DICKER DATA | Microsoft

Supercharge your security:
A practical guide to cyber threats and protection for ANZ SMBs in the age of AI

With regulations tightening and AI-powered attacks on the rise, building a pathway to security is now essential for your business.

This guide provides a practical overview of today's security landscape, explains key risks facing local SMBs and outlines how enterprise-grade security is now within reach for businesses of every size, with solutions that grow with your needs.

The new security landscape: Why SMBs are prime targets

Fuelled by AI, cyber attacks are becoming more sophisticated, more frequent and harder to detect. While breaches at large corporates have traditionally captured the headlines, small and medium businesses (SMBs) are also prime targets.

Contents

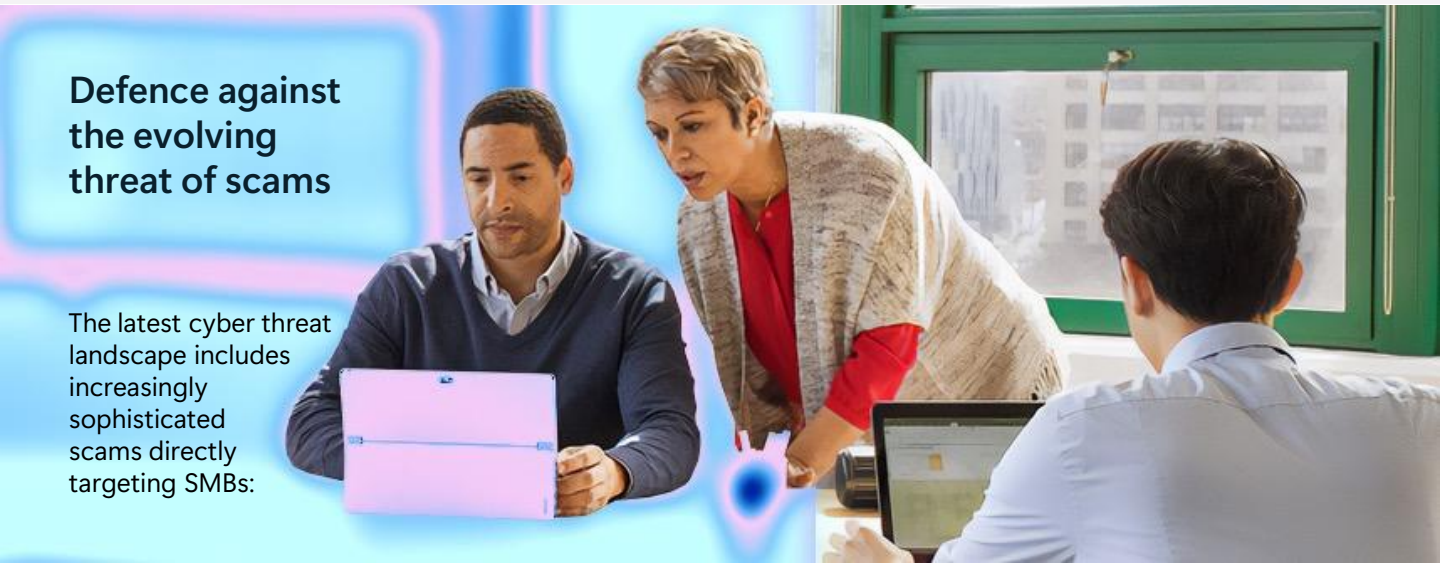
SMBs represent the perfect storm of valuable data and limited security resources

Microsoft Security research revealed that 80%[1] of organisations experienced more than one data breach in their lifetime, with the average cost of cyber crime to small businesses being $49,600[2]. For small businesses, a loss of this scale can represent an existential threat, with two-thirds[3] of SMBs that suffer a cyber attack going out of business within 6 months.

With the rise of AI-powered methods, criminals can now automate previously labour-intensive tasks such as crafting convincing phishing emails, generating deepfake scams, identifying network vulnerabilities and launching coordinated attacks.

