
CROFT
BESPOKE BY DESIGN
Managed IT Services and Support
Communications and Connectivity
Business Mobile Services

CROFT

BESPOKE BY DESIGN

Unlocking Business Premium: Secure IT for the Modern Workplace

Contents

The Why Behind the Upgrade

Risks and Concerns

Real Time Collaboration

Although significant effort and resources were dedicated to this during the Covid pandemic, many businesses continue to face challenges with fragmented systems and managing multiple disconnected tools and workflows.

Security

Costs of a cyberattack go beyond just financial costs and can impact productivity, future opportunities, and business reputation leading to negative long-term effects.

Cost

Complex solutions involving multiple vendors often increase expenses due to overlapping subscriptions and added complications, missing out on integrated benefit.

Source: SMB Cybersecurity Research Report 2024

Security is Top of Mind for Organisations

82%

Of ransomware attacks in the past Year targeted small businesses[1]

1 in 3

SMBs state that they had a security breach in the last year[2]

+90%

Over 90% of SMBs think cyber security is extremely important to their business[2]

80%

Of SMBs plan to increase their cyber security spending[2]

Source:

1. The Devastating Impact of Ransomware Attacks on Small Business, April 04, 2023

2. SMB Cybersecurity Research Report 2024

Risks and Concerns

False Sense of Protection

Despite cyber security awareness, some SMB mindsets put companies at increased risk of an attack.

Rising and Unexpected Costs of a Cyberattack

Costs of a cyberattack go beyond just financial costs and can impact productivity, future opportunities, and business reputation leading to negative long-term effects.

Increasing Operational Challenges

Security plays a critical role across business processes, both internal and external, and managing the threat landscape is important to not disrupt operations.

Source: SMB Cybersecurity Research Report 2024

Licensing Overview

Consumer → For Home
- Microsoft 365 Personal
- **Microsoft 365 Family**

SMB (<300) → For Business
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- **Microsoft 365 Business Premium**

Enterprise (>300) → For Enterprise
- Office 365 E1
- Office 365 E3 / EMS E3 / Windows E3
- Office 365 E5 / EMS E5 / Windows E5
- Microsoft 365 E3
- **Microsoft 365 E5**

For Enterprise → Firstline
- Microsoft 365 F1
- **Microsoft 365 F3**

Academic → For Education
- Microsoft 365 A1
- Microsoft 365 A3
- **Microsoft 365 A5**

New capabilities coming in 2026	Business Basic Lightweight web and mobile apps to kickstart your business.	Business Standard Powerful web, mobile, and desktop apps to run your business.	Business Premium Everything your business needs to be more productive and secure.	Office 365 E1 Lightweight web and mobile apps, and basic security.	Office 365 E3 Powerful productivity apps, basic security, and identity management capabilities.	Microsoft 365 E3 Powerful Productivity apps with enhanced security and compliance capabilities.	Microsoft 365 E5 Best-in-class AI-powered productivity apps with advanced security, compliance, analytics, and AI readiness capabilities.
Copilot Chat enhancements	●	●	●	●	●	●	●
Security, management, and analytics for Copilot Chat	●	●	●	●	●	●	●
URL checks in Outlook and Office apps (web and mobile)	●	●		●			
+50 GB email storage	●	●	●				
Microsoft Defender For Office 365 P1					●	●	
Microsoft Intune Remote Help						●	●
Microsoft Intune Advanced Analytics						●	●
Microsoft Intune P2						●	●
Intune Endpoint Privilege Management							●
Intune Enterprise Application Management							●
Microsoft Cloud PKI							●
Microsoft Security Copilot							●

Price Adjustments Driven by Microsoft

License Name	% Increase
Microsoft 365 Business Basic	16%
Microsoft 365 Business Standard	12%
Microsoft 365 Business Premium	N/A
Microsoft 365 E3	8%
Microsoft 365 E5	5%

Microsoft 365 SKUs for SMBs

Business Basic

Apps and services to kickstart your business.

Cloud Services

Web and Mobile Apps

Foundational Security

- Identity & access control
- Exchange Online Protection
- Mobile device management

Business Standard

Desktop apps and cloud services to securely connect, collaborate, and create.

Cloud Services

Web and Mobile Apps

Foundational Security

- Identity & access control
- Exchange Online Protection
- Mobile device management

Business Premium

Everything your business needs to be more productive and secure

Cloud Services

Web and Mobile Apps

Comprehensive Security

Microsoft 365 SKUs for SMBs

Business Premium

Everything your business needs to be more productive and secure

Cloud Services

Teams Exchange OneDrive SharePoint Bookings

Web and Mobile Apps

Outlook Word Excel PowerPoint Loop Clipchamp

Comprehensive Security

MS Intune MS Purview MS EntraID Azure Desktop MS Defence Defender for Office 365

- Microsoft Entra ID
- Microsoft Intune
- Microsoft Defender
- Microsoft Purview
- Azure Virtual Desktop
- Microsoft Defender for Office 365

Security Feature Breakdown

Layered Security Improves Your Security Profile

Microsoft 365 Business Premium

Identity and Access Controls

Microsoft Entra ID Plan 1

Multi-Factor authentication to protect against password loss

Passwordless authentication

Self Service Password Reset

Conditional Access to provide access controls to work data

Cloud App Discovery to discover Shadow IT

Device Management

Microsoft Intune

Keep devices up-to-date with the latest OS

Protect devices from bad actors and misuse

Allow more secure access to sensitive data – even from personal devices

Remotely wipe data from lost and stolen devices

Pre-load access to Wi-Fi, VPN with certificate management

Device Security

Microsoft Defender for Business

Ransomware protection with AI powered EDR with automatic attack disruption

Next gen-AV protection

Protection across Android, iOS,Max, Windows and Linux

Threat and vulnerability management

Monthly summary reports

Email and App Security

Microsoft Defender for Office 365

AI powered LLM based threat protection

Phishing and malware defense across email, Microsoft Teams, OneDrive and SharePoint

SafeLinks with time of click URL filtering

Safe Attachments with real-time attachment scanning in sandbox

Data Security

Microsoft Purview

Data Loss Prevention to protect sensitive data such as credit card or social security numbers

Classify and label sensitive data

Apply protection such as “Do Not Forward” or “Encrypt Email”

Audit, search and legal hold.

Layered Security Improves Your Security Profile

Microsoft 365 Business Premium

Identity and Access Controls

Microsoft Entra ID Plan 1

Multi-Factor authentication to protect against password loss

Passwordless authentication

Self Service Password Reset

Conditional Access to provide access controls to work data

Cloud App Discovery to discover Shadow IT

Device Management

Microsoft Intune

Keep devices up-to-date with the latest OS

Protect devices from bad actors and misuse

Allow more secure access to sensitive data – even from personal devices

Remotely wipe data from lost and stolen devices

Pre-load access to Wi-Fi, VPN with certificate management

Device Security

Microsoft Defender for Business

Ransomware protection with AI powered EDR with automatic attack disruption

Next gen-AV protection

Protection across Android, iOS,Max, Windows and Linux

Threat and vulnerability management

Monthly summary reports

Email and App Security

Microsoft Defender for Office 365

AI powered LLM based threat protection

Phishing and malware defense across email, Microsoft Teams, OneDrive and SharePoint

SafeLinks with time of click URL filtering

Safe Attachments with real-time attachment scanning in sandbox

Data Security

Microsoft Purview

Data Loss Prevention to protect sensitive data such as credit card or social security numbers

