Our expert panel guests

Jason Flynn
Microsoft

Modern Work & Security – Global Black Belt

Vipin Hooda
FUJIFILM CodeBlue

Principal Solutions Consultant

Tim O'Neill
Dicker Data

Microsoft Solution Sales Manager

Our special guest speaker: Jason Flynn

Modern Work & Security – Global Black Belt – **Microsoft**

After 10 + years at Microsoft leading technology strategy across multiple Financial Services customers and then focusing specifically in Security and Mobility for Enterprise, Jason stepped out of Microsoft and into a CIO role at Tourism Australia offering him a unique, customer's perspective of the Microsoft technology and forming global technology strategies and systems.

On his 'second tour' of Microsoft, Jason now works extensively with CIOs at Microsoft's largest and most complex customers on their cloud enabled technology. Concentrating on to-be state/vision, cost benefit analysis, capability gaps and identifying the links between Microsoft capabilities and strategic requirements. Jason's focus is primarily on collaboration, cyber security, and compliance solutions; accelerating the cloud migration journey for Microsoft customers through C-level engagement, backed up by detailed quantitative and qualitative analysis.

Microsoft

Run your business with peace of mind in a work-from-anywhere world

The way we worked: A snapshot of the Past
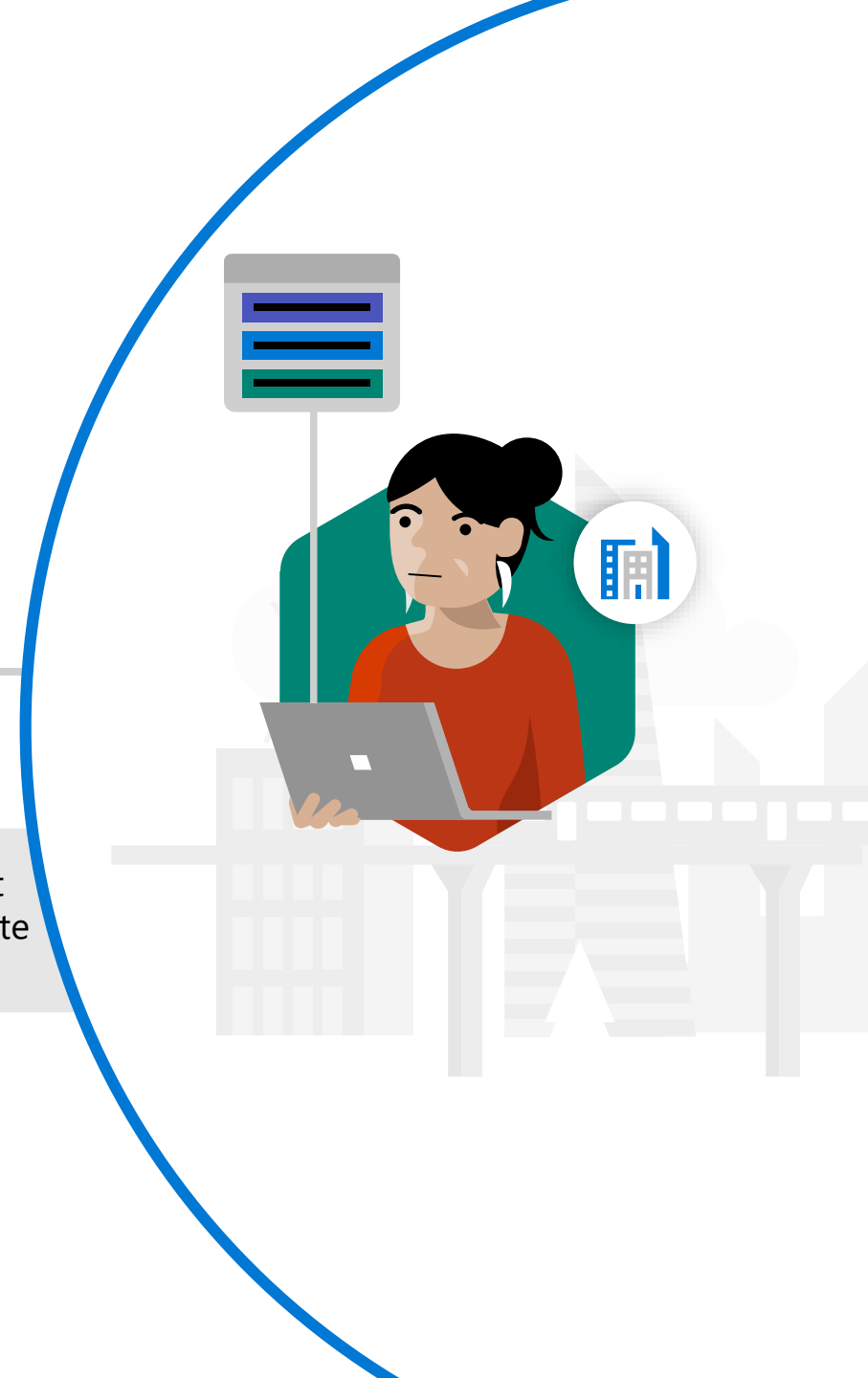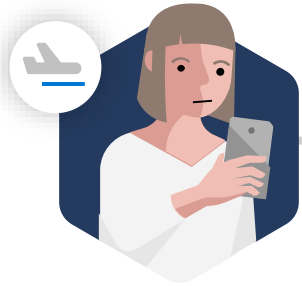
Northwind Traders Company

Physical proximity and security

The new normal | work from anywhere

Employees working from home and remotely

Multitude of personal and mobile devices

Increased security risks

74% Companies intend to shift some employees to remote work permanently

Top challenges for businesses...

