



**CISO ONLINE**  
CYBER SECURITY UPLIFT & AWARENESS

# SMB PACKAGE - **CYBER PREMIUM**

**CISO UPLIFT**

DATASHEET





**CISO ONLINE**  
CYBER SECURITY UPLIFT & AWARENESS

## **WHO IS CISO ONLINE**

CISO Online uplifts your cyber security posture through our cyber security uplift program, advanced professional services, and awareness training.

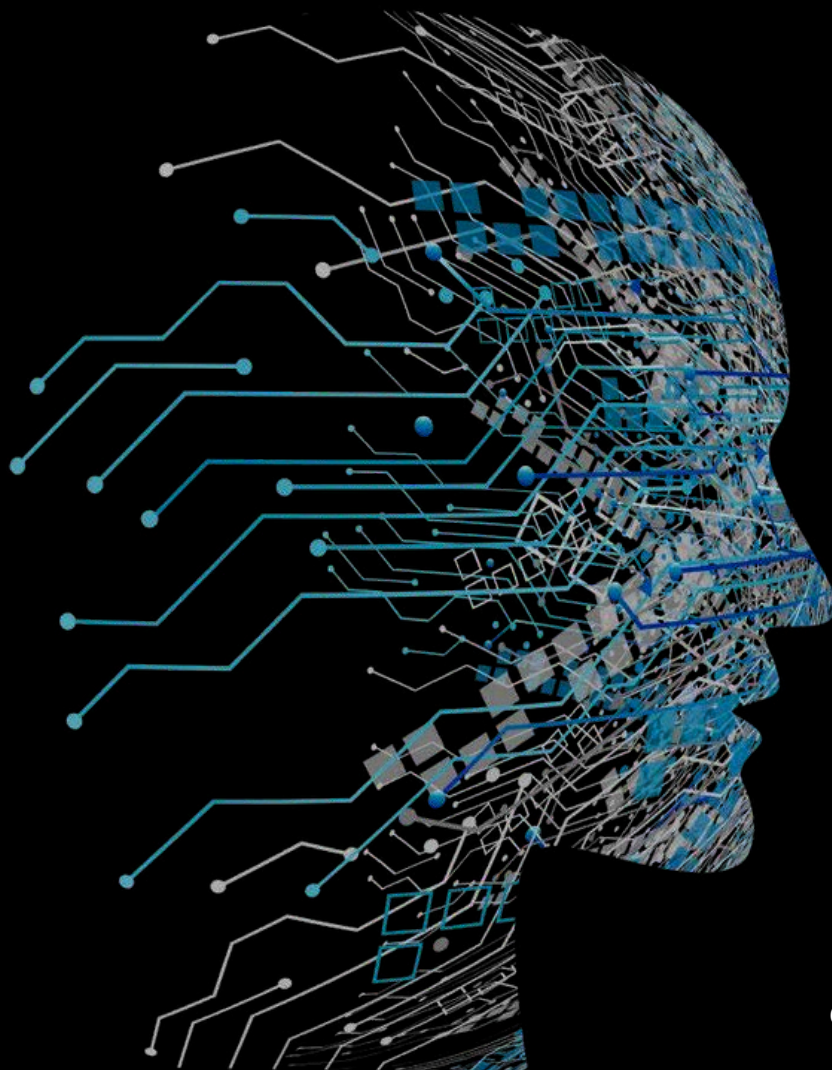
Whether you're an SME or a high-end Enterprise, with bad actors becoming increasingly smarter in their attack methods, safeguarding your business is more crucial than ever.

## **OUR VISION**

Is to create a working and collaboration environment safe from cyberattacks and allowing enterprises to focus on their core business.

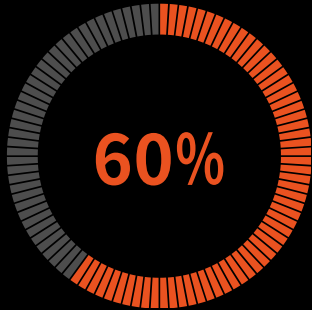
## **OUR MISSION**

Is to protect businesses and uplift their cyber security posture and behaviour.

