Northbridge Managed

MDR+

Managed Detection and Response. It watches your client's computers and user accounts around the clock, catches threats the moment they appear, and shuts them down automatically before they cause damage. Not software your client has to run. A full service, with our Australian team accountable for the outcome.

24×7	< 1 sec	10 devices	12 months
24×7 Australian based Detection and Response	Automated containment	Minimum commit	Telemetry retention

The three things that make it different

01

Endpoint and identity, together

We watch the devices and the Microsoft 365 accounts as one picture. Most rivals sell those as two separate products.

02

Detections built for each client

Most managed services run one shared rulebook across every customer. We build and tune detections for each client's own environment.

03

100% Australian, end-to-end

The team, the data and the response all stay in Australia. No overseas SOC rotation.

Threats handled immediately

A five-step loop runs non-stop on every device and account. The first three steps are automatic. The last two put a real analyst in the loop the moment human judgement is required.

THE 24×7 LOOP

01 · DETECT
Suspicious behaviour spotted

02 · ENRICH
Full context added instantly

03 · CONTAIN
Isolate at machine speed

04 · ESCALATE
Analyst validates the case

05 · INFORM
Client told what happened

Automatic Human in the loop - Australian analyst

WHAT'S INCLUDED

Platform & coverage

- Sensor on Windows, macOS and Linux
- 24×7 telemetry collection
- M365 and Entra ID identity

Detection & Response

- Northbridge detection rules
- Northbridge behavioural analytics
- Custom detections per client

Response & containment

- Automated process termination
- Endpoint isolation on policy match
- Analyst escalation by design

Operations & reporting

- 24×7 Australian based Detection and Response
- Monthly reporting and reviews
- Quarterly posture review

WHAT YOUR CLIENT EXPERIENCES

1 A 60-second install

A lightweight sensor per device. No reboot, no downtime.

2 Monthly service reports

What was detected, what was contained, how posture is tracking.

3 Real-time investigations

A report as an incident unfolds, not weeks afterwards.

4 A call on high-risk incidents

We ring, explain it plainly, and help their IT team fix it.

Three competitors, three cases

You will meet these three most often. Here is what each is good at, and where MDR+ has the stronger case.

CrowdStrike

ENTERPRISE EDR

WHO THEY ARE

Best-in-class detection technology. Falcon Complete is their managed tier, built for large enterprise budgets.

WHERE MDR+ WINS

Around half the price of Falcon Complete

10-device minimum, against roughly 250

Billed monthly, not a year upfront

24×7 Australian based Detection and Response

Coexists with Defender

Arctic Wolf

MID-MARKET MDR

WHO THEY ARE

Sydney SOC, a named concierge team and a $3M breach warranty. Built for customers who can absorb a $44K-plus annual floor.

WHERE MDR+ WINS

Stronger under 200 users

Genuinely end-to-end Australian, not a five-country rotation

Custom detections per client

Monthly billing, not a long prepay

Huntress

SMB EDR · CHANNEL-LED

WHO THEY ARE

A strong MSP brand with a managed SOC at every tier, but endpoint and identity are sold as two separate products.

WHERE MDR+ WINS

Works under 50 seats, where Huntress is not available

Identity bundled into one price

Sub-second containment, not analyst-gated

Australian data sovereignty

The short version: Under 50 seats there is no equivalent managed competitor. Between 50 and 200, MDR+ is the strongest commercial case in the market.

AND IF THEY ALREADY USE MICROSOFT DEFENDER

Keep it. We manage it.

Microsoft Defender Antivirus is genuinely good endpoint protection and it's already included right in your Windows and Microsoft 365 licensing. What it *does* do on its own is custom detection engineering, 24/7 active monitoring, pro-active threat hunting, automated containment, or identity-based attack detection. Defender Antivirus guards the front door while MDR+ watches what manages to slip through it. No rip-and-replace required.

Numbers to keep front of mind

10 devices

Minimum commit against roughly 250 for the enterprise alternatives.

Billed monthly

12-month term, paid monthly. No annual prepay, no big upfront cheque.

24×7

24×7 Australian based Detection and Response. Security operations around the clock, entirely in Australia.

Under 1 second

Automated containment, configurable per detection.

12 months

Telemetry retention included as standard, not an upsell.

ISO 27001 • E8 ML3

Independently verified. NV2 and NV1 cleared staff.

TWO THINGS WORTH KNOWING

Partner pricing

Buy price, volume tiers and margin are covered in the walkthrough so we can work them against your own client base.

Breach warranty

We do not offer one. That premium goes into detection quality, sub-second containment and custom detections instead. For most clients, cyber insurance does the warranty job more flexibly.

NEXT STEP

Book a session with us

sales@fifteenxv.com.au