How can we do distributed work better?

How can we maintain security?

How can we reduce our costs?

Employees working from multiple locations

Multitude of personal and mobile devices

Increased phishing and ransomware

Businesses are increasingly vulnerable to cyberattacks

+300% Ransomware attacks in the past year, with more than 50% targeted at small businesses [1]

Mission Critical

33% 1/3rd of all cyberattacks are targeted at small businesses.[2]

61% of small businesses that experienced a recent cyberattack were not able to operate.[3]

60% Businesses lack skills inhouse to deal with cyberattacks[4]

$108K average cost of a SMB data breach.[5]

1. Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report
2. Introduction to the 2020 DBIR | Verizon Enterprise Solutions
3. Microsoft commissioned Forrester Research
4. Underserved and Unprepared: The State of SMB Cyber Security in 2019
5. Kaspersky Global Corporate IT Security Risks Survey, 2019

LIVE BLOG   Follow our live coverage for the latest news on the coronavirus pandemic   ‹ 1/2 ›

Tradies frustrated by banks as business email scam costs them $51,000

By consumer affairs reporter Amy Bainbridge and Loretta Florance

Posted 8h ago

Jane Fleming realised too late she'd sent $51,000 to the wrong account. *(ABC News: Loretta Florance)*

Share f twitter share

As Jane Fleming lit the candles on her son's birthday cake, she was preoccupied with a substantial sum of missing money — $51,000 to be precise.
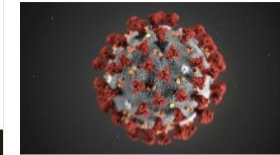
"It was a horrible day. I just felt sick all day, just wondering where the 50 grand was," she said.

It was on her son's ninth birthday that she realised she'd transferred that amount into a scammer's bank account.

Key points:

- Scammers intercepted an email and changed the banking details on the attached invoice

More on coronavirus

See our full coverage of coronavirus

Other languages

ABC中文 | 新冠疫情特别报道 →

Pandemik virus corona →

A '90 per cent effective' COVID vaccine is great news but it's not at the finish line yet

Very few countries are untouched by coronavirus. Here are those that claim to be COVID-free

You can get a great deal on overseas holidays for 2021 or 2022 — but there's a catch

ANALYSIS

The post-viral condition hitting some COVID-19 survivors

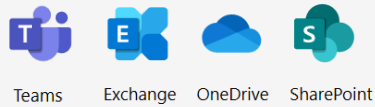'Grim milestone' as UK reaches 50,000 COVID-19 deaths on Remembrance Day

Top Stories

'Great day for Australia' as

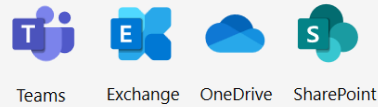# Microsoft 365 Business Premium

Microsoft 365 Business Basic

Cloud Services

Teams   Exchange   OneDrive   SharePoint

$8.20 per user/month

Formerly Office 365 Business Essentials

Microsoft 365 Business Standard

Cloud Services

Teams   Exchange   OneDrive   SharePoint

Desktop Apps

Outlook   Word   Excel   PowerPoint   Publisher   Access

$17.20 per user/month

Formerly Office 365 Business Premium

Microsoft 365 Business Premium

Cloud Services

Teams   Exchange   OneDrive   SharePoint

Desktop Apps
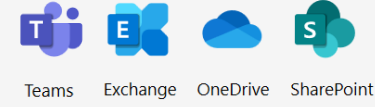
Outlook   Word   Excel   PowerPoint   Publisher   Access

Comprehensive Security

Intune   Azure Information protection   Azure AD Premium   Windows Virtual Desktop   Microsoft Defender
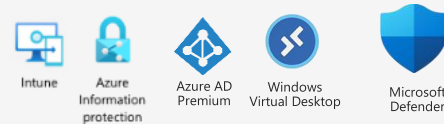
$30.20 per user/month

Formerly Microsoft 365 Business

[1]price is subject to change based on subscription term, currency and region

Note: Not all features/product logos shown.

# Common Challenges

Unauthorized access to work data

Northwind Traders' employees need access to work data as they work from home or on the go. However, bad actors outside the circle of trust may try to **gain access to work information, for example by stealing passwords and trying to gain access to the work data from another country.**

