Welcome to

SECURITY IN PRACTICE:

Is Microsoft 365 Business Premium worth it?

Do more with less - SMB.

myrtec

Microsoft

@myrtec

Presentation

OVERVIEW

- Defender
- Intune
- MDM
- Conditional Access
- Universal Print
- App control
- Password reset
- DLP & AIP
- Windows Autopilot
- eDiscovery
- Message Encryption

Microsoft 365 for business

(and old names for reference)

Microsoft 365 Business **Basic**

(Office 365 Business Essentials)

Microsoft 365 Business **Standard**

(Office 365 Business Premium)

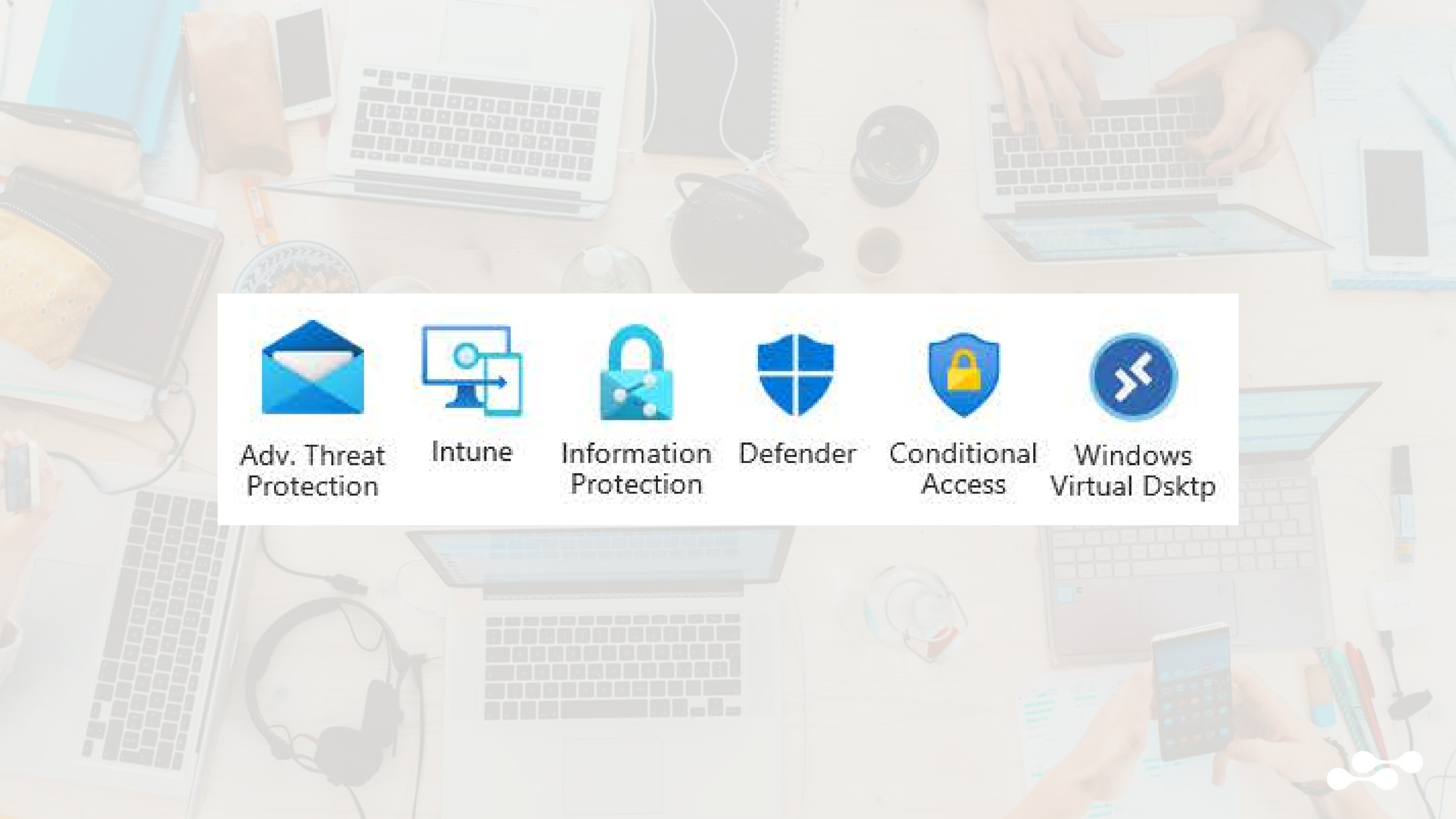
Microsoft 365 Business **Premium**

(Microsoft 365 Business)

Microsoft 365 **Apps**

(Office 365 Business)

Note: Not all features/product logos shown.