Classify and label sensitive data

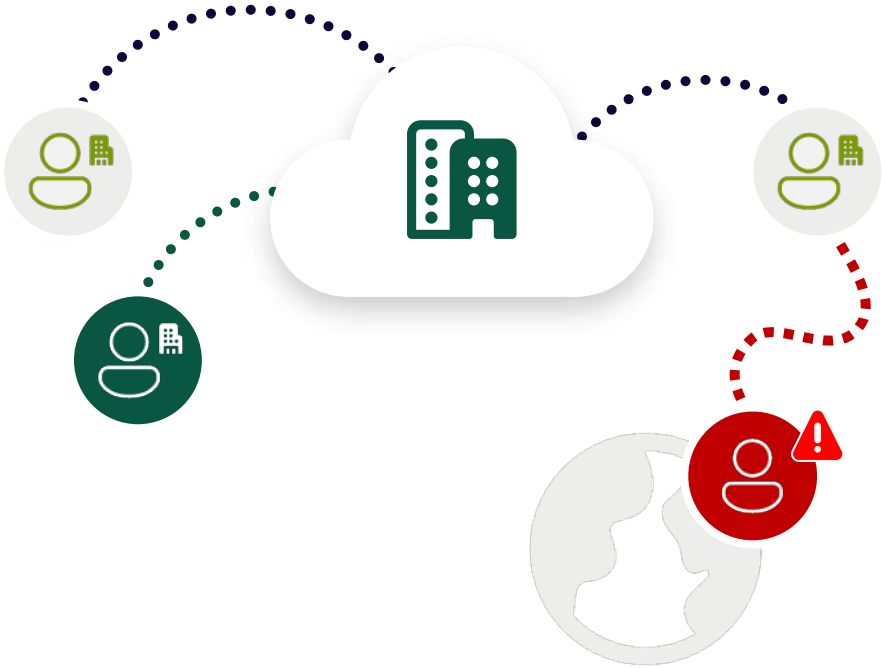
Apply protection such as “Do Not Forward” or “Encrypt Email”

Audit, search and legal hold.

Real World Examples

Challenge

Northwind Traders' employees need access to work data as they work remotely. However, bad actors may try to gain access to work information by stealing passwords and trying to gain access to the work data from anywhere in the world.

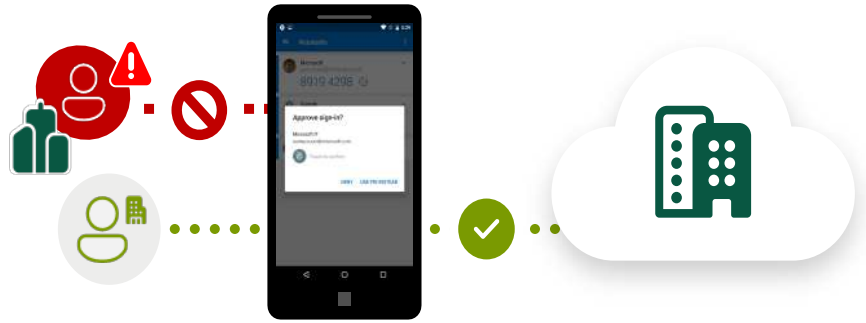


1Source: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ based on MSFT internal study

Solution

Entra ID – Conditional access

- Enforce advanced Multifactor Authentication (MFA) and Conditional Access policies with Microsoft 365 Business Premium.
- Ensure only authorised individuals access work data, regardless of location.
- Block access or require extra authentication for login attempts from non-business countries.



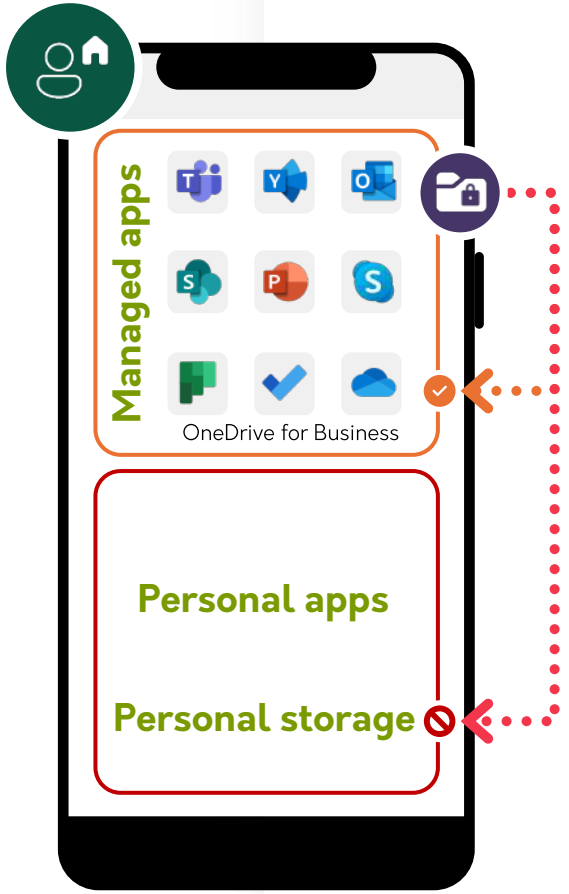
With Microsoft Entra ID P1 (formerly known as Azure AD Premium Plan 1)

- **Multifactor authentication**
- **Conditional Access policies**
- **Self service password reset**

99% **of identity attacks are thwarted by multifactor authentication.**[1]

Challenge

A Northwind Traders marketing manager is using her personal device to check company email and receives a confidential business plan. She accidently saves it to her personal share, which is not secure, for later reference.



Solution

Protection work data on Personal devices

With Microsoft 365 Business Premium, you can use Intune App Protection Policies to keep work apps separate from personal apps and ensure work documents are saved only in secure locations like OneDrive for Business.

64% of SMBs allow employees to access work data on personal phones and computers.[1]

50%+ of respondents in critical infrastructure sectors report that they have experienced significant security incidents involving mobile or IoT devices.[2]

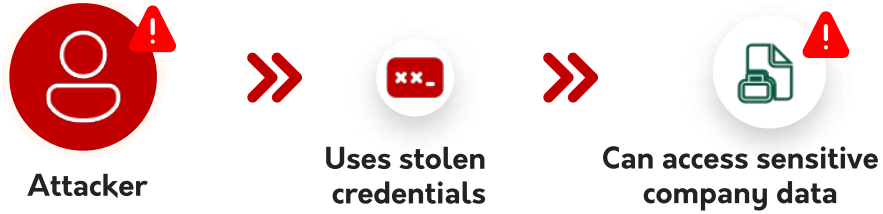
1Source: Microsoft Internal Research of SMBs (2-299 employees)

2Source: The Verizon 2024 MobileSecurity Index (MSI)

Challenge

A Northwind Traders employee receives an email with a link to a secure document, ostensibly from a well-known organisation. They enter their credentials to view it, but it fails to load. They move on to other work and forget about the glitch. This was a phishing attack.

They just delivered their username and password to hackers, who can now use it to access email and other Northwind accounts.



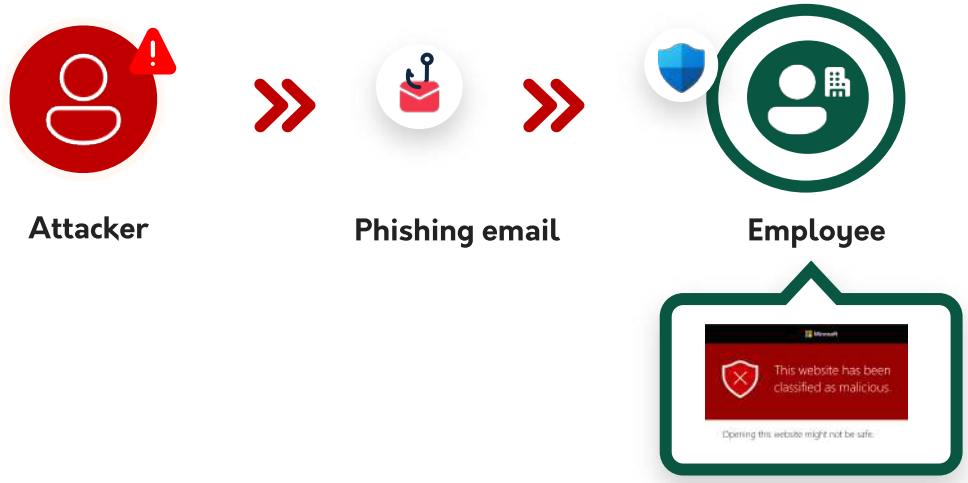
1 in 4 SMBs experience a security breach[1]

1 Source: Microsoft security in the New Work environment research pane, 2022

Solution

AI-powered phishing defenses

A Northwind Traders employee receives an email with a malicious link to a document. Microsoft 365 Business Premium INCLUDES Defender for Office 365, which check the link in a "security sandbox" , alert the user to the threat and protect against the attack. It will also check attachments in real-time for malware and other threats.

