

of Chief Information Officers (CIOs) in ANZ expect cybersecurity to receive the most significant increase in technology investment by 2025

[Gartner](#)

Sales Play 3: All-in-one Enterprise Security, Information Protection & Governance Upgrade from M365 E3 to M365 E5

Upgrade customers from M365 E3 to M365 E5 to elevate their security with unified threat detection and response (XDR), compliance capabilities and advanced data management tools for a resilient and compliant business environment.

Drive growth and security for your customers with M365 E5

SMB Challenges

Growing Cybersecurity Threats:

Expanding attack surface increases vulnerability to ransomware, insider threats and data breaches.

Fragmented Compliance Tools:

Customers struggle to manage compliance across hybrid environments with disconnected solutions.

Inconsistent Access Control:

Securing access to critical data and applications while ensuring compliance is complex without centralised, automated solutions.

Transformative Actions for IT Partners/ MSPs

✓ Unified Protection Across Identities & Endpoints:

Implement Microsoft Defender and Azure AD Premium P2 to provide comprehensive, proactive security across your customers' environments.

✓ Automated Compliance & Risk Management:

Utilise Microsoft Purview Compliance Manager and Insider Risk Management to streamline compliance processes, reduce manual effort and mitigate insider risks.

✓ Advanced Access Governance:

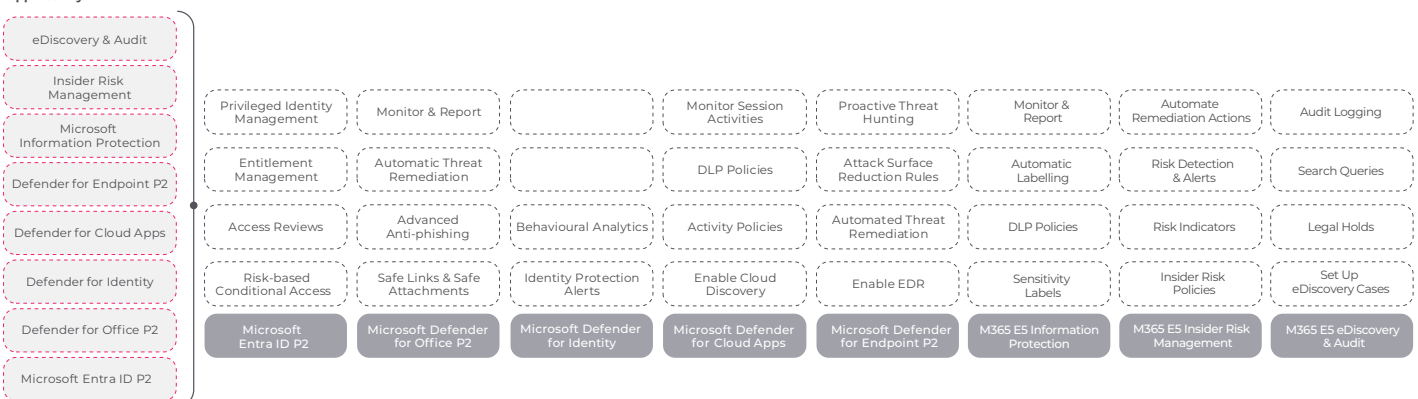
Leverage risk-based conditional access and policies to ensure seamless, secure access management for your customers, driving both security and compliance improvements.

✓ Include 24x7 Managed Cyber Security Services:

Pair this advanced security stack with Chorus MXDR for a fully managed SOC experience. We integrate Microsoft's XDR capabilities with their AI-driven automation and human expertise, reducing risk and accelerating response.

Partner Opportunity with M365 E5

Add-on services opportunity



\$22K - \$100K

Partner professional services opportunity



Why Chorus Cybersecurity Is the Partner of Choice for Microsoft Security

Chorus Cyber delivers Managed Detection and Response (MDR) and Managed Extended Detection and Response (MXDR) services through a channel partner model, enabling partners to offer enterprise-grade cybersecurity without building their own SOC.

Partner Value Proposition

Built for Microsoft Partners: Chorus leverages Microsoft-native signals (Defender, Entra ID, Sentinel) to deliver full-spectrum threat management.

No Additional Agents: All services run within the customer's existing Microsoft investment—cost-effective and operationally simple.

Verified Microsoft Security Partner: Chorus is a member of MISA and holds Microsoft-verified MXDR status.

Rapid Response Metrics: <3 min MTTA and <17 min MTTC vs. 180 min industry median.

Why Chorus Is a Winner

24x7x365 CSOC: Global coverage with some of the fastest response times in the industry.

Established Channel Model: Easy onboarding, no consumption commitment at stage one.

Strategic Microsoft Alignment: Services built entirely on Microsoft Security, maximizing licensing ROI and reducing third-party tool reliance.

