlaps:

THIRD-PARTY SPEND	INCLUDED ALTERNATIVE	CAVEAT
Standalone antivirus / endpoint protection	Microsoft Defender (Business Premium and above)	Verify coverage for any servers and specialist clinical devices first
Separate MFA tokens or apps (per-user subscription)	Entra ID MFA and conditional access	Plan the cutover; never run a gap between old and new
Email archiving and continuity service	Purview retention and Exchange native capability	Confirm your funding-body and clinical retention periods are configured before decommissioning
Mobile device management platform	Intune	Pilot with one team before fleet-wide enrolment
Secure file-sending / large-file tools	OneDrive and SharePoint sharing with DLP policies	Configure DLP first, or you have convenience without control

Two honest cautions. First, not every overlap should be killed: occasionally the third-party tool is genuinely better for a specific need, and the right answer is keeping it deliberately rather than by inertia. Second, decommissioning is sequencing work: the replacement control must be configured, tested and adopted before the old tool is switched off. The saving is real, but it is earned in that order.

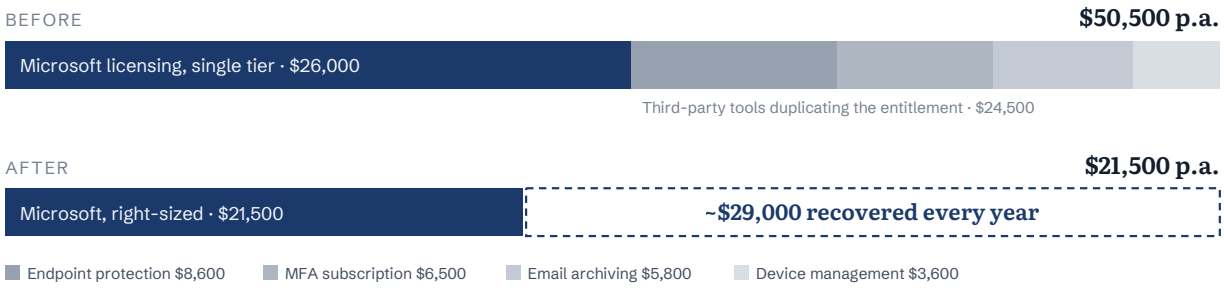
06

A worked example

The figures below are illustrative (a composite of what the pattern typically looks like for a Victorian care provider of around 120 staff), not a quote. Your numbers depend on your renewal terms, eligibility and current contracts, which is precisely why the first step is an audit rather than a purchase.

ITEM	BEFORE (P.A.)	AFTER (P.A.)
Microsoft licensing: 120 seats, single tier	$26,000	—
Microsoft licensing, right-sized: 30 Foundation (free), 78 Core, 12 Privileged	—	$21,500
Third-party endpoint protection (120 users)	$8,600	$0
Standalone MFA subscription (120 users)	$6,500	$0
Email archiving service	$5,800	$0
Mobile device management platform (60 devices)	$3,600	$0
Total annual	**$50,500**	**$21,500**

FIGURE · THE WORKED EXAMPLE: ANNUAL SPEND BEFORE AND AFTER THE RESET



Indicative recovered spend: about **$29,000 a year, while materially raising the security posture**. MFA everywhere, managed devices, data-loss prevention on client records, privileged access controlled. For most providers in the 80-200 seat range the recoverable figure lands somewhere between $15,000 and $35,000 a year. That is the budget that funds the reset.

07

The fifteen-minute self-check

Answer honestly (Yes, No or Unsure), ideally with your IT manager or MSP in the room. Unsure counts as No: in security, not knowing is the finding.

#	QUESTION	Y / N / U
01	Do you know your Microsoft renewal date and what your licensing will cost at that renewal?	☐ ☐ ☐
02	Do you know which of your licences were affected by the July 2025 grant retirements?	☐ ☐ ☐
03	Has anyone mapped your Microsoft entitlements against the third-party security tools you pay for?	☐ ☐ ☐
04	Are licences matched to roles: no volunteers on premium seats, no clinical or finance staff on the free tier?	☐ ☐ ☐
05	Is multi-factor authentication enforced for every account, including part-time, casual and volunteer accounts?	☐ ☐ ☐
06	Are the devices that access client information managed: encrypted, PIN-protected, remotely wipeable?	☐ ☐ ☐
07	Could you produce, today, a list of everywhere client health information is stored and shared?	☐ ☐ ☐
08	Are there rules in place that stop client records leaving the organisation by email or Teams?	☐ ☐ ☐
09	Do you know who holds administrator access, and is that access time-limited rather than permanent?	☐ ☐ ☐
10	Would you detect a compromised staff mailbox within a day, and who would be alerted?	☐ ☐ ☐
11	Has the board received a cyber and information-risk report in the last twelve months?	☐ ☐ ☐
12	If ransomware struck and a payment was made, does your executive know its 72-hour reporting obligation?	☐ ☐ ☐

Reading your score

0–2 No/Unsure: you are in better shape than most of the sector. Verify the answers with evidence at your next renewal.

3–6 No/Unsure: you have real gaps, and very likely real recoverable spend. Worth a structured look before your renewal date, while the licensing decision is still open.

7+ No/Unsure: the licensing event is your opportunity: the organisation can materially improve its security and its cost base in the same exercise. Treat it as a board-visible piece of work, not an IT task.

08

The sequence before your renewal

Whether you do this internally, with your MSP, or with independent help, the order of operations matters more than the tooling:

01 **Find the renewal date.** Everything is easier with months in hand; almost nothing is fixable in the week the invoice arrives. Annual upfront billing is now the default, so the decision locks in for a year.

02 **Audit entitlement against usage.** What you hold, what each role actually needs, what the third-party stack duplicates. Two days of work, and every later decision depends on it.

03 **Right-size the tiers.** Apply the three-tier model. Verify your Microsoft nonprofit eligibility formally before banking any number.

04 **Architect the controls.** MFA and conditional access first, then device management, then data-loss prevention. Identity is always first: it is the control that protects everything else.

05 **Decommission in order.** Retire each duplicated tool only after its replacement is configured, tested and adopted. Bank the savings; report the uplift to the board.

ABOUT VYFORITY, AND A NOTE ON INDEPENDENCE

Vyfority is a Melbourne-based cyber security and business architecture consultancy founded by Dean Kastelic: a former enterprise CISO and ex-KPMG Director of Cyber Advisory with more than twenty years across security architecture, regulated industries and critical services. Vyfority works with mid-market and not-for-profit organisations on exactly the kind of exercise this guide describes: engagements designed so that recovered spend funds the work, with fixed fees and a guarantee behind the outcome.

A note on independence: Vyfority does not resell Microsoft licences and earns nothing from your licensing decisions. Sometimes the right answer is the cheaper licence. That independence is the point.

If the self-check landed at three or more

The usual next step is a short, fixed-fee Licence & Exposure Snapshot: two days, your actual numbers, and a board-ready one-pager of what we found. No obligation follows it.

Dean Kastelic · dean.kastelic@vyfority.com.au · linkedin.com/in/deankastelic · vyfority.com.au