

## Sales Play 1e: Identity Protection M365 Business Premium + Identity Protection

Add Identity Protection to M365 Business Premium to help customers strengthen their identity management with advanced risk-based conditional access, seamless authentication and comprehensive governance to secure user access.



of ANZ businesses report disruption as the biggest cost of identity fraud

ASD Cyber Threat Report 2024

### SMB Challenges

#### Managing Excessive Permissions:

Small businesses often face challenges in ensuring users only have the access they need, which can lead to security risks and compliance gaps.

#### Securing Privileged Accounts:

Privileged accounts pose a significant risk if misused or compromised, especially when access is always enabled.

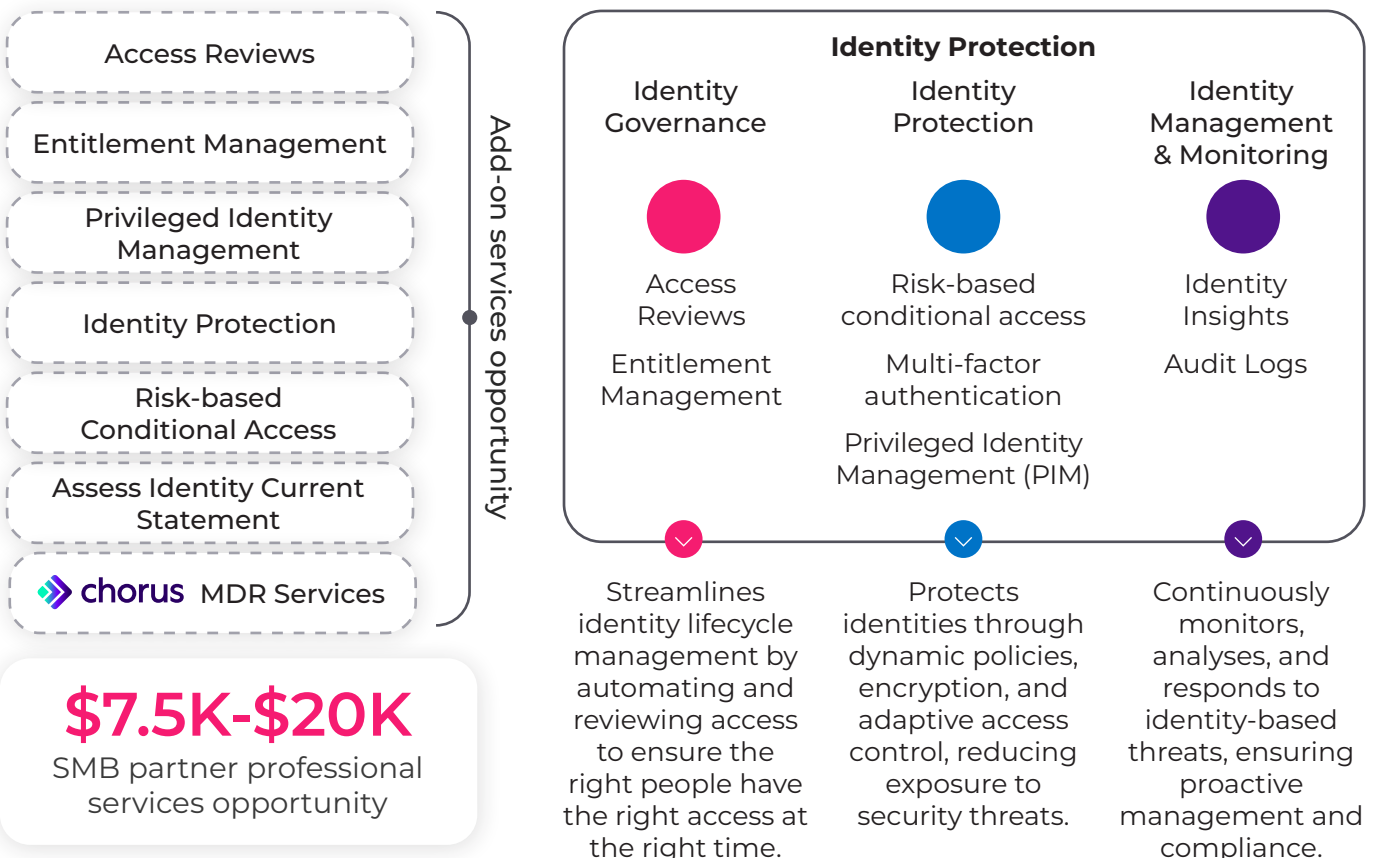
#### Addressing Identity-Based Threats:

Detecting and responding to identity-related risks can be challenging with limited resources.