Proven Outcomes: Real-world deployments show significant uplift in Microsoft licensing and Azure consumption.

Packaged Cybersecurity Solutions That Are Easy to Position

MDR (Managed Detection and Response)

Focused protection at the endpoint level—detects, investigates, and contains threats quickly and effectively.

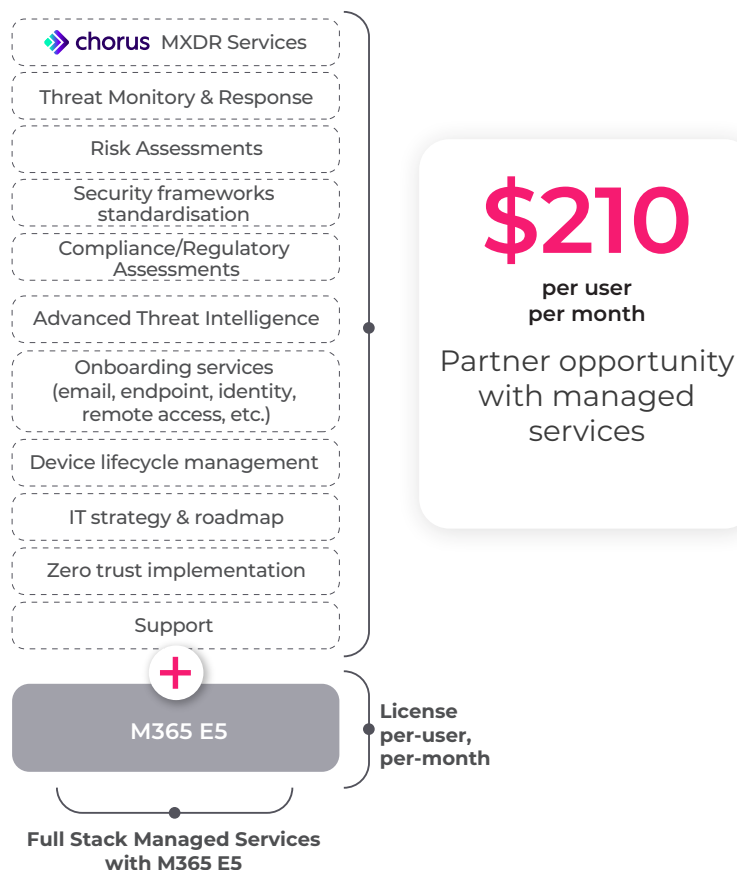
MXDR (Managed Extended Detection and Response)

Comprehensive threat coverage across identity, network, email, infrastructure, data, and applications—leveraging Microsoft-native and third-party telemetry.

SERVICE COMPARISON		MDR	MXDR
24x7x365 CSOC		✓	✓
Analysts available by phone 24x7		✓	✓
30 minute high severity SLA		✓	✓
Containment and response actions		✓	✓
Chorus proprietary analytic rules		✓	✓
Microsoft Security Suite coverage	Defender for Endpoint	✓	✓
	Defender for Identity		✓
	Defender for Cloud Apps		✓
	Defender for Office		✓
	Defender for Cloud		✓
	Azure services		✓
Microsoft Sentinel custom integration			✓
Custom security playbooks			✓
MITRE ATT&CK framework mapping			✓
External attack surface monitoring			✓
Threat Detection & Response Coverage	Endpoints	✓	✓
	Entra ID Identities	✓	✓
	Servers	✓	✓
	Active Directory Identities		✓
	Non-Azure cloud services		✓
	Networking log sources (Firewalls/Switching/APs)		✓
	3rd Party APIs/Logs		✓
Weekly security service reports		✓	✓
Cyber Essentials aligned TVM report		✓	✓
Endpoint threat hunting		✓	✓
Cyber Threat Intelligence		✓	✓
Standard security playbooks		✓	✓
Security recommendations & guidance		✓	✓
Service governance		✓	✓
Extended threat hunting			✓



Upgrade to M365 E5 for advanced security and compliance. Use the Defender Suite for threat protection, Information Protection for data security and Insider Risk Management to reduce internal threats. Protect identities with Defender for Identity, enable eDiscovery for legal needs and ensure compliance with Audit.



Main Resource

- Access the full sales toolkit, including a customer-ready brochure and pitch deck [here](#).

Other Resources

- Security Managed Services Partner Kit
- Get started with Microsoft 365 Lighthouse

\$62,800

**Average cost to a medium
business of cyber crime**

ACSC – Annual Cyber Threat Report 2022

Supercharge
your security offering

Dicker Data's local team of specialist people, practices and programs are here to help you serve your customers and capitalise on the surging demand for security services.

Learn more and contact us at www.dickerdata.com.au/microsoft