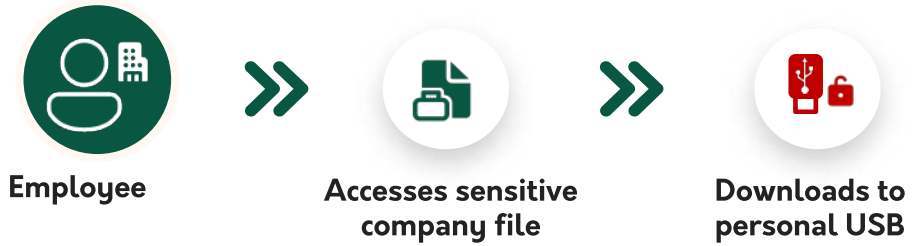


With Microsoft Defender for Office 365

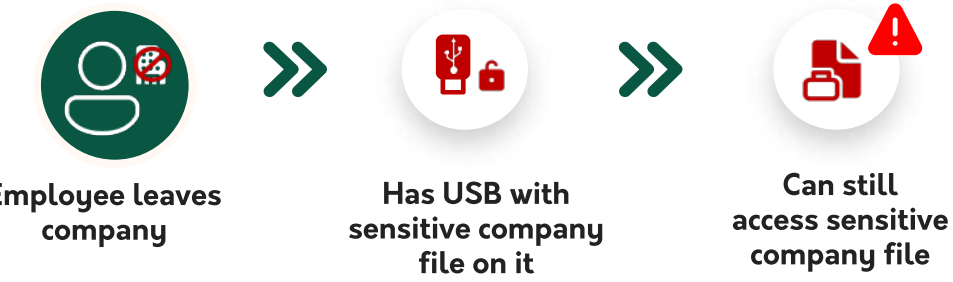
- Scan every attachment with Safe attachments in security sandbox
- Time of click URL filtering with Safe Links
- Anti-spoofing
- AI-powered enhanced email defense with a 99.995% attacker intent detection accuracy and filtering

Challenge

Northwind Traders sometimes password-protects Excel spreadsheets to guard sensitive company information. However, this security measure is used inconsistently, and many confidential documents are emailed around or saved on USB keys without any protections.



As a result, if the employee leaves the company confidential document is leaked, which is a business risk.

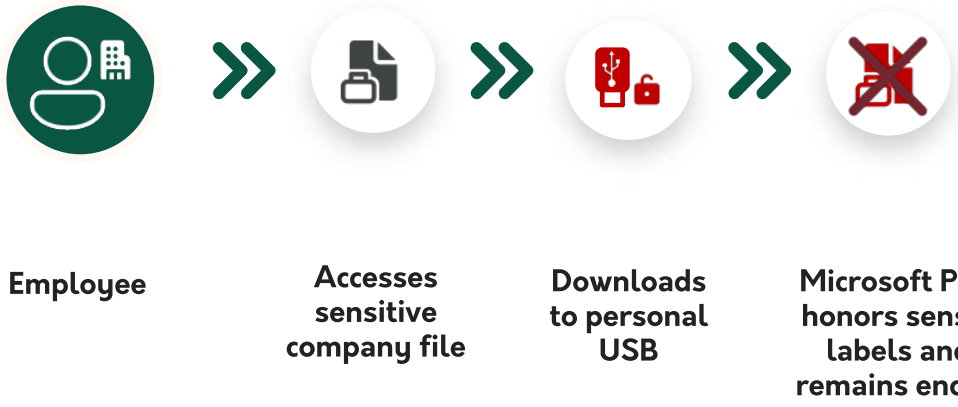


>80% of small and medium businesses handle PII data.[1]

Solution

Safeguard sensitive data

Microsoft Business Premium includes Microsoft Purview, which helps label and protect sensitive documents as "Highly Confidential" with features like encryption and forwarding restrictions. When using Copilot for Microsoft 365, the system honors sensitivity labels and verifies permissions before allowing access. If an employee leaves and has the document on a USB, they won't be able to access it since it is tied to their work credentials.



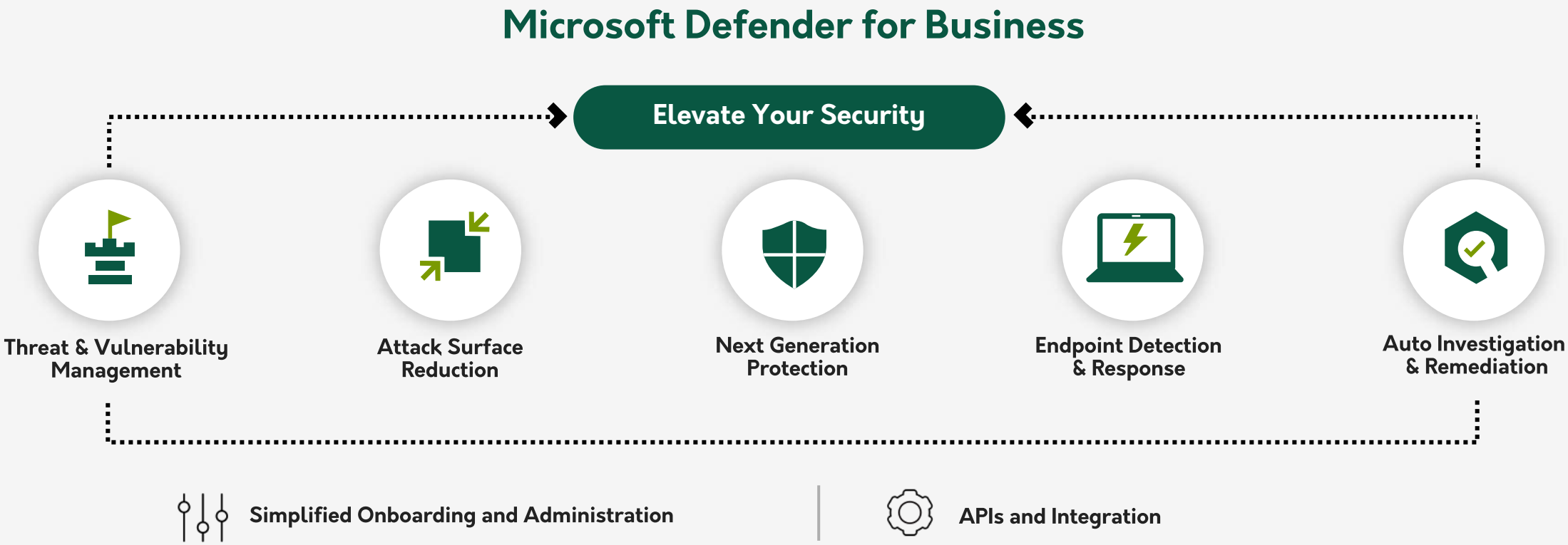
>55% SMBs say they are concerned about employees leaving their company with data on personal devices.[2]

1 **Source:** Microsoft Internal Research of SMBs (2-299 employees)

2 **Source:** Microsoft Internal Research of SMBs (2-299 employees)