Enable secure access to work data
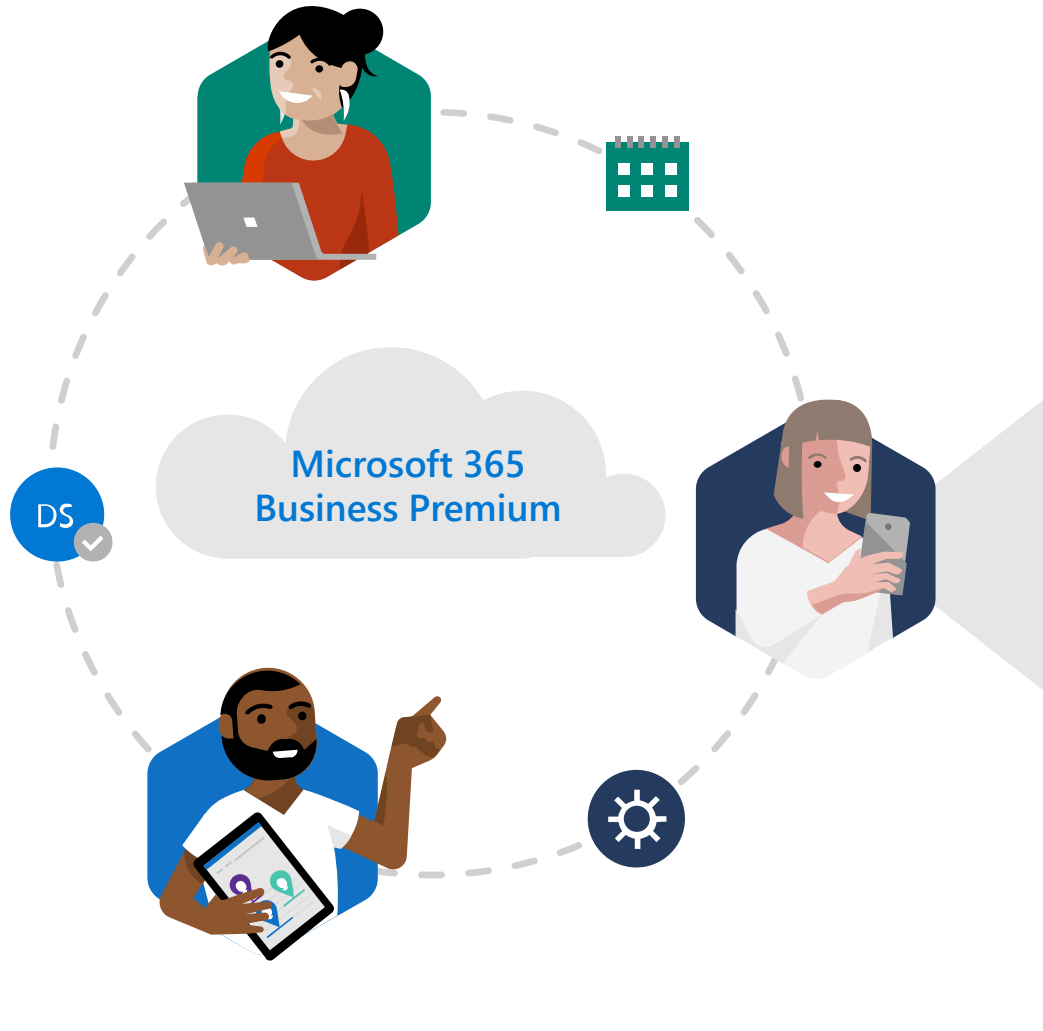
With Microsoft 365 Business Premium, you can apply advanced Multi-Factor Authentication (MFA) and Conditional Access policies, to help ensure that only the right people have the right access to work data, whenever and wherever they need. For example, with Conditional Access and MFA, you can set policies to block access or require additional authentication when you see an attempt to login from a country you don't do business in.

Microsoft 365 Business Premium

DS
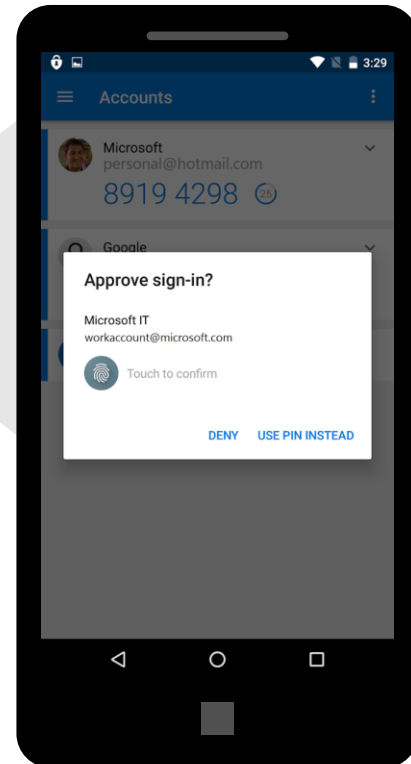
Azure AD Premium Plan 1

Identity and access governance

Multi-factor authentication

Conditional access policies

99% of identity attacks are thwarted by multi-factor authentication.[1]