Meanwhile, most SMBs lack dedicated security teams, advanced monitoring capabilities and comprehensive security strategies. Many rely on a patchwork of disconnected security tools that create costly complexity while leaving critical gaps in protection.

For many SMBs, the first sign of this protection gap comes only after a breach has occurred – when it's already too late.



Defence against the evolving threat of scams

The latest cyber threat landscape includes increasingly sophisticated scams directly targeting SMBs:

QR code phishing (Quishing)

Cybercriminals are using QR codes in emails, social media and even at physical locations to trick users into visiting malicious websites. The Australian Cyber Security Centre (ACSC) has identified this as an 'unseen threat' that bypasses traditional email security.

Video call deepfakes

In one recent attack reported by the Australian Computer Society (ACS), an employee was invited to a video conference call where all other participants were AI-generated deepfakes of colleagues. After recognising familiar faces, the employee was convinced to transfer $40 million from company accounts.

Celebrity Impersonation

Online scams that use high-profile personalities or brands to appear authentic are common. In one case reported by the ABC, a man lost more than $80,000 in life savings to such a scam. Even when not business-related, your staff can click malicious links on their business devices on their lunch break or commute, potentially compromising your systems.

Three critical security risks facing your business

As cyber threats evolve, three key risk areas demand immediate attention from every SMB:

1. Data Security & Information Protection

Your business data – like customer information, intellectual property and financial records – is your most valuable asset. Yet many businesses lack visibility into where sensitive data resides, how it's used and who can access it.

Without proper data classification, labelling and protection policies, sensitive information can be accidentally leaked, deliberately stolen or improperly retained, leading to financial and reputational damage.

Real Impact: Data breaches expose your business to significant financial penalties under privacy regulations, damage customer trust, lead to intellectual property theft and can even put SMBs out of business within six months[3], highlighting the need for robust cybersecurity measures.

Red flag

If you're unsure exactly where your sensitive data is stored, who has access to it or how it's being protected, you may have critical security gaps.

2. Identity Protection

Compromised credentials like basic usernames and passwords are a common cause of major data breaches. Despite this, many businesses still rely on passwords alone, leaving their systems vulnerable to credential theft through phishing, social engineering or brute force attacks.

As employees increasingly access business resources from multiple devices and locations, traditional security boundaries no longer exist. Without modern identity protection, it's difficult to verify who's accessing your systems.

Real Impact: Attackers who gain access through stolen credentials or passwords can remain undetected for months, exfiltrating data, launching ransomware attacks or using your systems to hack others.

Red flag

If you rely primarily on passwords, don't use multi-factor authentication or can't track who's accessing your systems, your business is at an elevated risk.

3. Endpoint Protection & Threat Defence

Every device that connects to your network – commonly servers, laptops, tablets, printers and mobile phones – represents a potential entry point for attackers. Traditional antivirus solutions are no longer sufficient against modern threats.

Without integrated, AI-powered threat detection and automated response capabilities, businesses lack visibility into potential threats and the ability to respond quickly when an attack occurs.

Real Impact: Security incidents that aren't quickly detected and contained lead to significantly higher costs, extended business disruption and more extensive data loss.

Red flag

If you're using basic antivirus without advanced threat detection or have limited visibility into device security status, your protection may be inadequate.

SMB security regulatory changes: What your business needs to know

The security landscape is changing not just technically but also legally. Two significant regulatory changes from 2025 will dramatically impact how Australian SMBs must handle security and data protection:

Privacy Act: Small business exemption removal

The Privacy Act 1988 applies to most Australian businesses, requiring them to handle personal information in accordance with strict guidelines.