Microsoft Defender for Business

Beyond Traditional Anti-Virus



Defender for Business brings enterprise grade endpoint security to Microsoft 365 Business Premium

		PRE MDB	WITH MDB	
		MS 365 Business Premium3	MS 365 Business Premium3	MS Defender for Business (MDB)[3]
eDiscovery and Audits	eDiscovery	•	•	
	Litigation Hold	•	•	
	Email Archiving	•	•	
Information Protection	Information Rights Management	•	•	
	File classification/labeling	•	•	
	File tracking and revocation	•	•	
Data Loss Prevention	Message Encryption	•	•	
	Data Loss Prevention	•	•	
	Data App Security	•	•	
Email and Collaboration Security	Safe links	•	•	
	Safe Attachments	•	•	
	Anti-phishing	•	•	
Device management	Windows device setup & management	•1	•1	
	Device health analytics	•	•	
	Mobile Device Management	•	•	
	Mobile App Management	•	•	
Identity and Access Management and Security	Risk based Conditional access	•	•	
	Multi-factor authentication	•	•	
Endpoint Security	Centralised management	•	•	•
	Simplified client configuration		•	•
	Next-gen protection	**Win10**	•	•
	Attack Surface Reduction	**Win101**	•	•
	Network Protection		•	•
	Web Category blocking		•	•
	Endpoint detection and response		•	•
	Cross platform support (iOS/Android/Mac)		•4	•4
	Automated investigation and response		•2	•2
	Threat and vulnerability		•	•
	Threat intelligence		•2	•2

1. Limited
2. Optimised for SMB
3. Microsoft Defender for Business is available in Microsoft 365 Business Premium and as a standalone SKU. Read the blog post to **learn more**.

4. iOS, and Android requires Microsoft Intune. Intune is included in Microsoft 365 Business Premium. Please see Documentation for more detail.

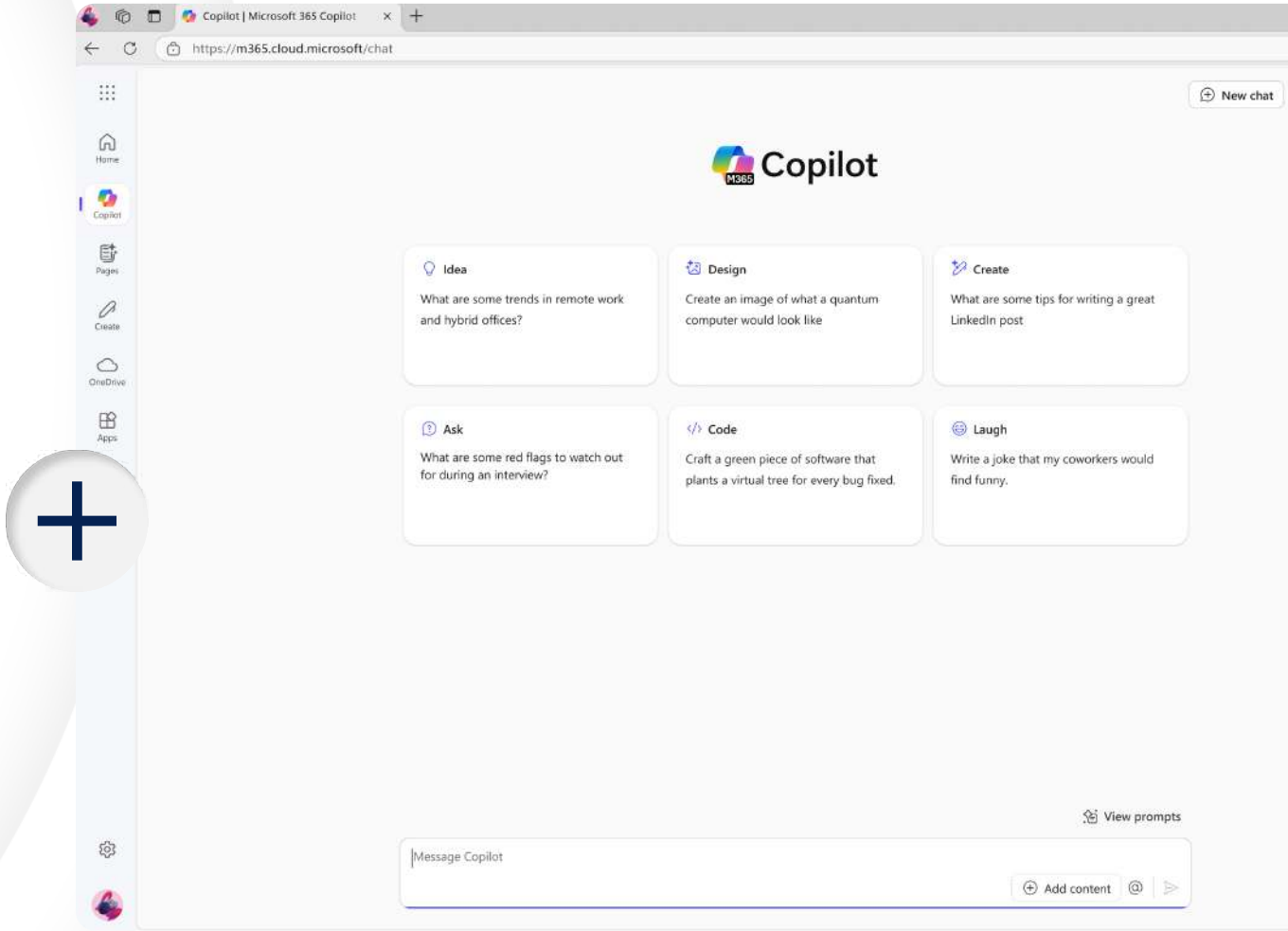
Copilot

Microsoft Approved AI Chat Tool

Microsoft 365 Copilot Chat is an AI chat tool built specifically for work. It uses the latest AI models and data from the web to answer your questions, generate content and ideas, and find information. It also protects your data so information from your chat conversation does not get exposed to the public.