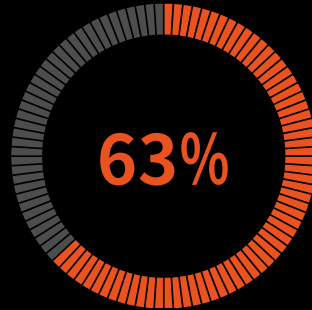




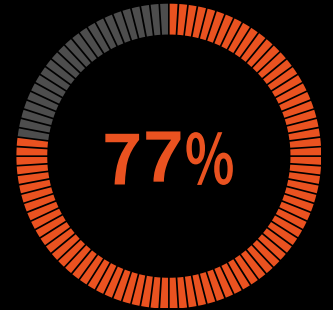
## CYBER SECURITY STATICS FOR SMB



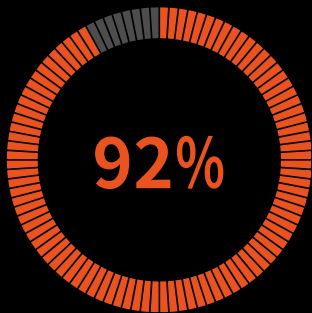
of **SMB's** have experience at least one data breach



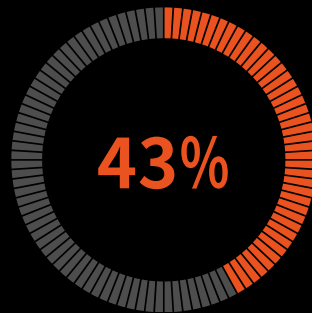
of **SMB's** have faced ransomware



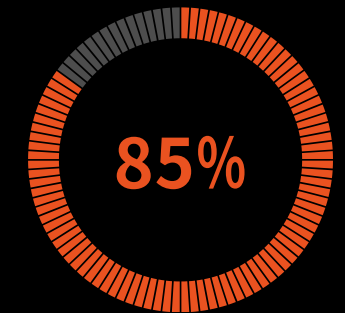
of attacks happen after hours or the weekend



of all cybercrime reports were made by **SMB's**



of cyberattacks specifically target **SMB's**



of data breaches are the result of **human error**

## IT'S NOT IF YOU FACE A CYBER ATTACK! IT'S WHEN!

**\$46,000**

Is the average cost of data breach for **small businesses**

**\$97,200**

Is the average cost of data breach for **medium businesses**

**33,000**

Cyber incidents are reported to the ACSC hotline in last FY

**10 minutes**

An SMB reports a cyber attacks

**309,000**

Australian SMB say they've been targeted by cyberattacks

**every 6 minutes**

A cybercrime is reported



## NOTIFIABLE DATA BREACHES (NDB) SCHEME



Updated Privacy ACT

**Australian organisations are required to notify any individuals likely to be at risk of serious harm by a data breach.**

[Directors liability]



**CRIMINAL RECORD**



### Examples of a data breach:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.



## OUR PURPOSE: CYBER SOLUTIONS FOR SMB

The Australian Cyber Security Centre (ACSC) reports a 23% increase in cybercrime last year, including identity fraud, online banking fraud, and business email compromise. Despite the increase in cyber incidents, nearly half of Australian Small and Medium-sized Businesses (SMBs) allocate less than \$500 annually to cyber security.

Recognising the budget constraints faced by SMBs, Our partnership with Microsoft as a Cloud Solution Provider (CSP), enables us to offer advanced and scalable cloud-based cyber security solutions and ongoing operations, so SMBs can focus on their core business rather than cyber security challenges.