However, SMBs with an annual turnover of less than $3 million have been generally exempt except for specific categories. If legislated, this exemption will be removed starting in 2025

To comply with the Privacy Act, all businesses regardless of size or turnover, need to:

- You must implement a privacy policy and data breach response plan
- If there is a breach, you'll face significant potential penalties (up to $50 million or 30% of adjusted turnover for serious breaches)

SMB1001 cybersecurity compliance framework

This new framework establishes baseline security standards specifically designed for SMBs.

What this means for your business:

- You'll need to implement specific security controls
- Regular security assessments will be needed to meet the standards
- You may need to demonstrate compliance to win certain contracts, particularly with government or enterprise clients

A more detailed explanation of these regulatory changes and compliance requirements is available in the additional resources at the end of this document.

These regulatory changes are coming quickly

Businesses have a limited window to prepare their systems and processes. Businesses that act now will reduce compliance risks and gain a competitive advantage as security becomes a key differentiator in the marketplace.

> *Australian small businesses require specific advice to better defend themselves from cybersecurity threats. While there are effective and inexpensive practices available to protect them against cyber incidents, many businesses are unaware these practices exist.*
>
> **Australian Cyber Security Centre (ACSC)**

The better approach: Integrated protection that grows with your business

Integrated seamlessly into the Microsoft 365 productivity suite, Microsoft's security solutions are tailored for businesses of all sizes, with affordable options that provide enterprise-grade protection without enterprise complexity or cost.

If you are like most small businesses, you already use a range of M365 tools for productivity and operations day to day, so integrating security is a natural extension.

By addressing each of the critical risk areas with integrated solutions, Microsoft's approach provides comprehensive protection that grows with your business needs:

For data security & information protection

Protect your most valuable information while meeting compliance requirements – without hindering productivity. Microsoft's information protection solutions capabilities, available as an add-on or built into certain M365 SKUs, help you:

- Automatically identify and classify sensitive information such as credit card numbers or personal details
- Apply protection that travels with your data wherever it goes – whether stored, in transit or shared externally
- Implement retention policies that ensure compliance with regulations like the Privacy Act
- Prevent data loss through accidental sharing or malicious exfiltration

For identity protection

Ensure only the authorised people access your systems and data, with administrative access limited to a defined timeframe. Microsoft's identity solutions, available as an add-on or built into certain M365 SKUs, help you:

- Implement strong multi-factor authentication to mitigate risk of credential theft
- Apply conditional access policies that adapt security requirements based on user, location, device and risk
- Detect and respond to suspicious sign-in attempts in real time, automatically blocking risky logins
- Simplify secure access to all your applications with single sign-on while maintaining strong protection

For endpoint protection & threat defence

Stop threats before they cause damage, reducing downtime and eliminating costly recovery efforts. M365 threat protection capabilities help you:

- Protect devices against malware, ransomware and other sophisticated threats without performance impact
- Detect and respond to advanced attacks before damage occurs, using AI-powered analytics
- Gain visibility across your entire environment with a unified security dashboard
- Automate security responses to contain threats quickly

The integration advantage

Unlike piecing together solutions from multiple vendors, Microsoft's security offerings work together seamlessly, sharing intelligence and automating responses across your environment. This integration provides:

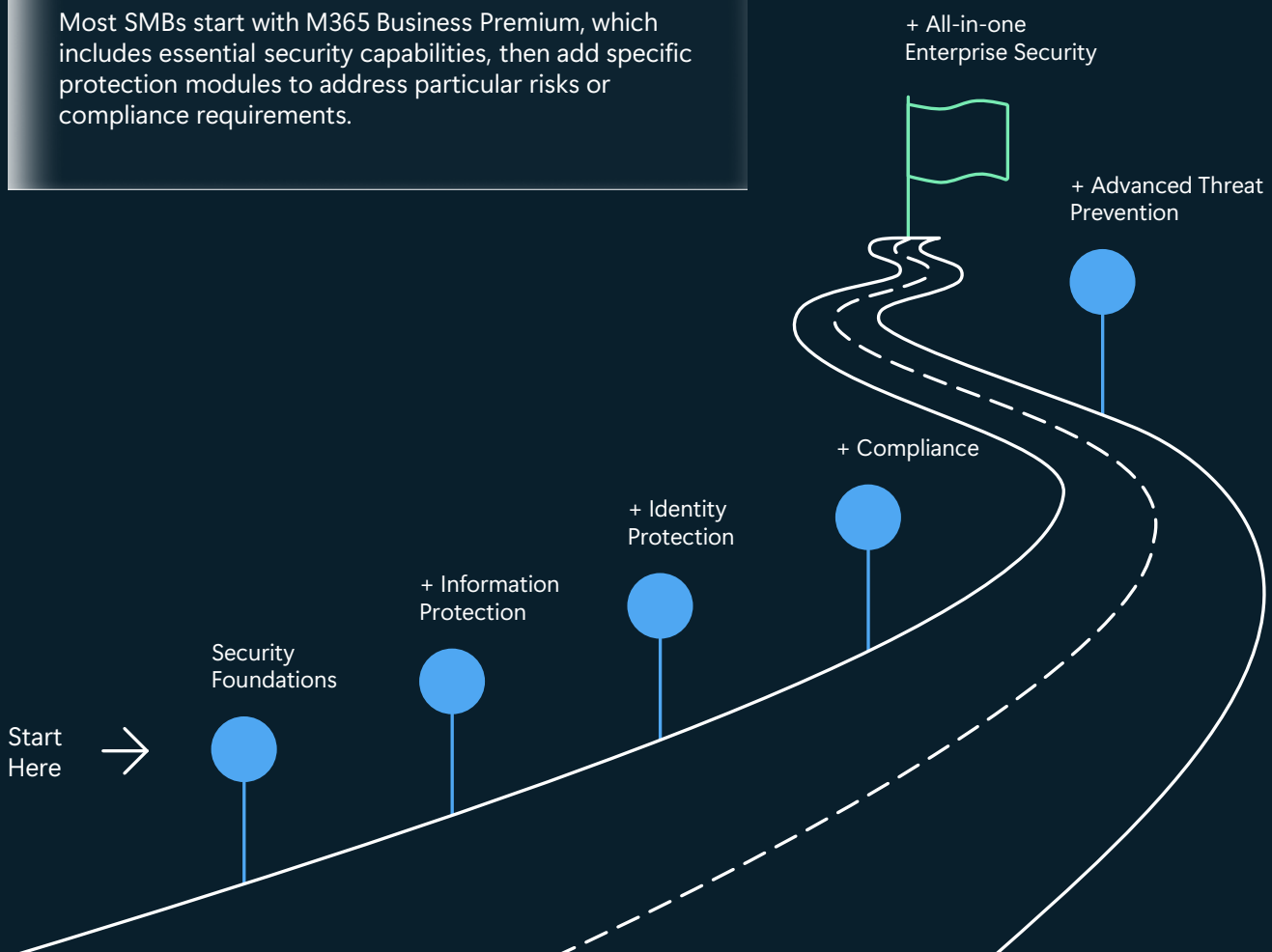
- **Cost efficiency:** Consolidated licensing may reduce overall security spending
- **Simplified management:** One dashboard instead of multiple portals
- **Comprehensive coverage:** No gaps between solutions from different vendors
- **Future-ready foundation:** AI-powered security that evolves as threats change

Real Impact: For example, when a suspicious email arrives, M365's integrated security automatically checks the sender, scans attachments, analyses links and verifies the user's identity – all within seconds and without disrupting workflow.

Start where you are, grow as you need

M365's modular approach to security means you can begin with foundational protection and add advanced capabilities as your business grows and your security needs evolve.

Most SMBs start with M365 Business Premium, which includes essential security capabilities, then add specific protection modules to address particular risks or compliance requirements.



Security solutions for your industry

Every industry faces unique security challenges. A knowledgeable security partner can help tailor protection to meet your unique business requirements.