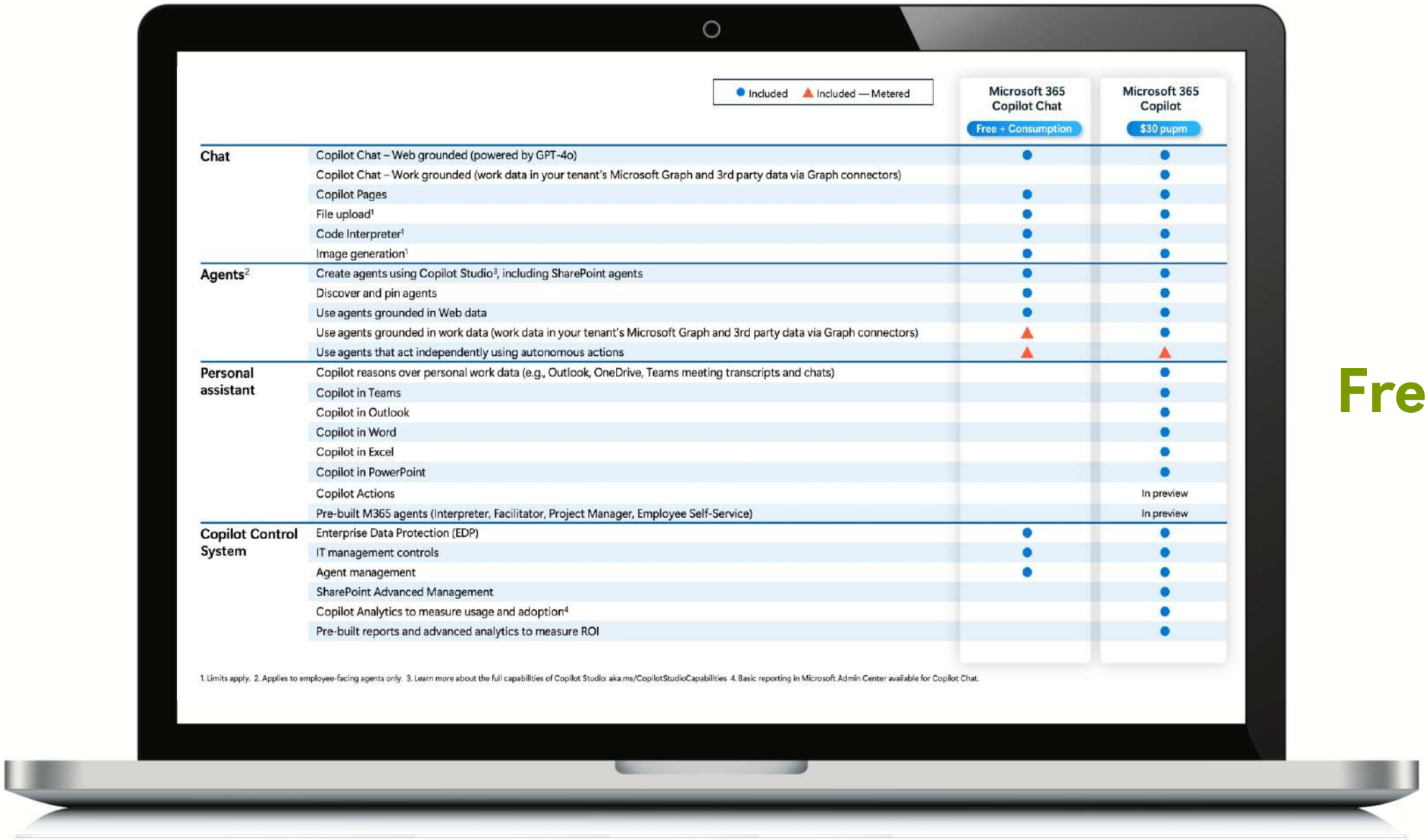
In addition, with Copilot Chat you can:

- Upload files to get responses based on information from your work documents, presentations, etc [1].
- Generate images 1 and data visualisations.
- Refine and collaborate on chat responses.
- Connect Copilot Chat to your organization data like team documents and internal SharePoint sites [2].



1 Image generation and file upload limits apply.

2 Connecting Copilot Chat to your organisation data is only available if your organization admin has enabled this capability.



● Included ▲ Included — Metered

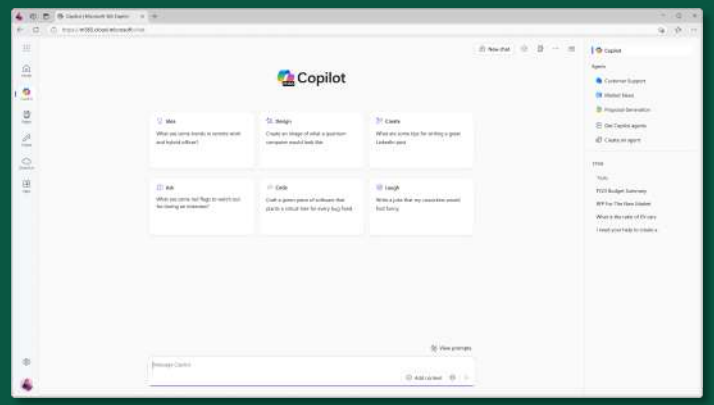
		Microsoft 365 Copilot Chat Free + Consumption	Microsoft 365 Copilot $30 pupm
Chat	Copilot Chat – Web grounded (powered by GPT-4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload[1]	●	●
	Code Interpreter[1]	●	●
	Image generation[1]	●	●
Agents[2]	Create agents using Copilot Studio[3], including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded in Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g., Outlook, OneDrive, Teams meeting transcripts and chats)		●
	Copilot in Teams		●
	Copilot in Outlook		●
	Copilot in Word		●
	Copilot in Excel		●
	Copilot in PowerPoint		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		In preview
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption[4]		●
	Pre-built reports and advanced analytics to measure ROI		●