## OUR TRUSTED PARTNERS for SMB PACKAGES

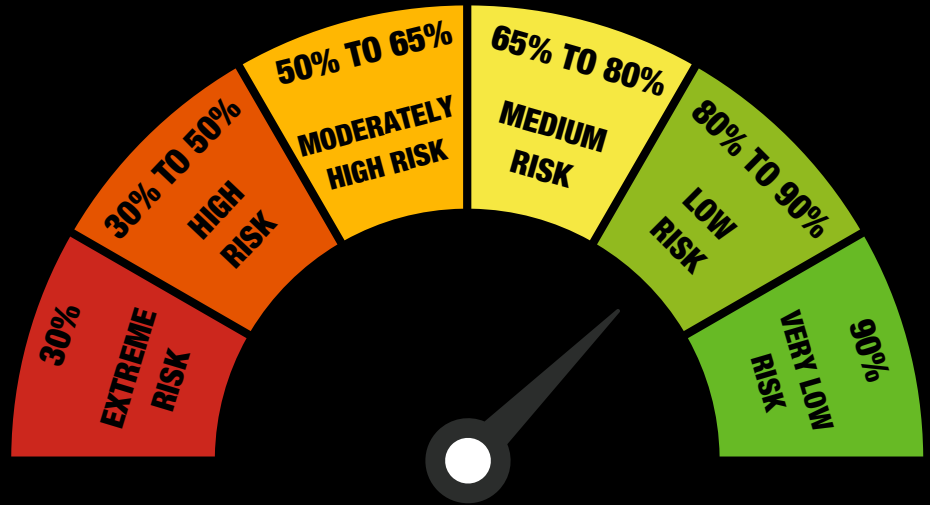
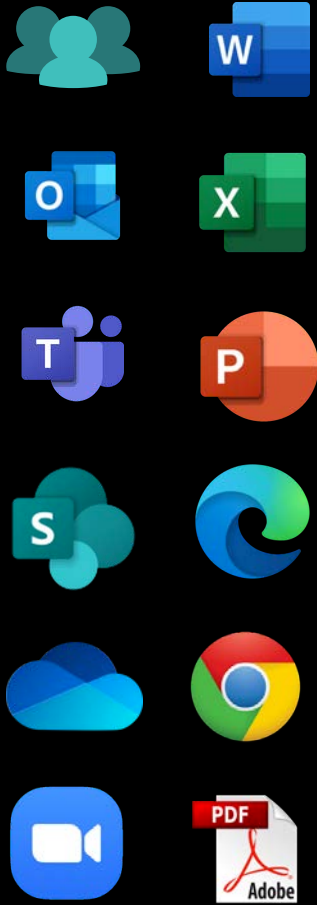


## OUR CERTIFICATES





## How Secure is your collaboration / working environment?



### Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

**Secure Score: 47.23%**

529.49/1121 points achieved



Breakdown points by: Category



Actions to review

32 Regressed | 125 To address | 0 Planned | 0 Risk accepted | 0 Recently added | 0 Recently updated

Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Firewall in macOS	+0.89%	To address	Device
Require MFA for administrative roles	+0.89%	To address	Identity
Turn on Microsoft Defender Antivirus PUA protection in block m...	+0.8%	To address	Device
Block process creations originating from PSEXEC and WMI comm...	+0.8%	To address	Device
Use advanced protection against ransomware	+0.8%	To address	Device
Block Win32 API calls from Office macros	+0.8%	To address	Device
Block execution of potentially obfuscated scripts	+0.8%	To address	Device
Block Office applications from injecting code into other processes	+0.8%	To address	Device