[1] Source: 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*

Phishing attacks

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

Document cannot load
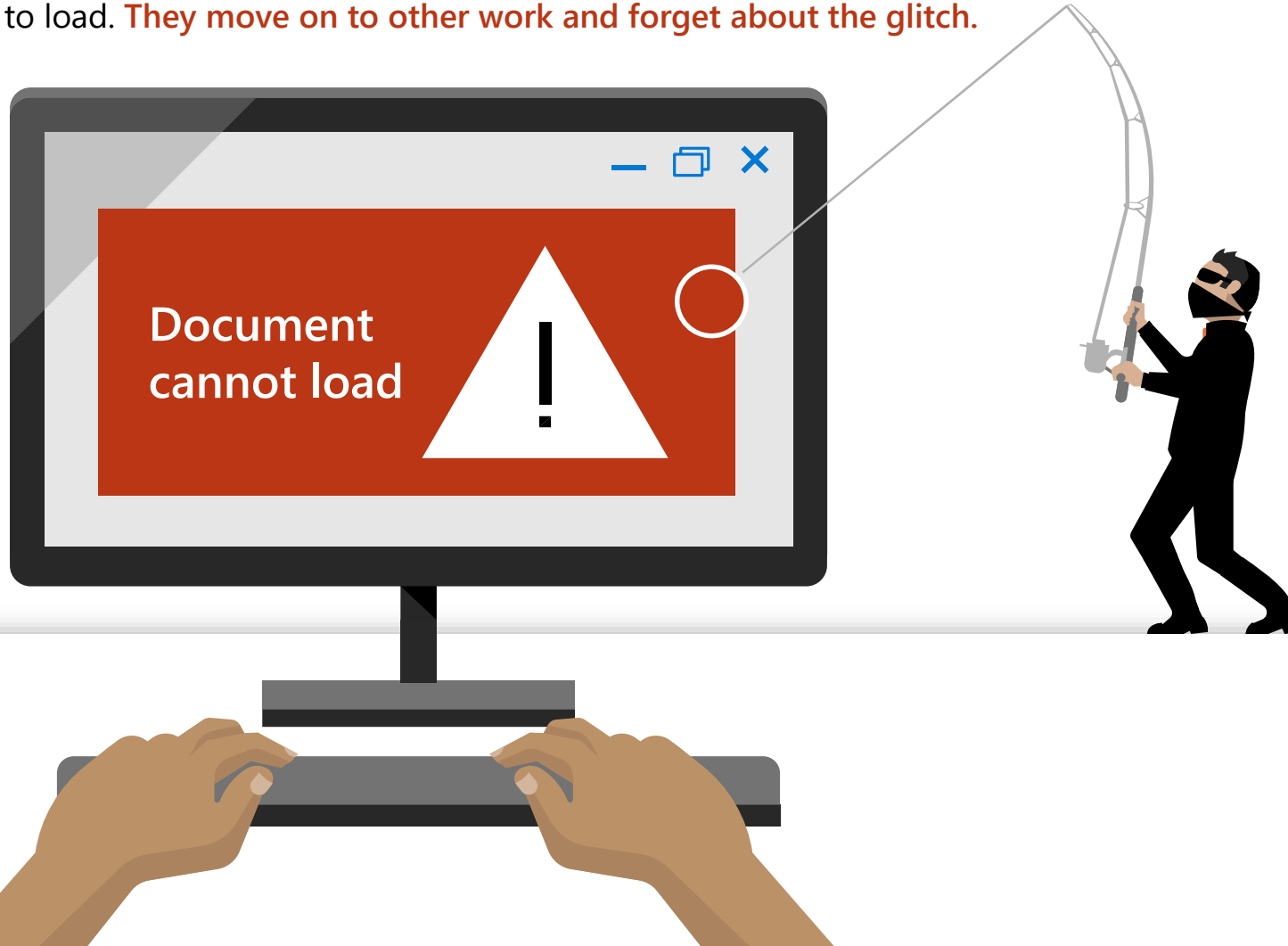
This was a phishing attack. They just delivered their username and password to hackers, who can now use it to access email and other online accounts, including Northwind Traders systems and data.

250%

Increase in phishing email detections from January to December 2018 worldwide.[1]

Sophisticated phishing defenses

With **Microsoft 365 Business Premium**, a Northwind Traders employee receives an email with a link to a secure document. The link is "sandboxed", and the user is alerted to the threat.
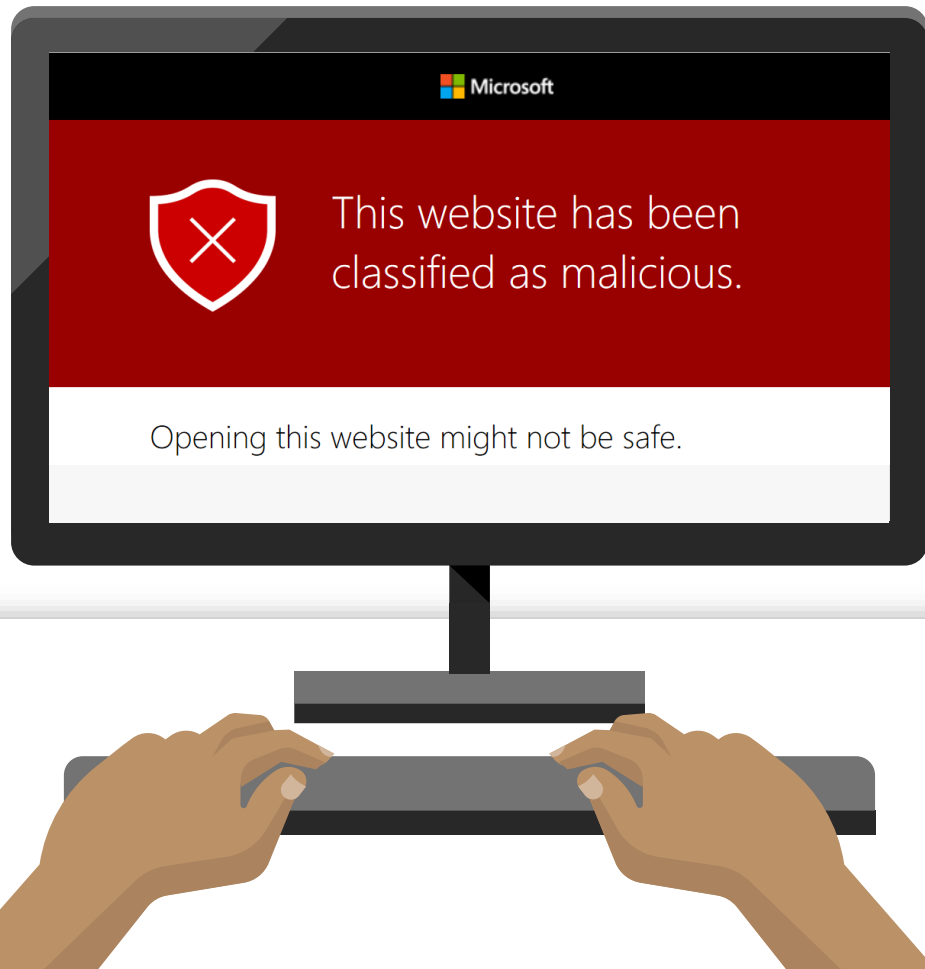
Microsoft 365 Business Premium comes with Microsoft Defender to protect against phishing attacks.