Here's how advanced security solutions address the specific threats in a range of sectors:

Healthcare

If you operate in the healthcare sector, your security priorities likely centre around protecting sensitive patient information and maintaining continuity of care.

The healthcare industry has seen a surge in ransomware attacks targeting patient data. As reported in The Courier-Mail, Australian SMB Bloom Hearing Specialists, suffered a ransomware attack that compromised tens of thousands of clients' personal and health information.

Healthcare businesses typically prioritise:

- **Data encryption** to protect sensitive patient information
- **Access control** to ensure only authorised personnel can access patient data
- **Network security** to prevent cyber attacks on healthcare networks

Financial Services & Insurance

Financial services and insurance organisations face heightened scrutiny and sophisticated attacks targeting valuable assets, sensitive personal data and private client information. A breach can have devastating consequences, with Cisco reporting that 74%[4] of SMBs in the Asia-Pacific region believe a major cyber incident could jeopardise their organisation's survival.

Both sectors collect and store extensive personal and financial information that makes them attractive targets for cybercriminals. Key priorities in these sectors include:

- **Data breach prevention** to safeguard confidential client information, policy details and financial records
- **Fraud detection and prevention** to identify and block fraudulent transactions, claims and activities
- **Compliance with regulations** to meet strict industry standards and avoid hefty fines and legal consequences

Security solutions for your industry

Retail

Retail businesses must protect both customer payment information and maintain operational continuity and defences across multiple channels.

Collecting data from and transacting with thousands of customers and payments – across ANZ and globally, online and off – retailers are increasingly targeted by cybercriminals using tactics like quishing. Retail businesses typically focus on:

- **Data breach prevention** to protect customer information
- **Fraud detection** to safeguard online transactions
- **Supply chain security** to protect complex retail networks

Government

Government entities need to balance public accessibility with the need to safeguard sensitive information and critical services and infrastructure.

Like SMBs, local government agencies across Australia can be seen as a vulnerable target and are experiencing increased attacks on essential services. Business email compromise (BEC) attacks have been identified as a major threat, potentially causing significant financial damage. Governments prioritise:

- **Data protection** to safeguard sensitive information
- **Cyber threat intelligence** to stay ahead of emerging threats
- **Network security** to ensure the integrity of governmental communications

The partner advantage: Why expert guidance matters

Security is complex and constantly evolving. Working with an expert Microsoft security partner gives you access to expertise and technology to complement your in-house capabilities and access specialised resources that may otherwise be cost-prohibitive.

A qualified Microsoft security partner can:

- Assess your specific risks and compliance needs
- Design a tailored security roadmap aligned to your business strategy
- Implement and scale security solutions with minimal disruption
- Provide ongoing monitoring and management
- Keep you updated on evolving threats
- Advise you on regulatory compliance specific to your industry

Most importantly, the right partner becomes your trusted security advisor – someone who understands both your business needs and potential security threats. This gives you the confidence to make informed decisions that protect your organisation while enabling growth.

Our approach

We work with you as a trusted security partner, providing:

Security assessment:
We evaluate your current security posture against best practices, industry standards and regulatory compliance requirements

Tailored roadmap:
We develop a practical security strategy aligned with your business goals and budget

Implementation & management:
We deploy and manage the right Microsoft security solutions to protect your business

Ongoing support:
We provide continuous monitoring, updates and user training to keep you protected as threats evolve

Compliance guidance:
We help you navigate regulatory requirements and prepare for audits

Invest in a secure future

Microsoft offers a range of security solutions packaged in M365 SKUs and add-ons or mini bundles to provide cost effective, enterprise-level security to SMBs.

With the average cost of a data breach for an Australian SMB exceeding $49,000 – on top of reputational damage and business disruption – the business case for protection is clear.

With Microsoft's flexible approach, you can start with essential protection and add capabilities as needed for a fixed and transparent investment.