Comparison

Your score: 47.23/100  
Organizations like yours: 46/100

History

Resources

Messages from Microsoft



**CISO ONLINE**  
CYBER SECURITY UPLIFT & AWARENESS

**Microsoft**  
Cloud Solution Provider

**CISO UPLIFT**  
**CYBER SECURITY UPLIFT & AWARENESS**



**CYBER PREMIUM**  
**PACKAGE**





**RECOMMENDED**

## **CISO UPLIFT CYBER PREMIUM**



- **User Behaviour Protection by AI**
  - Next-gen protection with adaptive AI security
- **Identity Protection**
  - Advanced protection of your identity, login details and credentials
  - Seamless login to business Apps using single sign on (SSO) (start with 3 Apps)
  - Work anywhere securely on any Windows device
  - Branded user login experience and terms of use
- **Email Protection**
  - Advanced email protection against next-gen threats
- **Device Protection**
  - Advanced computer & laptop protection against viruses, malware and ransomware
  - Dedicated protection for company-issued and BYOD devices (laptops, smartphones, tablets)
- **Data Protection**
  - Data classification and standard data loss & leakage protection on any device
- **Internet Protection**
  - Standard website filtering
  - Shadow IT report (Cloud Apss visibility)
- **Vulnerability remediation**
  - Advanced Vulnerability Remediation
  - Advanced Log Collection
- **Security Awareness Training**
  - Security Awareness Training for 1 year (25 licenses included)
  - Simulated Phishing attacks (25 licenses included)



**INVESTMENT: ONE OFF IMPLEMENTATION FEE**



**Bulletproof your environment with  
CYBER PREMIUM**



**Microsoft  
Entra**



**Microsoft  
Defender**



**Microsoft  
Intune**



**Microsoft  
Purview**



**Microsoft  
Sentinel**



**Microsoft  
AI**





# CISO UPLIFT - CYBER PREMIUM

## User Behaviour Protection by AI

### Next-Gen protection with adaptive AI security

Next-generation protection leveraging AI to catch and block all types of emerging threats. This rapid evolution underscores the need for agile and innovative security solutions using AI and machine learning models, behavior analysis, and heuristics.

#### How is this achieved?

- Behavior-based and real-time protection, which includes always-on scanning using file and process behavior monitoring and real-time protection.
- Detecting and blocking apps that are deemed unsafe, but might not be detected as malware.



## Identity Protection

### Advanced protection of your identity, login details and credentials

Cyber Security starts with protecting your identity. Protecting your personal and business identity, preserving privacy, maintaining reputation, complying with Privacy ACT, and avoiding financial and legal consequences associated with identity theft and fraud.

#### How is this achieved?

- Dedicated Admin account and user accounts hardening
- Multi Factor Authentication (MFA)
- Conditional Access Policies
- Biometric Sign in
- Password Protection
- Self Service Password Reset



## Identity Protection

### Seamless login to business Apps using single sign on (Start with 3 Apps)

Use your protected M365 login across your business applications such as your accounting or CRM is accomplished by implementing Single Sign-On (SSO). This adds additional security and simplifies access. (3 business applications included)

#### How is this achieved?

- Implementing Seamless Single Sign-On (SSO).
- Securely access multiple applications by using Microsoft 365 credentials.
- Leverage strong Microsoft 365 authentication methods for business applications, such as multi-factor authentication (MFA).





# CISO UPLIFT - CYBER PREMIUM

## Identity Protection

### Work anywhere securely on any windows device

The concept of "Work anywhere securely on any device" refers to the ability to perform work tasks from any location using any device, while ensuring that data and systems remain secure. The Zero Trust security model is often implemented to protect such environments, as it does not automatically trust any environment.

#### How is this achieved?

- Roaming desktop for Windows machines
- Providing users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
- Setting up and pre-configure new devices, getting them ready for productive use.



## Identity Protection

### Branded user login experience

M365 branding package involves personalising the Microsoft portal with your company's branding. You can also present Terms of Use information to end users along with conditional Access policies to employees or guests before getting access.

#### How is this achieved?

- Customising images and text on the sign-in pages to create a consistent experience for users
- Standard Terms of Use statements to employees or guests
- Determine who has or hasn't accepted Terms of Use



## Email Protection

### Advanced email protection against next-gen threats

Email protection is essential for defending against phishing attacks, malware threats, Business Email Compromise (BEC) scams, maintaining business continuity, and preserving reputation and trust in today's digital environment.