Time of click protection against malicious links

URL detonation

Anti-spoofing technology

Multi-factor authentication

Microsoft uses artificial intelligence to identify and protect against emerging threats in real-time.

Microsoft

This website has been classified as malicious.

Opening this website might not be safe.

Ransomware

During the busiest time of the year, Northwind Traders' mission critical files became unusable. **Hackers used ransomware to encrypt Northwind's files**, demanding a payment for the encryption "key". Northwind must either pay up or lose their data, which could result in business closure.

80% of SMBs list ransomware as a top concern.[1]

Mission Critical

!

!

Protect against ransomware

With Microsoft 365 Business Premium, devices are protected with features like Microsoft Defender. Microsoft Defender prevents unauthorized access to common folders such as Desktop or Documents. This means that unauthorized apps, scripts, and executable files won't be allowed access, so ransomware that attempts to encrypt your files in these locations will be blocked.
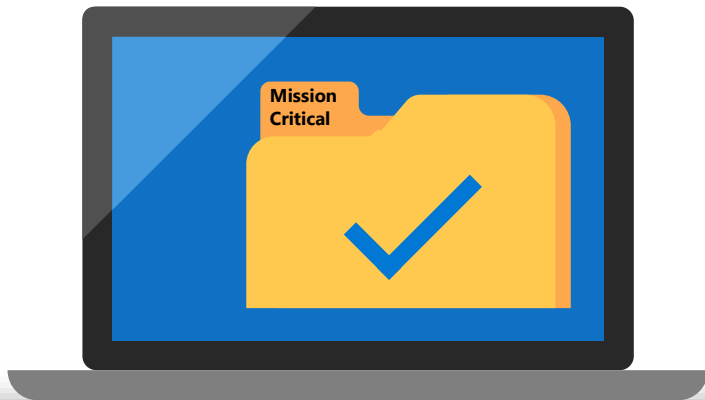
In 2020 the average cost of downtime associated with ransomware attacks rose[1]

94%

Microsoft 365 Business Premium

Microsoft 365 Business Premium protects against ransomware in 3 ways:

Email sandbox and Safe Links for untrusted senders

Device protection with Microsoft Defender

File recovery via OneDrive for Business

[1]*Source: Datto's 2020 Global State of the Channel Ransomware Report, statistics pulled from a survey of more than 1,000 MSPs around the world.*

Accidental data loss or data breach

Northwind uses occasionally use a password on an excel spreadsheet to guard sensitive info like salaries.

But these security measures are used inconsistently. Lots of documents are emailed around or saved on USB keys without any protections. **Anyone can download a confidential document and leave the company.**

Over 80%

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

.

Secure sensitive data

Adrian creates the company's sales forecast and classifies it as "Highly Confidential." As Northwind Traders is now using **Microsoft 365 Business Premium, "Highly Confidential" files are automatically encrypted,** and only accessible to company employees.

Laura, a Northwind Traders salesperson, attempts to open the file. Microsoft 365 Business Premium verifies that she is a Northwind Traders employee and decrypts the file for her.

Even if any employee leaves the company, and stores the document on a personal device, they cannot access it because the document access is tied to their work credentials.