Adv. Threat Protection
Intune
Information Protection
Defender
Conditional Access
Windows Virtual Dsktp

DEFENDER

- Real-time protection
- Advanced threat protection
- Centralised management
- Integration with other Microsoft tools

WHY SHOULD YOU USE DEFENDER?

- Avoid outsourcing a separate Antivirus by keeping everything in Microsoft stack
- Eliminate the cost of your existing Antivirus
- Includes recommendations to improve you organisations security

DEFENDER - EXAMPLE

- A large financial services company was using Microsoft Defender across their network of devices to protect against cyber threats. One day, one of their employees received an email that appeared to be from a trusted source. The email contained a malicious attachment that, when opened, installed malware on the employee's computer.
- Fortunately, Microsoft Defender was able to detect the malware and quarantine it before it could spread to other devices on the network. The security team was notified of the incident and was able to investigate further, identifying the source of the email and taking steps to prevent similar attacks in the future.
- Because of Microsoft Defender's real-time protection and advanced threat detection capabilities, the financial services company was able to quickly detect and respond to the attack, minimizing the damage and preventing a larger security breach.

INTUNE

- Mobile device management
- App management
- Security management
- PC management
- Integration with other Microsoft tools

WHY SHOULD YOU USE INTUNE?

- Integrates with Defender and Conditional Access to control access to resources/2fs based on the health and status of the device
- Ability to wipe a device remotely if a staff member leaves or a device is stolen
- Order and autopilot new devices (install all software and apply all configuration) without having to stage them first (i.e shipped directly to the end-user) to minimise IT delays
- Build a standard operating environment (i.e all computers have Edge/Adobe/CRM automatically deployed) - Supports Windows, macOS, iOS and Android

INTUNE - EXAMPLE

- A large healthcare organisation was using Microsoft Intune to manage their mobile devices and computers. One day, an employee lost their mobile device, which contained sensitive patient information. Because the device was enrolled in Microsoft Intune, the IT team was able to remotely wipe the device to ensure that the data did not fall into the wrong hands.
- In addition to this, the organisation had a policy in place that required all devices to have a passcode or biometric authentication enabled, which helped to prevent unauthorised access to the lost device.
- Thanks to Microsoft Intune's mobile device management and security management capabilities, the healthcare organisation was able to quickly respond to the incident, ensuring that sensitive data was protected and that the risk of a data breach was minimised. The IT team was also able to track the device's location, which helped in the recovery process.
- Overall, Microsoft Intune played a critical role in the organisation's incident response, helping to protect sensitive data and ensuring that the organisation remained compliant with relevant regulations and policies.

MOBILE DEVICE MANAGEMENT

- Device management
- App management
- Security management
- Self-service management
- Integration with other Microsoft tools

WHY SHOULD YOU USE MDM?

- Requires a work profile on a device to keep work data and personal data separate
- Enforce PIN/sign-in/encryption
- Prevent personal apps from accessing work profile
- Wipe the work profile from a device if a staff member leaves (or wipe the entire device if it is company owned)
- With Conditional Access, you can only allow users to connect from a mobile with a work profile setup
- Control or deploy applications into the work profile

** Supports Android/iOS but some of the features differ between platforms

MOBILE DEVICE MANAGEMENT: EXAMPLE

- A disability service provider with employees located around the country. The company relies heavily on mobile devices for their employees to stay connected and productive. However, using these devices also presents a security risk to the company's sensitive data and systems.
- To address these concerns, the company implemented Microsoft Mobile Device Management (MDM) to manage and secure their mobile devices. With Microsoft MDM, the company can can:
  - ~Enforce device-level encryption to protect data at rest and in transit
  - ~Apply password policies to prevent unauthorised access
  - ~Remote wipe lost or stolen devices to prevent data breaches
  - ~Enforce app-level data protection to control access to sensitive data
  - ~Monitor device compliance and enforce security policies to ensure devices remain secure
- By using Microsoft MDM, the company can ensure that their mobile devices are secure and compliant with industry regulations. They are also able to track and monitor device usage, quickly identify and respond to any security threats, and enforce policies that align with their corporate security requirements.