1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

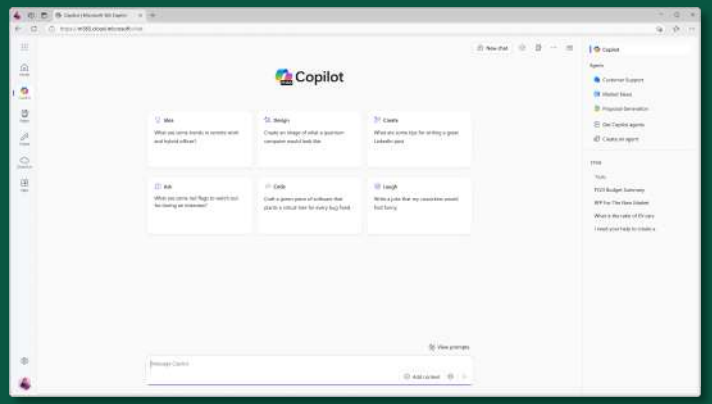
Free vs Paid

Access Copilot Chat From Where You're Working

M365Copilot.com

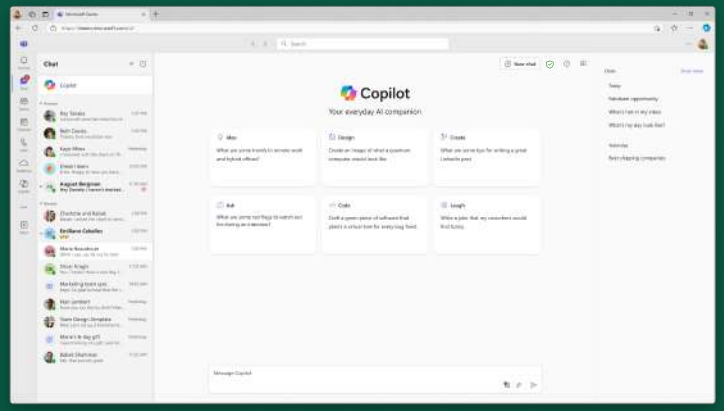


Microsoft 365 Copilot App*

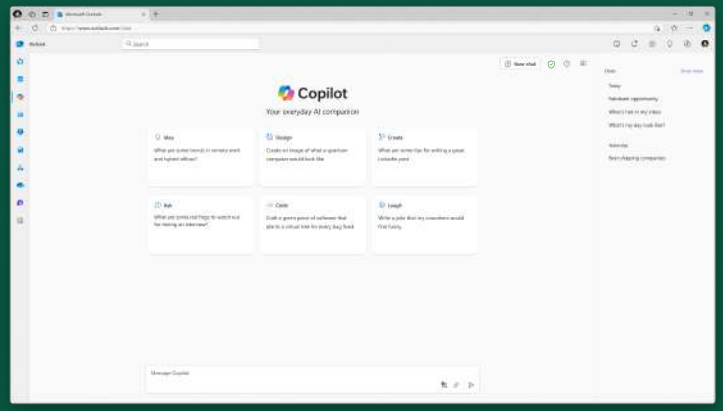


Edge Browser Sidebar

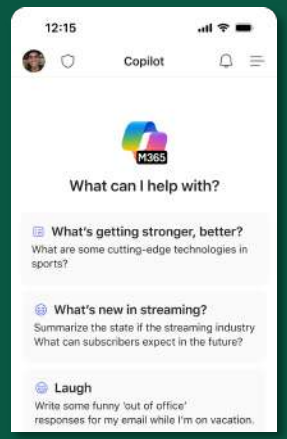
Teams App



Outlook App



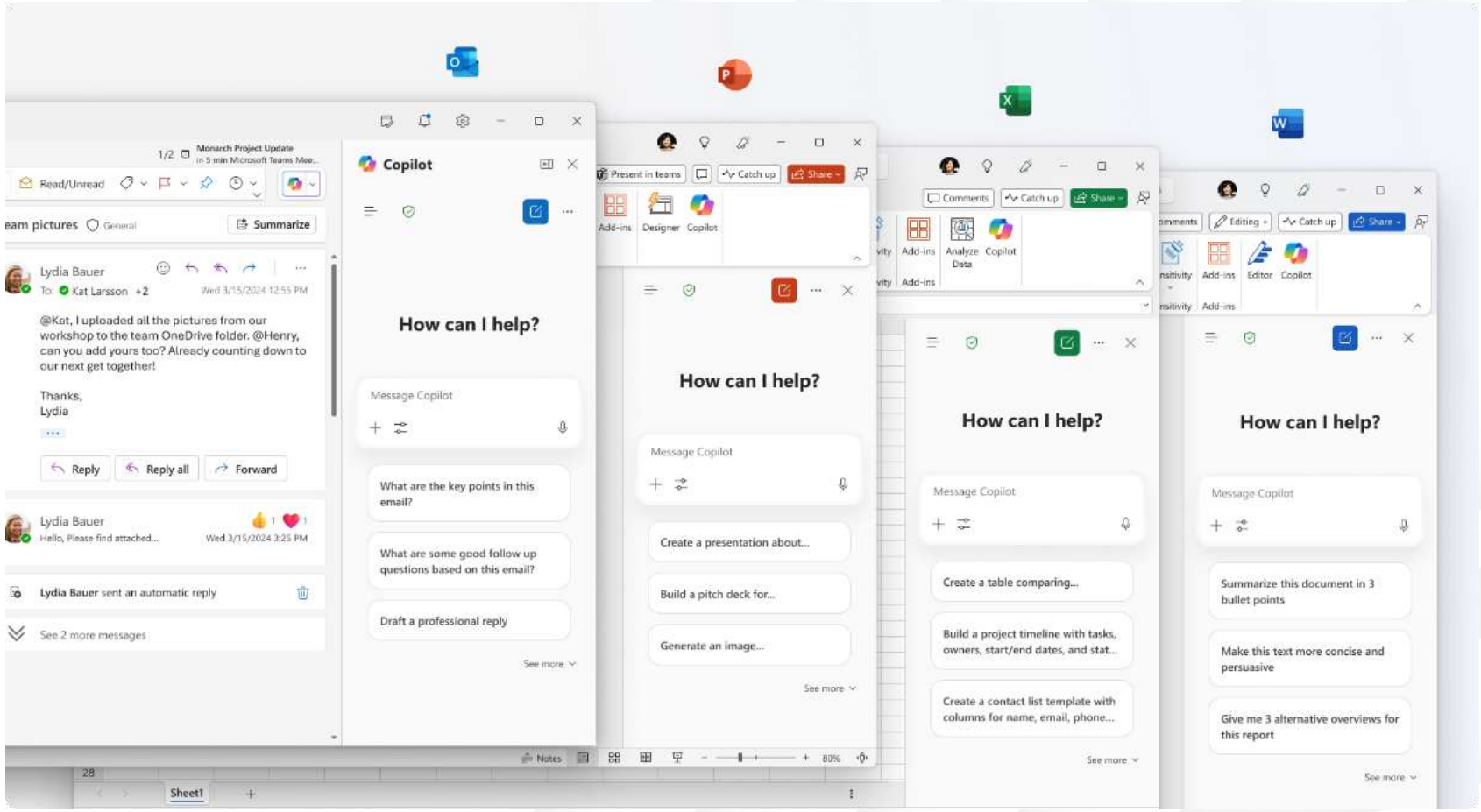
Microsoft 365 Copilot Mobile App



*Ensure Copilot is pinned to your left navigation across Teams, Outlook, and the Microsoft 365 app

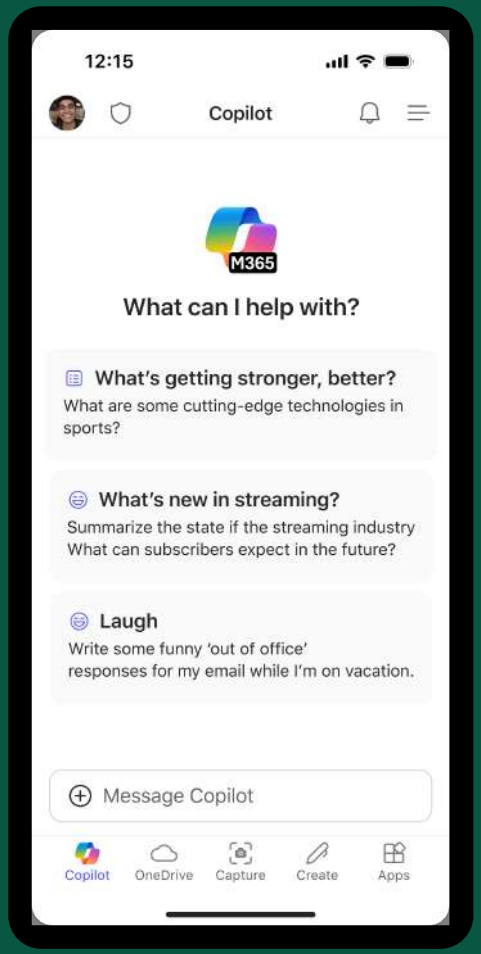
Access Copilot Chat From Your Apps

When using Copilot Chat within an app you can reference the open document in your queries.



Use Copilot Chat On The Go

Download the Microsoft 365 Copilot mobile app and sign in with your work account to access Copilot Chat



How to Use Copilot Chat in 3 Steps

1

Enter Your Prompt

Enter your detailed prompt in the text box at the bottom. If you would like Copilot to source information from any reference files, you can upload them in your prompt by selecting the “Add content” button.

2

Check Sources

Copilot Chat is transparent about the sources of its information. See these sources listed underneath the answer.

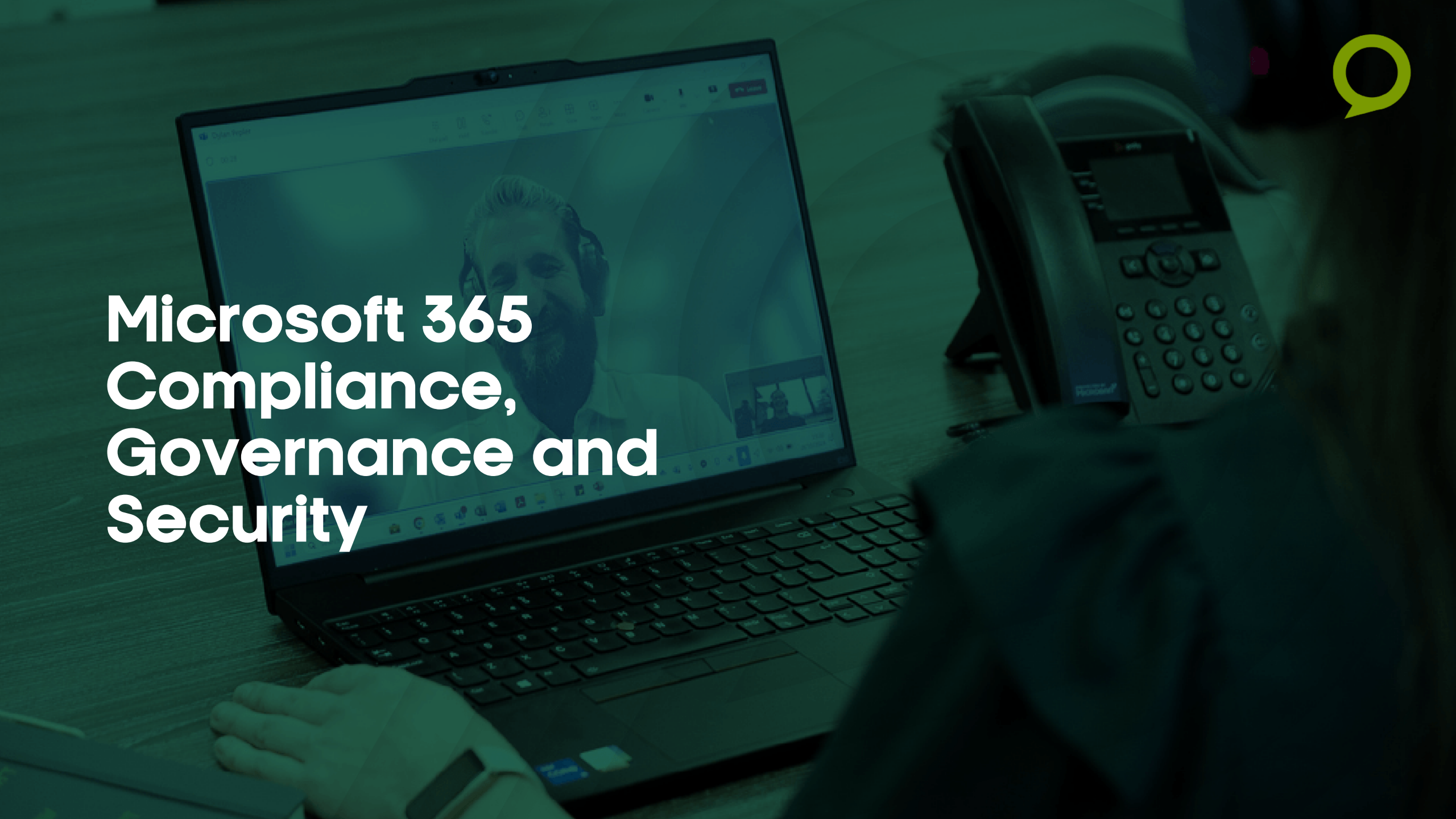
Vet these sources and validate your answers.