Security Solution	Protection against	What You Get	Total cost (per user, per month)
M365 Business Standard **$18.90**	Basic protection with email safeguards and multi-factor authentication (MFA)	Productivity suite, limited email and identity protection	**$18.90**
M365 Business Premium (A $14.20 upgrade from M365 Business Standard)	Advanced threat protection and endpoint security	Plus comprehensive endpoint protection, identity management and data loss prevention	**$32.90** Includes M365 Business Standard Productivity capabilities + Defender for Business
Microsoft Entra ID P2 add-on ($13.50)	Identity-based threats, unauthorised privilege escalation and account compromise	Plus centralised identity protection with automated risk detection	**$46.40** M365 Business Premium + Microsoft Entra ID P2
+$10.50 for Microsoft Information Protection add-on	M365 Business Premium protection + Accidental sharing of confidential information	M365 Business Premium plus Automated data classification, encryption and governance	**$43.40** M365 Business Premium + Microsoft Information Protection
+$18 to add **E5 Security mini bundle**	M365 Business Premium protection + Advanced threat detection, layered security protection	M365 Business Premium plus AI-powered threat protection across email, identity, endpoints and cloud apps	**$50.90** M365 Business Premium + E5 Security

All prices are in AUD and exclude GST and are subject to change at Microsoft's discretion.

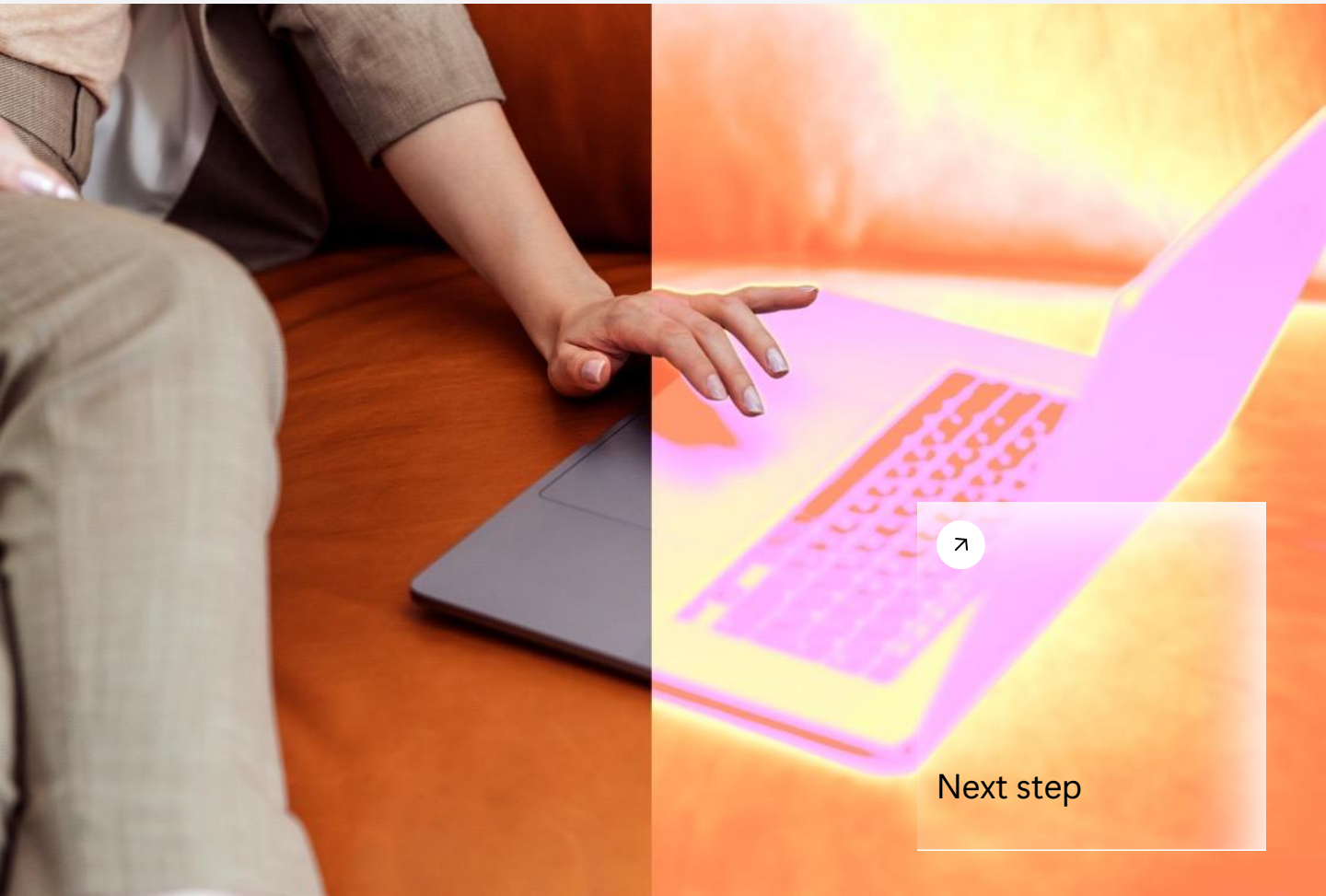
Next step:
Schedule your free security assessment

