Microsoft Defender for Office 365

Integrated and Holistic protection for all of Office 365

Overview

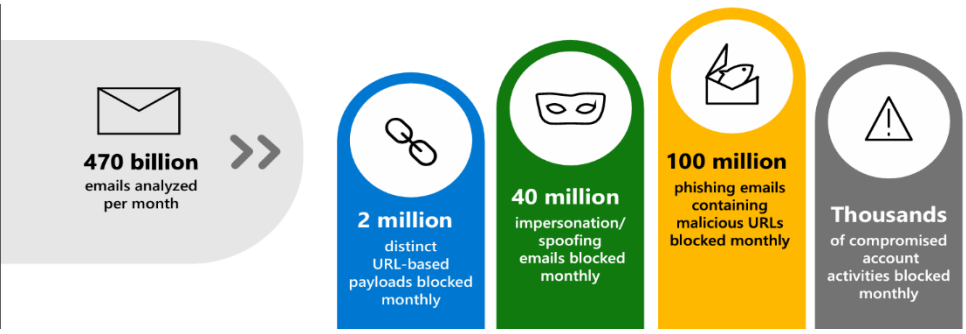
Securing an organisation has never been simpler.

Microsoft Defender for Office 365 offers a comprehensive solution to protect your organisation and employees from advanced, targeted and zero-day phishing, malware and business email compromise attacks.

Microsoft Defender for Office 365 is part of an integrated set of threat protection solutions from Microsoft that offer a holistic view of security for your organisation.

Microsoft 365 Defender and Microsoft Defender for Cloud deliver the most comprehensive XDR solution on the market and Microsoft Sentinel is an innovative cloud-native SIEM.

With the integration of these tools, defenders have more actionable context than ever so they can focus on stopping threats across the entire enterprise.



WYCOM TECHNOLOGY

At-a-Glance

The frequency and sophistication of cyber events have increased dramatically, and with more organisations pivoting to embrace hybrid work, we're living through unprecedented growth of digital interactions.

Key Benefits

Protect against the latest email security threats
Email remains the number one entry point for cyberattacks. Help ensure that email-based cyberattacks - including phishing via malicious links or QR codes, business email compromise (BEC), and malware - don't reach your users.

Secure your collaboration platform
Help ensure safe collaboration across Microsoft Teams, SharePoint, and OneDrive - with inline protection against malicious URLs, real-time detonation of attachments and links, and other features. Full visibility into cyberthreats with alerts and data across Microsoft collaboration tools.

Get an AI-powered defence
As adversaries improve their techniques using AI, it's critical that your defence does the same. Help protect your business from the most sophisticated cyberthreats. Microsoft uses language models with sentiment analysis to provide AI-powered email and collaboration security.

Disrupt sophisticated cyberattacks with XDR
Use automated capabilities with extended detection and response (XDR) to disrupt in-progress attacks. XDR technology analyses the attacker's intent, identifies compromised assets, and contains cyberthreats in near-real time, minimising the impact of attacks—such as business email compromise (BEC)—on your organisation.

Contact Wycom:

Location:
1/20 Donaldson St,
Wyong NSW 2259

Call Us:
02 4351 1361

Email Us:
info@wycom.com.au

Website:
www.wycom.com.au

Microsoft Defender Features

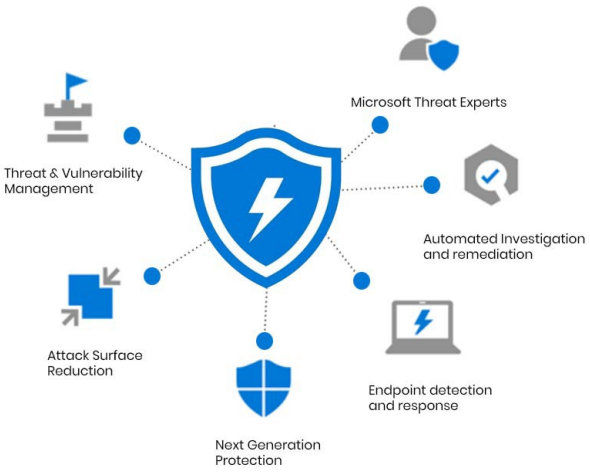
AI-Powered sentiment analysis
Help ensure effective filtering of malicious emails and messages with a comprehensive prevention stack, including generative AI-based analysis.