Highly Confidential

$$$

Highly Confidential
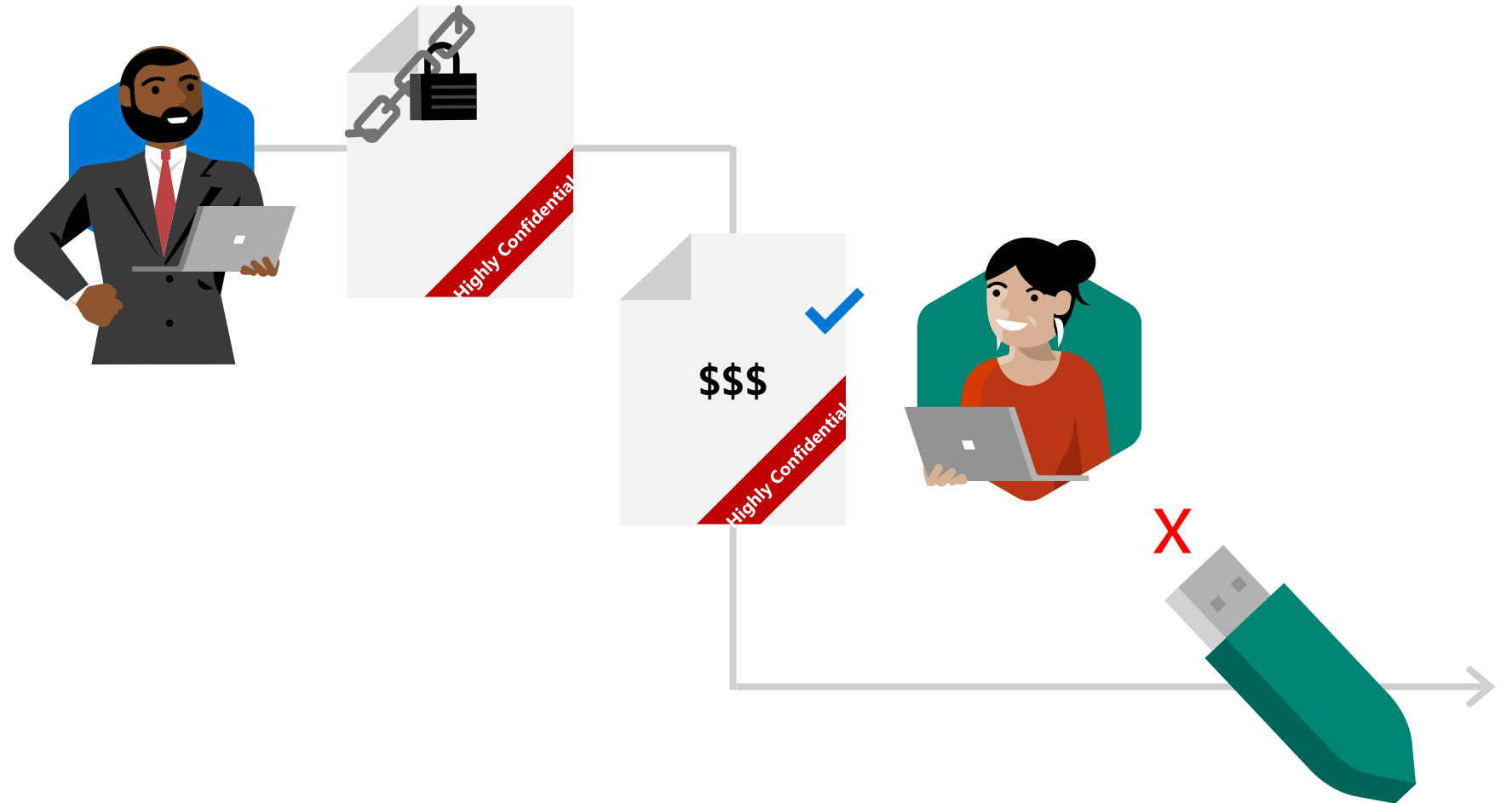
Secure sensitive data

With **Microsoft 365 Business Premium, you get advanced capabilities like Data Loss Prevention and Azure Information Protection,** to help classify and protect sensitive data like customer or employee information, confidential business data, medicare numbers, credit card numbers and more.

Over 55%

Businesses say they are concerned about employees leaving their company with data on personal devices.[1]
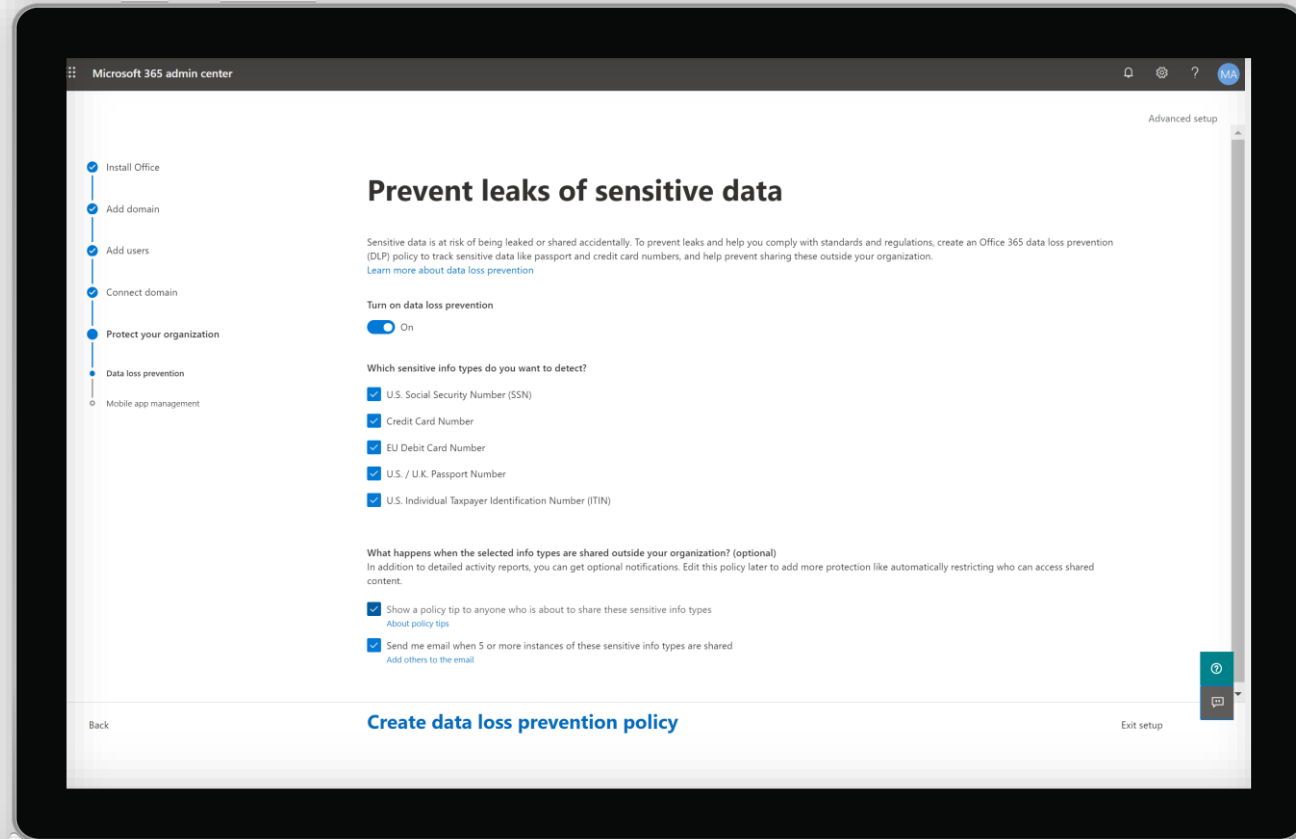