3

Continue the Conversation

You can ask follow-up questions as you would in a conversation. You can refine the answer too.

For example, try “Write a shorter answer" or "Give me more detail." You can also select suggested prompts.



Microsoft 365 Compliance, Governance and Security

Why Choose Microsoft Defender Suite?

Enhanced Security

Protect your business from cyber threats across devices, email, identities, and apps

Reduced Costs

Save more compared to standalone licenses

Industry Recognised

Recognised as a leading security vendor for businesses by independent industry experts

Enhanced Security

Microsoft Defender for Business

Identity and Access Controls | **Identity Protection** | **Device Security** | **Collaboration Security** | **SaaS Security**

Microsoft Entra ID Plan 2

Risk-based conditional access and real-time dynamic user and sign-in assessment

Identity protection using advanced machine learning to identify risky sign-ins, compromised accounts, and insider threats

Granular control over privileged accounts with automated elevation and access reviews

Adjusts access policies in real-time based on user risk

Microsoft Defender for Identity

Threat and suspicious user activity detection across identities and infrastructure

Built-in response and automated playbooks for quick threat mitigation

Context-rich identity insights during incident investigations—like recent events, activities and risk scoring

Tailored configuration vulnerabilities and attack path modeling

Microsoft Defender for Endpoint Plan 2

Industry-leading antimalware, cyberattack surface reduction, and device-based conditional access

Comprehensive endpoint detection and response (EDR)

Advanced hunting with support for custom detections

Attack surface reduction capabilities powered by Secure Score

Microsoft Defender for Office 365 Plan 2

Protection against advanced attacks like phishing and malware business email compromise and spam

Protection beyond email to Microsoft Teams, OneDrive and SharePoint

AI and automation to investigate, analyze, and respond to email threats

Cyberattack simulation training and detailed reporting

Microsoft Defender for Cloud Apps

Full SaaS security capabilities.

Visibility into "Shadow IT" by discovering apps in useSaaS app security posture that uncovers configuration gaps and offers recommendations

OAuth-enabled and line of business app monitoring, governance and protection

Challenge

Siloed tools are not enough

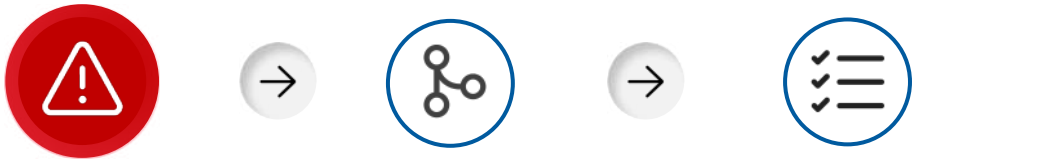
Attacks like those launched by Octo Tempest leverage a broad variety of tactics—like brute spray, social engineering, phishing, and malware—to try and gain entry. Once they have a foothold, they work to increase their privileges and gain access to valuable data, crossing different identities, endpoints, workloads, and even cloud. These types of coordinated attacks are hard to detect without comprehensive alert correlation.

Attacker launches multiple waves targeting organisations

Once successful, they begin moving inside the organisation

Eventually reaching your data and exfiltrating it

Meanwhile, your security team is trying to manually correlate alerts while the attacker is active in the environment.



Multiple alerts trigger across multiple portals

Defender has to manually correlate together across different sources

Remediation requires yet more manual steps, giving the attacker valuable time to continue their efforts

90% **of successful ransomware attacks involve an unmanaged device. 1**

1Source: Microsoft Digital Defense Report, 2024

Solution

Microsoft Defender XDR delivers incident-level visibility across the entire kill chain, so your analysts can focus on fully mitigating the threat instead of uncovering what happened. Automatic attack disruption will stop lateral movement of advanced cyberattacks, such as ransomware, with AI to limit the attacker's progress early on, and give your SOC team full control to investigate and remediate cyberthreats.

Attacker launches attack waves

Defender coordinates defense across domains

Attack is disrupted

Security professionals clean up after and implement changes to reduce exposure

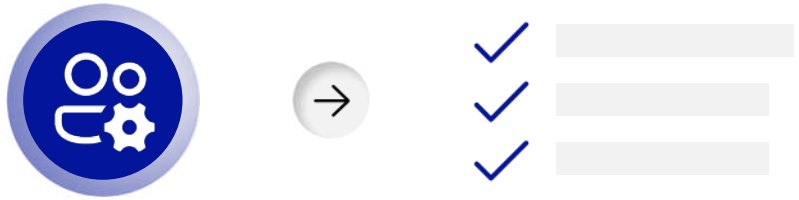
3 mins **average time to disrupt a ransomware attack with Defender XDR.2**

2Source: Microsoft Internal Research

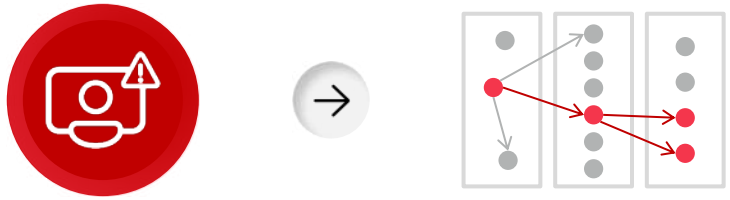
Challenge

Managing Risk Exposure

The average large organisation has tens of thousands of exposures—prioritising these effectively takes more than just burning-down lists of vulnerabilities of configuration problems. Attackers don't just target your biggest vulnerability—they target the group that cumulatively result in the biggest exposure.