CONDITIONAL ACCESS

- Security feature to control access to resources based on a set of conditions
- Conditions can include user location, device used, time of day, and other factors
- Ensures that only authorised users with approved devices and appropriate security settings can access resources
- Reduces the risk of data breaches and cyber attacks
- Allows businesses to customise security controls based on their specific needs
- Can require MFA for users accessing sensitive data outside of the company network
- Can require up-to-date security software on devices accessing company resources
- Provides flexible and customisable security controls for managing and securing resources

WHY YOU SHOULD USE CONDITIONAL ACCESS

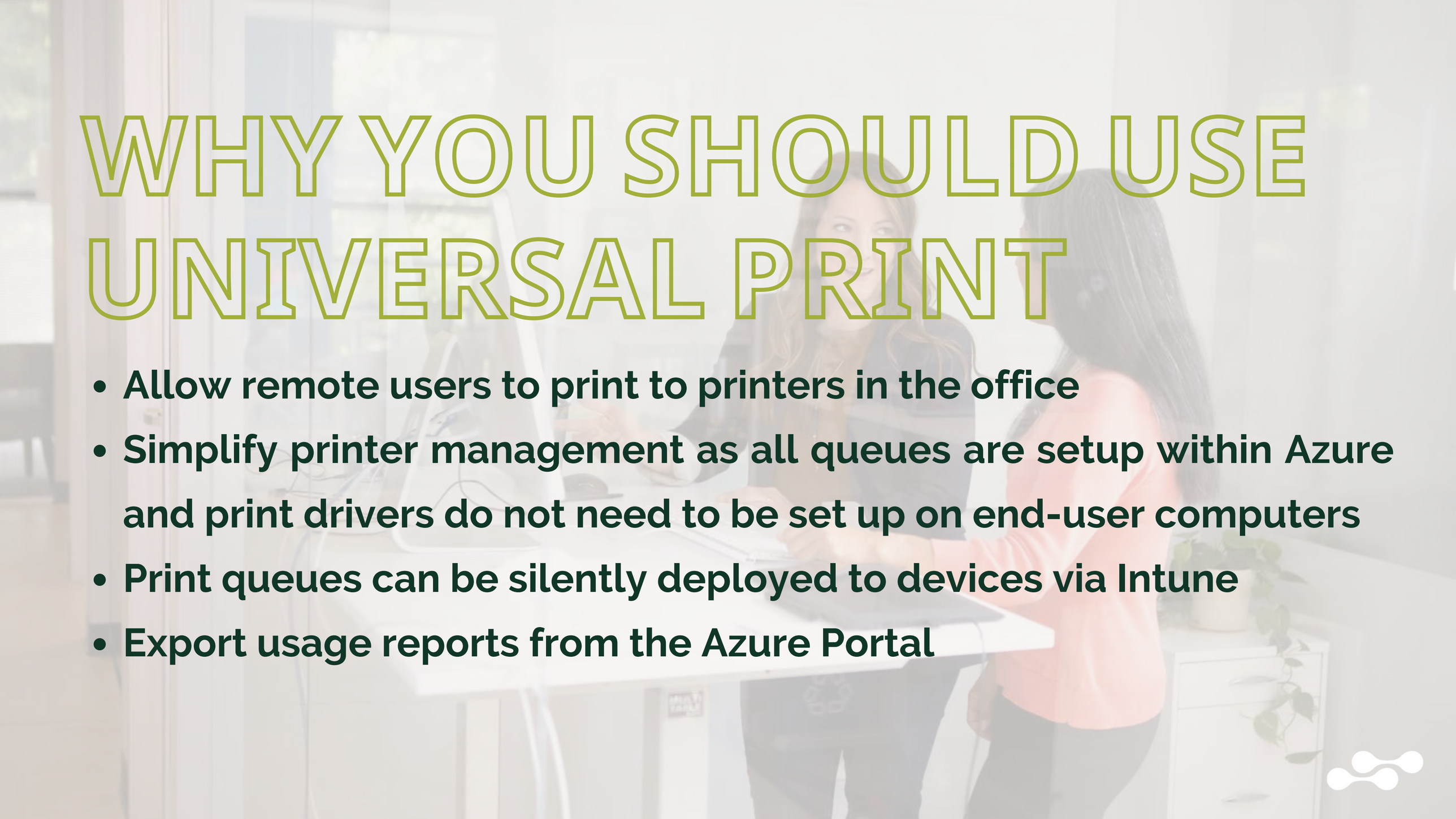
- Fine-grained control over how users authenticate, for example, requires an admin to use MFA for every sign in attempt
- Control a user's access so they can only access certain applications from a company-managed device
- Block legacy or insecure sign in methods
- Only allow certain users access from your office network