Prevent leaks of sensitive data

Sensitive data is at risk of being leaked or shared accidentally. To prevent leaks and help you comply with standards and regulations, create an Office 365 data loss prevention (DLP) policy to track sensitive data like passport and credit card numbers, and help prevent sharing these outside your organization. Learn more about data loss prevention

Turn on data loss prevention

⬤ On

Which sensitive info types do you want to detect?

☑ U.S. Social Security Number (SSN)

☑ Credit Card Number

☑ EU Debit Card Number

☑ U.S. / U.K. Passport Number

☑ U.S. Individual Taxpayer Identification Number (ITIN)

What happens when the selected info types are shared outside your organization? (optional)
In addition to detailed activity reports, you can get optional notifications. Edit this policy later to add more protection like automatically restricting who can access shared content.

☑ Show a policy tip to anyone who is about to share these sensitive info types
About policy tips

☑ Send me email when 5 or more instances of these sensitive info types are shared
Add others to the email

Back   **Create data loss prevention policy**   Exit setup

Work data on personal devices

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

Save to personal storage

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

Protect work data on personal devices

Managed apps

Personal apps

Confidential

Save to OneDrive
for Business

With Microsoft 365 Business Premium, you can set up Intune App Protection Policies, so work apps can be separated from personal apps. Administrators can specify that work documents and attachments are only saved on authorized and secure work share like OneDrive for Business, safeguarding sensitive work information.

58%
of employee devices on average are configured with proper security protocols and fewer than 1 in 5 saying that all employees undergo security training.[1]

[1]*Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2019 survey of Businesses (1-499 employees)*

Microsoft Defender for Business

Microsoft Defender for Business

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.

Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.

Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.

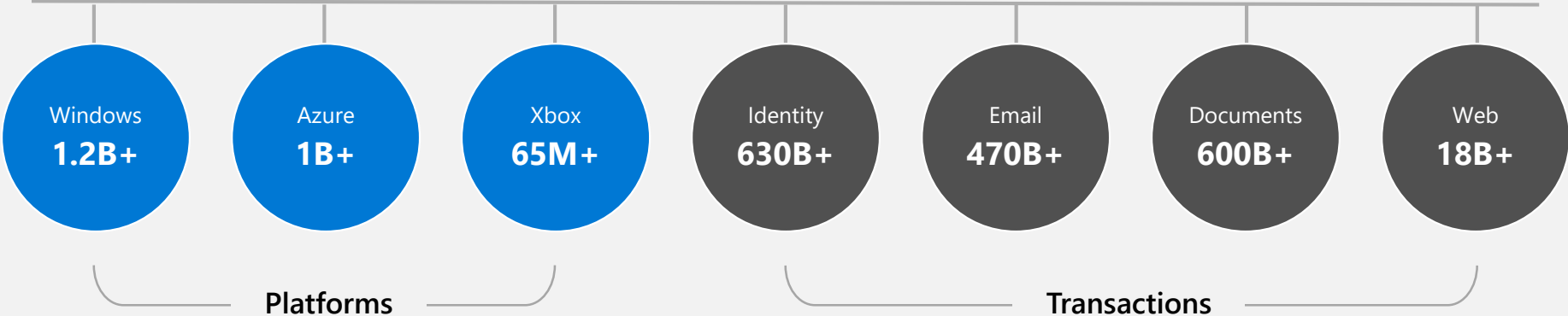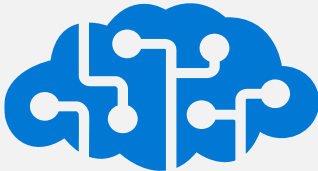### Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

Read the blog post to learn more

Microsoft's unique vantage point on security intelligence

Platforms

- Windows 1.2B+
- Azure 1B+
- Xbox 65M+

Transactions

- Identity 630B+
- Email 470B+
- Documents 600B+
- Web 18B+

300B
User activities profiled and analyzed in 2019

2.3B
Endpoint vulnerabilities discovered daily

11B
Malicious and suspicious messages blocked in 2019

12B
Cloud activities inspected, monitored, and controlled in 2019

Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

Endpoint Protection Platforms

Unified Endpoint Management

*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
*Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

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

		BEFORE MARCH 1 Microsoft 365 Business Premium[3]	AFTER MARCH 1 Microsoft 365 Business Premium[3]	Microsoft Defender for Business[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	Centralized management	•	•	•
	Simplified client configuration		•	•
	Next-gen protection	Win10	•	•
	Attack Surface Reduction	Win10[1]	•	•
	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]
	Microsoft Threat Experts			