Security is a journey, not a destination. As your trusted security partner, we'll help you build a mature security posture that evolves with your business.

Here's how to get started:

- **Book your complimentary security assessment:** Identify your current risks, compliance gaps, and quick-win opportunities without disrupting your operations
- **Review your personalised security roadmap:** Receive a practical plan that prioritises balances critical security needs with business goals and budget constraints.
- **Deploy foundational protection:** Implement essential security capabilities for immediate risk reduction
- **Build security awareness:** Train your team on security best practices that complement technical controls
- **Continuously improve:** Regularly review and enhance your security posture as threats evolve

Implementing robust security doesn't have to be overwhelming or disruptive. With the right partner and Microsoft's integrated security solutions, you can achieve enterprise-grade protection that fits your business needs and budget.



Let's work together to supercharge your security

Our Microsoft security experts will help you navigate the complex threat landscape and build a security foundation that protects your business now and in the future.

About Dicker Data

As Australia's largest owned and operated technology distributor, we represent over 8,000 technology providers. We've created a network of specialist cyber security partners who help Australian healthcare organisations mitigate risks and defend against increasing threats.

Meet our proven healthcare security partners

CUBESYS

cubesys is a Microsoft Partner helping healthcare organisations modernise with Azure, Microsoft 365, automation and managed services. We deliver secure, scalable solutions that support compliance, protect data and improve workflows. We work closely with our customers to ensure fast, effective, and secure outcomes. Learn more at cubesys.com.au or email sales@cubesys.com.au.

daraco I.T. SERVICES

Daraco IT, a leader in technology services and Cyber Security, exceling in safeguarding digital landscapes. With a mission to empower healthcare providers through cutting-edge technologies and expert strategies, we provide robust protection against cyber threats, fostering secure and resilient environments for our clients. Learn more at www.daraco.com.au/health-solutions or call 1300 327 226

Spirit

Spirit delivers secure, scalable ICT solutions tailored for the unique and evolving needs of the healthcare sector. We support our clients to boost productivity, achieve seamless connectivity and ease the administrative burden. Spirit empowers healthcare teams with reliable solutions that keep operations secure and efficient. Learn more at spirit.com.au or email spirit@spirit.com.au.

Connect with a proven healthcare security specialist:
dickerdata.com.au/microsoft/healthcare-security

References:
1. Microsoft: Microsoft Data Security Index Report, 2024
2. ASD: Annual Cyber Threat Report 2023-24
3. ASBFEO Newsletter 2023
4. Cisco: Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense, 2021