#### How is this achieved?

- Anti-malware, Anti-spam and Anti-phishing policies
- Safe attachments and Safe links
- email authentication (DMARC, SPF, DKIM)
- Phishing report email quarantine







# CISO UPLIFT - CYBER PREMIUM

## Device Protection

### Advanced computer & laptop protection against viruses, malware and ransomware

Protecting computers and laptops is essential for protecting data, defending against viruses & malware threats, ensuring business continuity in both personal and organisational contexts.

#### How is this achieved?

- Defender for Endpoint and Windows Security, providing Antivirus protection, continually update and scans for malware and viruses.
- Identify new malware and blocks it within seconds, offering rapid protection against emerging threats
- Windows Firewall as a security feature that helps to protect your device by filtering network traffic that enters and exits your device.



## Device Protection

### Dedicated protection for company-issued and BYOD devices (Laptops, Smartphones, Tablets)

Device protection such as laptops, smartphones and tablets is essential for safeguarding Apps and protection for company data on any device preserving privacy, preventing identity theft, enabling remote device management.

#### How is this achieved?

- Device encryption
- Mobile Device Management (MDM) policies
- Mobile Application Management (MAM) policies
- Remotely wipe lost or stolen devices
- Secure and manage M365 apps (Outlook, Teams, OneDrive, Word, Excel, PowerPoint) on any devices
- Protect organisational data on company provided and bring on your own (BYOD) devices
- Mobile Defender and Antivirus for Android and iOS devices



*\* a security profile needs to be pushed into mobile devices to achieve all capabilities*

*\* computers and laptops require windows 11 professional and needs to be AAD joint*



# CISO UPLIFT - CYBER PREMIUM

## Data Protection

### Data classification and standard data loss & leakage protection on any device

Data classification and sensitive data loss and leakage protection are crucial for safeguarding sensitive information and preventing unauthorised access. By implementing data loss prevention (DLP) measures, you can reduce the risk of data breaches, regulatory fines, and reputational damage.

#### How is this achieved?

- Identify and classify sensitive information, such as personal data, your intellectual property (IP), or financial records, across your data estate.
- Classifying and labelling your documents and data (structured and unstructured for supported platforms)
- Define policies to control access to sensitive information and prevent unauthorised access and unauthorised change.
- Tracks the movement of sensitive information within the organisation.



## Internet Protection

### Standard Website filtering

Website filtering is crucial for you to prevent access to malicious or inappropriate websites, enhancing network security whilst maintaining a more productive work environment

#### How is this achieved?

- Users are blocked from accessing certain websites, categorised as restricted, regardless of their location.
- Access to detailed web reports from a single central location, providing insights into both attempted and actual web accesses, enhancing visibility into web usage.



## Internet Protection

### Shadow IT Report (Cloud Apps visibility)

Shadow IT refers to the use of software, applications, and services available on the Internet without explicit approval or oversight from the IT department.

#### How is this achieved?

- Visibility into all cloud applications to obtain a comprehensive picture of cloud apps activity and enact security measures accordingly





# CISO UPLIFT - CYBER PREMIUM

## Vulnerability remediation

Vulnerability remediation is a critical process, involving the identification and resolution of security vulnerabilities within your M365 environment. This includes addressing weaknesses that could be exploited by cyber threats in software, systems, or cloud. The goal is to patch, block, or fix vulnerabilities to prevent potential data breaches or system disruptions.

### How is this achieved?

- Identify, assess, remediate, and track all your biggest vulnerabilities across your most critical M365 assets, all in a single solution.
- Rapidly and continuously prioritises the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.



## Advanced log collection

Regular advanced log collection is required to detect and mitigate security incidents, enhancing overall cybersecurity resilience.

### How is this achieved?

- M365 unified log collection and centralised management of audit logs, which includes collecting and processing logs from various sources.
- Logs essential for threat detection, compliance, and security incident management.
- Archive logs for compliance purposes



## Security Awareness Training & Simulated Phishing

Human error is how most organisations get compromised and hackers are always looking for new ways to exploit vulnerabilities and this include humans! To keep your employees educated on the latest tactics we offer one (1) year of a computer-based cybersecurity awareness training (starts with 25 user) as well as our proactive simulated phishing attacks (incl. 25 free licenses)

### How is this achieved?

- Baseline security awareness training
- Ongoing monthly videos followed by a quiz to test the users understanding
- Reminders of key lessons learnt from the animated video in the form of an infographic and poster
- Simulated Phishing emails that are tailored and customised to test your employees.