Defenders think in lists, working across tables of alerts, vulnerabilities, and threat intelligence



Attackers are thinking in graphs, mapping vulnerabilities together

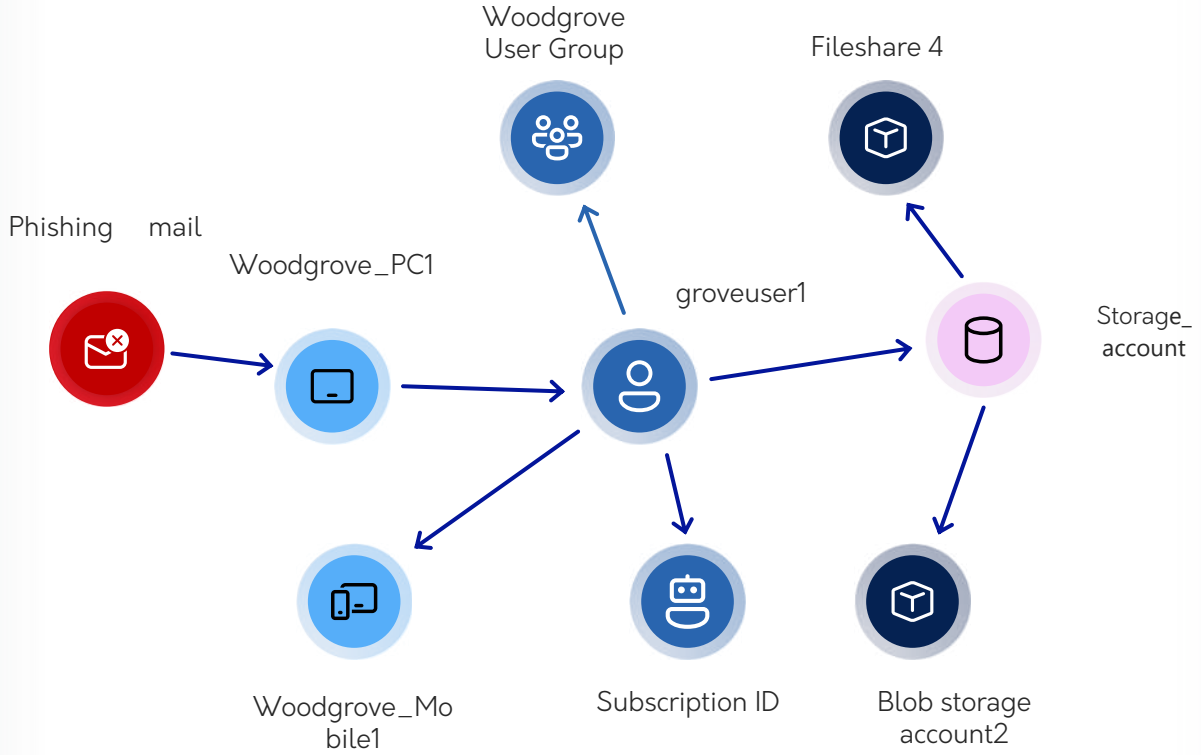
80% **of organisations have attack paths that expose critical assets.** [1]

[1]**Source:** Microsoft Digital Defense Report, 2024

Solution

Unified Exposure Management

Microsoft Security Exposure Management helps your team build a continuous threat exposure management program by unifying disparate data silos, providing security teams with end-to-end visibility of their organisation's security posture.



Why Choose Microsoft Purview Suite?

Data Security	Data Governance	Data Compliance
Data loss prevention	Data catalog	eDiscovery and audit
Insider risk management	Data quality	Communication compliance
Information protection	Data management	Data lifecycle management
Data security investigations	Data estate health	Records management

Shared capabilities

Classification l Labels l Audit

Microsoft Purview Suite for Business Premium

Business Premium + Purview Suite

Microsoft 365 Business Premium

Productivity and Security suite

- Entra ID P1: **Conditional Access** based on predefined conditions like device compliance, location, and app sensitivity
- MDO P1: Email and collaboration security, including **anti-phishing, anti-malware, and safe links/attachments.**
- MDB: AI-powered, SMB optimised **endpoint security with EDR and automatic attack disruption.** Across Windows, macOS, Linux, Android, and iOS.
- Purview Information Protection: **Encrypt emails** and discover, classify, and manually label sensitive data.
- Intune P1: Manage **devices and work data** on company-owned and employee devices. Remove business data from lost or stolen devices

+

Microsoft Purview Suite

Simplified compliance and data governance

- eDiscovery & Audit: Empowers legal and compliance teams with integrated tools and deep visibility to **streamline investigations, enforce legal holds, and maintain regulatory readiness.**
- Insider Risk Management: Helps detect and mitigate internal threats with **privacy-respecting behavioral analytics and granular communication controls.**
- Information Protection & Governance: Enables organizations to **classify, protect, and manage sensitive data across its lifecycle**, ensuring secure collaboration and compliance at scale.

Bridge Data Security Gaps

A negligent user accidentally exposed sensitive information

Jane Doe

Collected proprietary info from multiple companies leveraging her privileged title.

Attempted to copy the info to an external hard drive but was blocked by the DLP policy at Company A.

She found a loophole and uploaded sensitive content to her personal cloud storage at both companies.

She copied those files from the cloud storage to an external hard drive at Company B.

She was terminated from both companies and her hard drive underwent an authority investigation.

Microsoft Purview Data Security

Leverage **Data Security Posture Management** recommendations to create correlated DLP and Insider Risk Management policies to identify risks of sequential activities that might leak sensitive data.

Use built-in ML trainable classifiers in **Information Protection** to discover and auto-label intellectual property and protect it with encryption and access policies.

Use 100+ ready-to-use indicators and ML models in Insider Risk Management data leak/theft polices to detect Jane Doe as a repeat offender.

To better understand the breadth and depth of the data impacted by Jane's actions, perform AI-powered deep content analysis with Data Security Investigation.

Use Adaptive Protection to enforce a block Data Loss Prevention policy on high-risk users. Jane's actions to upload files to a cloud storage and copy to a hard drive can be blocked dynamically, while others could work as usual.

Adaptive Protection with Entra Conditional Access can help block access to apps that store data.

Prevent Data Leakage

A negligent user accidentally exposed sensitive information.

John and Alice

John is working on a highly sensitive M&A deal which only a few Contoso employees know about.

John mentions the name of company he is studying without sharing anything more about the deal with Alice.

Alice asks Copilot for M365 to find information on the deal and Copilot provides her a summary with the link to the document.

Alice then uses the summary to ask Contoso's finance agent to email her sensitive details about the project.

Out of curiosity, Alice wants to see what ChatGPT would summarise, so she pastes the content of the file in ChatGPT.

Microsoft Purview Data Security

Use **DSPM for AI** to understand how your users are interacting with Copilot and other GenAI apps. Get details on which GenAI apps are being used and what sensitive data is flowing through the prompts, as well the risk level of the users using GenAI apps.

Use Oversharing assessments for **Copilot in DSPM for AI** to get details on labeled and unlabeled files and the files use.

Use **Information Protection** to apply default sensitivity labels to document libraries such that new documents automatically inherit the same protection.

Use built-in ML trainable classifiers in **Information Protection** to discover and auto-label M&A documents and protect it with encryption and access policies.

Copilot inherits the labels and the protections that come with it.

Create a **DLP for Microsoft 365 Copilot** policy to prevent Copilot from summarising the labeled documents.

Use **Data Loss Prevention** policy to prevent out of policy sharing of sensitive data, such as emailing it or users pasting or uploading sensitive data to consumer GenAI apps through an email or endpoint DLP policy.

Summary

Microsoft 365 Business Premium

One solution to run your business securely from anywhere

Comprehensive

Microsoft 365 apps, Teams, and security in one solution

Ease licensing complexity

Get up and running quickly with simplified deployment

Cost Effective

Save costs vs buying multiple security solutions

Reduce operational expenses with automation

Lower help desk overhead

Enterprise-grade Security

Top rated security vendor

Comprehensive security across identity, devices, apps, and data

Industry first, automatic attack disruption

Contact Us

sales.it@croftmsp.com

01920 454 035

croftmsp.com

Follow us for technology updates. Search for croftmsp

Managed IT Services and Support

Communications and Connectivity

Business Mobile Services