CONDITIONAL ACCESS - EXAMPLE

- A financial services firm that provides investment advice and manages portfolios for clients. Due to the sensitive nature of their business, the company needs to ensure that client data is protected at all times. They have implemented Microsoft 365 for their email and document management, but are concerned about the risk of unauthorised access.
- To address these concerns, the company sets up a Conditional Access policy that requires multi-factor authentication for all users accessing their Microsoft 365 resources from outside of the company network. This policy applies to all devices, regardless of whether they are owned by the company or the user.
- With this policy in place, the company can be confident that only authorised users with approved devices and appropriate security settings can access their resources. They are also able to track and monitor user access, and quickly identify and respond to any suspicious activity.
- In addition, the firm set up a separate Conditional Access policy that requires all devices accessing Microsoft 365 resources to have up-to-date security software installed. This policy helps to prevent malware and other security threats from compromising their data.
- Overall, the use of Microsoft's Conditional Access policy provides the company with a high level of security and control over their resources, ensuring that client data remains protected and compliant with industry regulations.

UNIVERSAL PRINT

- Printer setup
- User authentication
- Print job submission
- Printer selection
- Print job retrieval



WHY YOU SHOULD USE UNIVERSAL PRINT

- Allow remote users to print to printers in the office
- Simplify printer management as all queues are setup within Azure and print drivers do not need to be set up on end-user computers
- Print queues can be silently deployed to devices via Intune
- Export usage reports from the Azure Portal

UNIVERSAL PRINT - EXAMPLE

- A large commercial legal firm with many employees working remotely, needed a printing solution that would allow their team to print documents from anywhere, without the need for on-premises print servers.
- To address these concerns, the firm implemented Microsoft Universal Print. With Universal Print, their employees can print documents from anywhere, on any device, using a simple and secure cloud-based printing solution.
- For example, an employee working remotely on their laptop can initiate a print job using Universal Print. The print job is securely sent to the cloud and stored until the employee is ready to print it. The employee can then select a printer located in a different city or even a different country, and the print job is retrieved and printed out on that printer. This allows employees to print documents easily and securely, without the need for a complicated setup process or dedicated print server.
- Overall, the use of Microsoft Universal Print has allowed the law firm to streamline their printing processes and make it easier for their employees to work remotely. By providing a simple and secure cloud-based printing solution, Universal Print has helped the firm to improve their productivity and stay competitive in a fast-paced business environment.

APP CONTROL

- Improved security
- Compliance
- Enhanced productivity
- Simplified IT management
- Better cost control

WHY YOU SHOULD USE APP CONTROL

- Supplements antivirus by only allowing approved applications to run (so malware cannot be executed)
- Required for Essential 8/ISO27001 compliance, may be extended for companies working with government or private information
- Only allow approved applications to run (preventing malware from executing)

APP CONTROL - EXAMPLE

- A mid-sized training organisation was experiencing frequent security breaches caused by employees downloading and installing unauthorised applications on company devices. These unauthorised applications were often sources of malware and other security threats that posed a significant risk to the company's sensitive data.
- To address this issue, the company implemented Microsoft App control, which allowed them to create policies that restricted the use of unapproved applications on company devices. Specifically, the company set policies that only allowed applications with a trusted digital signature to run, and blocked any applications that were not approved by the IT department.
- After implementing App control, the organisation saw a significant reduction in security breaches caused by unauthorised applications. The IT department was able to easily manage which applications were allowed to run on company devices, and employees were no longer able to download and install unapproved applications that posed a risk to the company's security.
- Overall, Microsoft App control provided the organisation with a powerful tool to improve its security posture and reduce the risk of security breaches caused by unauthorised applications.