## All SMB Packages

Secure Cloud Services	CYBER ESSENTIALS	 RECOMMENDED CYBER PREMIUM	CYBER ELITE
<b>Identity Protection</b> Login details and passwords	✓ Standard	✓ Advanced	✓ Advanced
<b>Email Protection</b>	✓ Standard	✓ Advanced	✓ Advanced
<b>Device Protection</b> Computers, Laptops, Smartphones, tablets	✓ Standard	✓ Advanced	✓ Advanced
<b>Data Protection</b> Data Loss and Leakage	✗	✓ Standard	✓ Advanced
<b>Internet Protection</b>	✗	✓ Standard	✓ Advanced
<b>User Behaviour Protection by AI</b>	✗	✓ Advanced	✓ Advanced
<b>Vulnerability Remediation</b>	✓ Standard	✓ Advanced	✓ Advanced
<b>Security Awareness Training</b>	✓ Standard	✓ Advanced	✓ Advanced
<b>Suitable for but not subject to</b>	Micro Businesses with 1 to 10 users	Small Businesses with 1 to 250 users	Medium Sized Businesses with 250 to 500 users





**CISO ONLINE**  
CYBER SECURITY UPLIFT & AWARENESS

**Microsoft  
Surface**  
Authorized Reseller

## ULTIMATE ENDPOINT SECURITY WITH MICROSOFT SURFACE

When you purchase a Microsoft Surface laptop from CISO Online, you have the opportunity to natively integrate your laptops with Cyber Premium security features for the ultimate security.



## SECURITY OUT OF THE BOX

Our SMB cyber packages are crafted to offer comprehensive protection tailored specifically for small and medium-sized businesses. By integrating these packages with Microsoft's industry-leading, built-in security features, Surface devices safeguard you and your data, no matter where you work.



### Hardware

Easily encrypt and protect your data in a sandboxed environment that stores passwords, PIN numbers and certificates with Trusted Platform Module 2.0. (TPM 2.0)



### Firmware

Automated updates to Microsoft firmware make start up faster and more secure, while DFCI enables remote management of hardware components. (camera, Bluetooth)



### AI-enabled

Ultrathin laptop designed for enhanced AI experiences, with industry leading AI acceleration to unlock powerful new features.



### Cloud

Get peace of mind with always-on security features to keep data, devices and identities more secure than ever.



**CISO Uplift  
SMB Packages**



**CISO Operation  
SMB Packages**



**CISO Defence  
SMB Packages**



**Cyber Security Uplift  
Risk Based Approach**



**CISOaaS  
CISO on Demand**



**Secure Laptops**



**Essential 8**



**Penetration Testing**



**Security Risk  
Assessment**



**Security Solution  
Architecture**



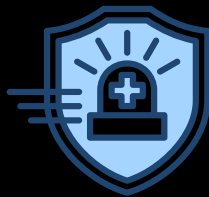
**Security Implementation**



**Business Continuity &  
Disaster Recovery  
(BCDR)**



**Digital Forensics**



**Incident Response**



**ISO27001/ISMS  
Consultancy**



**IRAP Assessment**



**Governance, Risk,  
Compliance (GRC)**



**Security Operation  
Centre (SOC)**



**Cybersecurity  
Awareness Training**



**Simulated Phishing  
Attack & Phish Alert**



**CISO ONLINE**  
CYBER SECURITY UPLIFT & AWARENESS

**Contact us:**



[cisoonline.com.au](http://cisoonline.com.au)  
[info@cisoonline.com.au](mailto:info@cisoonline.com.au)



1300 710 677



Three International Towers, Level 24,  
300 Barangaroo Ave, Sydney, NSW 2000, Australia



AUG 2024