### Transformative Actions for IT Partners/ MSPs

- ✓ **Access Management Solutions:** Use access reviews and entitlement management to automate permissions, ensuring users only have necessary access. Regularly audit and revoke unnecessary permissions.
- ✓ **Secure Privileged Accounts:** Leverage privileged identity management (PIM) for just-in-time access, minimising misuse by limiting persistent privileged access.
- ✓ **Addressing Identity-based threats:** Implement risk-based conditional access and MFA to secure identities and respond to suspicious activity without overburdening small business resources.
- ✓ **Include 24x7 Managed Cyber Security Services:** Combine this identity upgrade with Chorus MDR for enhanced detection and response across identities and endpoints. This ensures that advanced identity governance is backed by real-time monitoring and incident response from our CSOC.

## Partner Opportunity with Identity Protection





## 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.

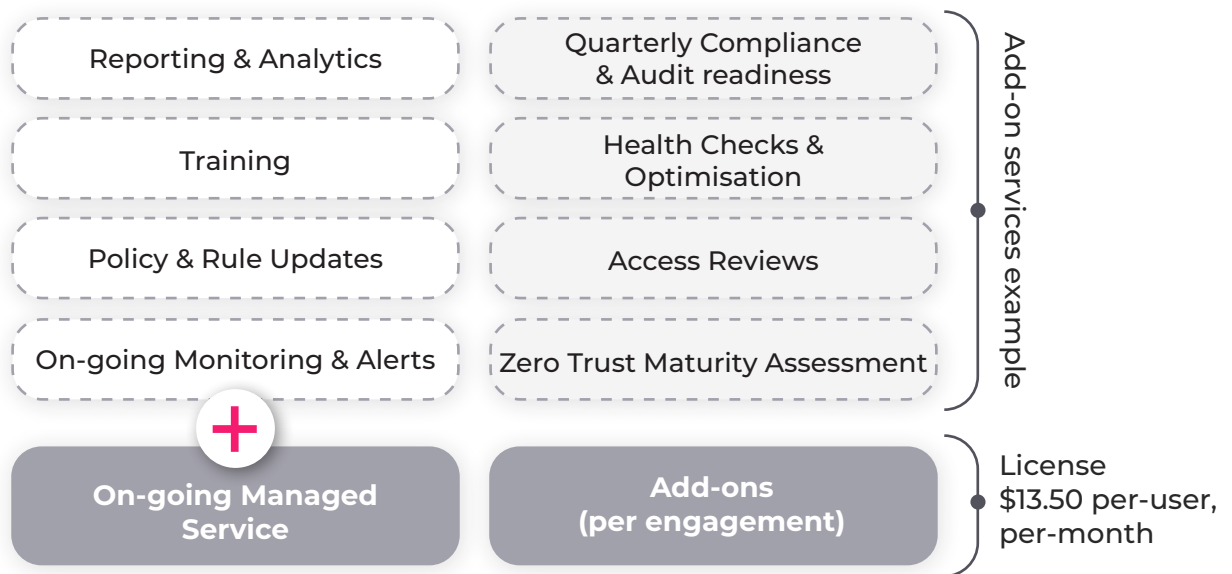
#### MXDR (Managed Extended Detection and Response)

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			✓



**Example of partner-managed services for Identity Protection: Secure user identities, manage access permissions, conduct regular access reviews, implement just-in-time privileged access and enforce conditional access policies.**



## Main Resource

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

## Other Resources

- Get started with Microsoft 365 Lighthouse

**\$98M**

**lost to email compromise and identity theft in 2021-2022**

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](http://www.dickerdata.com.au/microsoft)