SELF SERVICE PASSWORD RESET

- Reduced IT support workload
- Increased productivity
- Improved security
- Compliance

WHY YOU SHOULD USE SSPR

- Enable users to manage their own password resets by providing recovery information (and you can control how many forms of ID they need)
- Password resets do not require a support case/costs and can happen after hours
- If you centralise access to other applications using the users Microsoft identity it will also work for these applications as well

SELF SERVICE PASSWORD RESET - EXAMPLE

- A healthcare organisation had over 50 employees spread across multiple locations. Prior to implementing Microsoft SSPR, the IT department was inundated with password reset requests, which took up a significant amount of their time and resources.
- After implementing SSPR, the organisation saw a significant reduction in password-related requests, with over 60% of password resets being handled by users themselves. This allowed the IT department to focus on more critical issues and projects, improving their overall productivity and efficiency.
- Additionally, the organisation saw improvements in security, as SSPR encouraged employees to use stronger, more complex passwords. The organisation was also able to comply with industry regulations related to password management and data protection.
- Overall, the implementation of Microsoft SSPR helped the healthcare organisation to reduce IT support workload, improve productivity, enhance security, and comply with industry regulations.

DLP + AIP:

DLP - Data Loss Prevention:

- Improved security
- Enhanced visibility
- Increased compliance

AIP - Azure Information Protection:

- Improved security
- Simplified compliance
- Increased collaboration

WHY YOU SHOULD USE DLP + AIP:

- DLP can detect confidential data and block or alert if the data is sent/shared externally
- DLP can block common confidential data in Australia including:
  ~Australia Personally Identifiable Information (PII) Data
  ~Australia Privacy Act Data
  ~General Data Protection Act (GDPR)
  ~Australia Health Records Act (HRIP Act)
  ~Australia Financial Data
  ~PCI Data Security Standard (PCI DSS)
- Notifications can be enabled if sensitive data is shared outside the organisation (and tips can be shown to users)
- DLP policies apply to Outlook, SharePoint, OneDrive and Teams

- AIP is used to classify sensitive documents and emails
- Allow users to classify documents as Highly Confidential, Confidential etc
- Documents can be auto labelled based on their contents, i.e set TFN numbers to Confidential (additional license required)
- Prevent downloading, printing or sharing of data based on the classification
- Requires certain classifications to be encrypted

DLP + AIP - EXAMPLE

- A financial services firm, with fewer than 50 employees, dealt with sensitive financial information and was subject to regulations around data protection and privacy.
- Prior to implementing Microsoft DLP and AIP, the firm had difficulty identifying and protecting sensitive data. The firm's IT department was tasked with manually monitoring data usage and access, which was time-consuming and prone to errors.
- After implementing Microsoft DLP, the firm was able to identify and protect sensitive data automatically. The IT department set policies that prevented the unauthorised sharing or leakage of sensitive data, such as social security numbers and financial statements.
- In addition, the firm implemented Microsoft AIP, which allowed them to classify and protect their files at the file level. They were able to define policies that automatically classified files based on their content and apply appropriate levels of protection, such as encryption and restricted access.
- Overall, the implementation of Microsoft DLP and AIP helped the financial services firm to improve security, increase compliance, and simplify data protection. The firm was able to reduce the risk of data breaches and comply with industry regulations around data protection and privacy. Additionally, the firm was able to increase collaboration by securely sharing sensitive data with authorized users, even if those users were outside the organisation.

WINDOWS AUTOPILOT

- Zero-touch device deployment for faster and easier setup
- Customisable device configurations and policies
- Integration with Intune for mobile device management
- Automatic updates and security patches for improved security

WHY YOU SHOULD USE WINDOWS AUTOPILOT

- Enables new computers to be ordered and shipped directly to the end user from the manufacturer/distributor without any staging from IT
- The new device serial is loaded into autopilot and when the device turns on and connects to wifi it can be auto-provisioned
- Along with Intune, the standard company software can be deployed to the device automatically
- The end user can then just log in and start working immediately without any interactions from IT
- If a user leaves the device can be wiped and reset automatically via Autopilot so it can be disposed of or re-assigned to another staff member

WINDOWS AUTOPILOT EXAMPLE

FUSION is a medium-sized marketing agency relies heavily on technology, and employees use laptops to complete daily tasks. Prior to using Windows Autopilot, FUSION's IT team had to manually configure and deploy each laptop, which was a time-consuming and tedious process.

After discovering the benefits of Windows Autopilot, their IT team was able to enrol new laptops in the Autopilot service before they were shipped to employees. This allowed the laptops to be pre-configured with all the necessary settings and applications before they even reached the employees. The solution also allowed employees to easily set up their own devices without requiring IT support. The end result was a significant reduction in the time and resources required for laptop deployment and a more streamlined process for employees to get up and running with their new devices.