Inline user protection
Block and prevent malicious links and attachments directly in Outlook and Microsoft Teams with user awareness banners.

BEC (Business Email Compromise) attack disruption
Get AI-based containment of BEC attacks through automatic disabling of compromised users, isolation of compromised devices, and post-delivery removal of malicious emails.

Security posture optimisation
Apply recommended security configurations to strengthen your organisation's resilience against email and collaboration-based threats.

Priority account support
Get heightened security and configuration for the most sensitive accounts in your organisation.



Investigation and hunting
Uncover and mitigate cyberthreats with a unified incident experience that offers complete visibility into the cyberattack lifecycle and empowers security operations (SecOps) to act decisively.

Want to see more?
Click here to view our Microsoft Defender for 365 Video

Wycom Technology Pty Ltd
ABN: 63 150 235 144
Phone: 02 4351 1361 **Email:** info@wycom.com.au
Website: www.wycom.com.au

Top 10 Advantages of Defender for Office 365

Feature	Details
1. Industry leading protection	• Built on Microsoft's trillion-day security signals. • Low latency file detonation. • URL detonation in mail-flow and at time-of-click. • Enhanced spoof protection beyond DMARC Checks.
2. Integrated protection across Office 365	• Advanced protection for Teams, SharePoint, and OneDrive. • Time-of-click protection within Office 365 apps (Word, Excel, PowerPoint) and Microsoft Teams. • Native client experiences increase user awareness. • Native hover experience to show original URLs for wrapped links.
3. Easy to configure policy settings	• Preset security policies for quick deployment • Simple checkbox policies. • Configuration analyser for policy tuning. • Advanced delivery for phishing simulations and SecOps mailboxes
4. Detailed and actionable reporting	• Priority Account Protection tracks critical users. • Reports uncover configuration gaps. • Enriched details for SOC (Security Operation Centre Team) effectiveness. • APIs to create customised detection reports.
5. Powerful campaign analysis	• Big-picture views of entire email campaigns. • Easy identification of configuration flaws, vulnerable users. • Integrated with automated investigation and response.
6. Threat investigation & hunting	• Advanced tools that reduce investigation time by 92%. • Detailed email analysis tools with API access. • Ability for SecOps to submit emails, URLs, files to Microsoft for analysis.
7. Automated response	• Automated response playbooks integrated across Office 365. • Trigger automated investigations manually. • Integrated investigation and response across Microsoft 365 Defender workloads.
8. Compromise detection & Response	• Based on anomalous email patterns and Office 365 activities. • Configurable sending limits to limit scope of breach. • Disable external forwarding automatically. • Powerful automation for quicker remediation.
9. Built-in Simulation & Awareness Training	• Powerful phishing simulation using direct injection. • No whitelisting required of IP's and URL. • Assign end user training based on simulation results. • Detailed reporting of clicks, IPs, devices and browsers used. • Outlook report message add-on integration.
10. Microsoft 365 Defender	• XDR integration to amplify prevention, detection, and response across Microsoft products • Automated Investigation and response integration across Defender for Office 365, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and Azure Active Directory. • Powerful advanced hunting across the digital estate

Wycom Technology Pty Ltd
ABN: 63 150 235 144
Phone: 02 4351 1361 **Email:** info@wycom.com.au
Website: www.wycom.com.au

Microsoft Defender for 365 Packages

FEATURES	Defender for Office 365 (Plan 1) CORE + ATS + EDR	Defender for Office 365 (Plan 1) CORE + ATS + EDR + MDR
Protection against email and collaboration-based cyberattacks across email, Teams, SharePoint, and OneDrive	✓	✓
Real-time protection for malicious links and QR codes	✓	✓
Protection against zero-day malware and viruses in attachments	✓	✓
Language model-based sentiment analysis to protect against phishing campaigns	✓	✓
Protection for internal email	✓	✓
Real-time reporting	✓	✓
Advanced protection for Teams		✓
Support to open documents in protected view for added cybersecurity		✓
Cyberattack simulation training		✓
Detailed reporting to identify and analyse recent cyberthreats		✓
Tracking of cyberthreat campaigns that might impact your organization		✓
Automated investigation and response		✓
XDR capabilities, such as cross-domain hunting and incident correlation		✓

Wycom Technology Pty Ltd
ABN: 63 150 235 144
Phone: 02 4351 1361 **Email:** info@wycom.com.au
Website: www.wycom.com.au