Microsoft Defender consistently rated top AV

1 **AV-TEST**: Protection score of 6.0/6.0 in the latest test

2 **AV-Comparatives**: Protection rating of 99.7% in the latest test

3 **SE Labs**: AAA award in the latest test

4 **MITRE**: Industry-leading optics and detection capabilities

6.0/6.0
Protection score in AV-TEST
Achieved perfect protection score in the past 8 cycles

99.7%
Real-world protection in AV-Comparatives
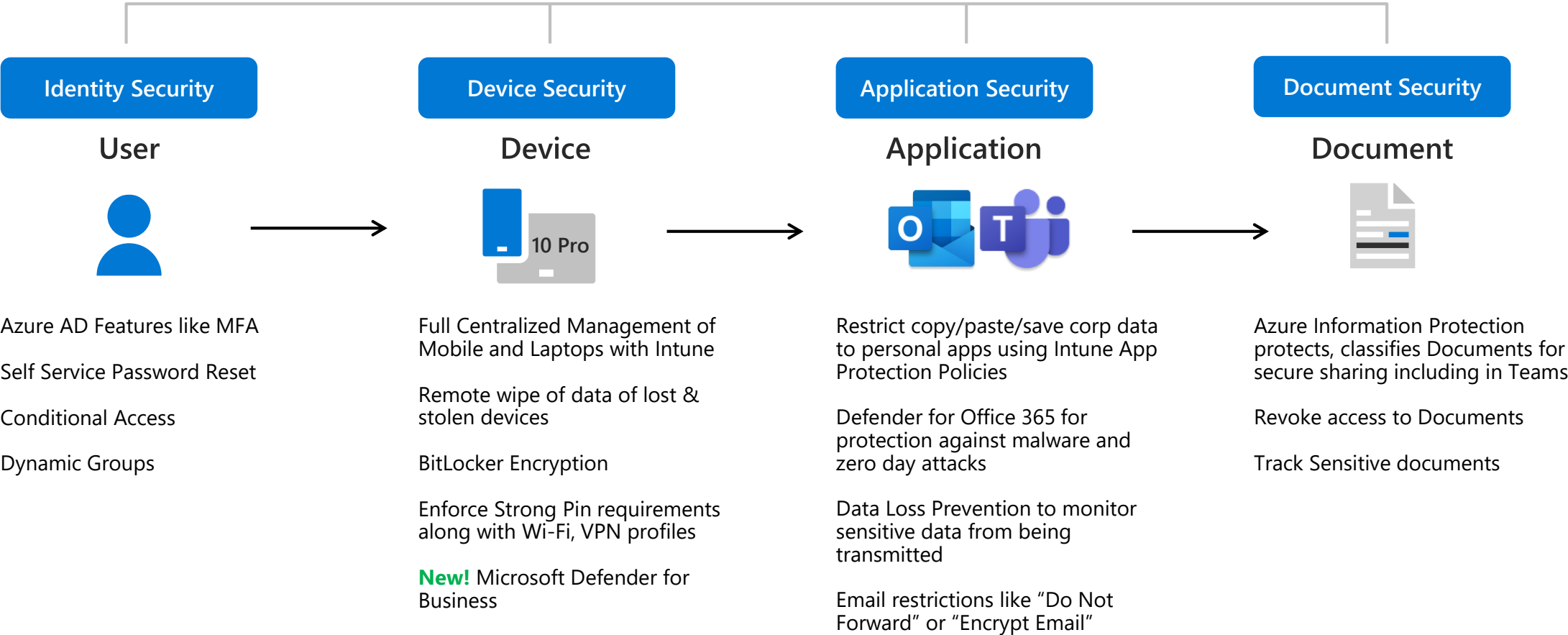Scored consistently high in Real-World Protection Rates

AAA
Award from SE Labs in past 4 cycles
Achieved 97% cycles total accuracy in latest cycle

Today's sophisticated attacks call for Layered security

Microsoft 365 Business Premium

Identity Security	**Device Security**	**Application Security**	**Document Security**
User	Device	Application	Document

Identity Security — User

Azure AD Features like MFA

Self Service Password Reset

Conditional Access

Dynamic Groups

Device Security — Device

Full Centralized Management of Mobile and Laptops with Intune

Remote wipe of data of lost & stolen devices

BitLocker Encryption

Enforce Strong Pin requirements along with Wi-Fi, VPN profiles

New! Microsoft Defender for Business

Application Security — Application

Restrict copy/paste/save corp data to personal apps using Intune App Protection Policies

Defender for Office 365 for protection against malware and zero day attacks

Data Loss Prevention to monitor sensitive data from being transmitted

Email restrictions like "Do Not Forward" or "Encrypt Email"

Document Security — Document

Azure Information Protection protects, classifies Documents for secure sharing including in Teams

Revoke access to Documents

Track Sensitive documents

Panel discussion and question time

Jason Flynn
Microsoft

*Modern Work & Security –
Global Black Belt*

Vipin Hooda
FUJIFILM CodeBlue

*Principal Solutions
Consultant*

Tim O'Neill
Dicker Data

*Microsoft Solution
Sales Manager*

**Have a question
for the team?**
Type it into the
chat!

Not sure about your environment?

Book a discussion with an IT expert.

- Your current IT environment or needs
- Microsoft Business Premium or your current Microsoft Enterprise license
- Technology and applications to support your remote or hybrid working environment

Thank you for attending our Microsoft Modern Work event.

Keep an eye on your inbox for your attendee take away kit, which includes:

- A copy of this presentation
- A link to a recording of this webinar
- Microsoft playbooks and more

>> Learn more about booking your expert Microsoft meeting.