Furthermore, Windows Autopilot also offers other benefits such as simplified device management, improved security, and automatic updates. With all these features, FUSION was able to ensure that their laptops were always up-to-date with the latest security patches, applications, and settings, while also minimising the amount of time and effort required to manage them.

E-DISCOVERY

- Electronic discovery for legal and compliance purposes
- Search and analysis of electronic data, including email and documents
- Preservation and collection of data for legal holds
- Integration with other Microsoft security solutions like Compliance Manager

WHY YOU SHOULD USE E-DISCOVERY

- Search SharePoint/users mailbox for a contract or document
- Create retention policies to retain all emails (even ones that users delete) for a set period of time, for example, if a user resigns and deleted all of the emails and empties their recycle bin, these emails can be recovered via E-Discovery
- If a staff member sends a confidential email to a competitor/customer and then when they realise they delete it from their sent items. This email can be recovered via E-Discovery for use internally or in court
- Create a hold on data that prevents any of it is deleted and then export this data if it needs to be used for legal purposes

E-DISCOVERY - EXAMPLE

A real estate agency, which is subject to various legal and compliance requirements related to electronic data, found that managing these requirements was a time-consuming and challenging process. Prior to using Microsoft eDiscovery, the real estate's administration team had to manually search through large volumes of electronic data to identify relevant information. This process was time-consuming and often resulted in the teams spending several hours, or even days, locating and analysing electronic data.

After implementing Microsoft eDiscovery, the agency was able to streamline its legal and compliance processes related to electronic data. The tool provided a centralised platform for managing all electronic data requests and responses, making it easier for the legal and compliance teams to track and manage requests. The platform's advanced search and filtering capabilities allowed the teams to quickly locate relevant information, reducing the time required to identify and analyse electronic data. Additionally, the tool's integration with other Microsoft services, such as Exchange Online and SharePoint, made it easier to manage electronic data across different platforms and applications.

Overall, Microsoft eDiscovery helped the agency improve the efficiency and effectiveness of its legal and compliance processes related to electronic data. The tool allowed the agency to reduce the time and resources required to manage electronic data requests, while also providing advanced search and analysis capabilities to ensure that relevant information was identified quickly and efficiently.

MESSAGE ENCRYPTION

- Secure email communication with end-to-end encryption
- Protection against data breaches and unauthorised access
- Compliance with industry standards and regulations
- Integration with other Microsoft security solutions like Exchange Online Protection

WHY YOU SHOULD USE MESSAGE ENCRYPTION

- You can encrypt confidential financial information over email with DoNotForward and DoNotPrint
- Clients such as Gmail will force the user to sign in on their Gmail account to view the message
- Legacy clients will need to sign in and use a single-use code to view the message
- Microsoft manages the encryption methods so it is seamless for users

MESSAGE ENCRYPTION - EXAMPLE

Fierce Wealth is a large financial services company that handles sensitive information, such as personal and financial data. The company needed to ensure that its email communications were secure and compliant with industry regulations. Prior to using Microsoft Message Encryption, Fierce Wealth relied on basic email encryption tools that were difficult to manage and did not provide the level of security required by the company.

After implementing Microsoft Message Encryption, the company was able to improve the security and compliance of its email communications. The tool provided advanced encryption capabilities that ensured that only the intended recipient could access sensitive information sent via email. In addition, Microsoft Message Encryption provided a range of security and compliance features, such as message expiration dates and tracking capabilities, which helped the company comply with industry regulations and maintain the confidentiality of sensitive information.

Overall, Microsoft Message Encryption helped Fierce Wealth improve the security and compliance of its email communications, reducing the risk of data breaches and ensuring that sensitive information was protected at all times. The tool's advanced encryption capabilities and security features made it a valuable investment for the company, providing peace of mind and reducing the risk of regulatory fines and reputational damage.

Microsoft 365 Business Basic

AU$8.20 user/month

(Annual subscription–auto renews)[1]
Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Get started

Try free for one month[2]

- Web and mobile versions of Microsoft 365 apps only
- Chat, call, meet up to 300 attendees
- 1 TB of cloud storage per user
- Business-class email
- Standard security
- Anytime phone and web support

Most popular

Microsoft 365 Business Standard

AU$17.20 user/month

(Annual subscription–auto renews)[1]
Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Get started

Try free for one month[2]

Everything in Business Basic, plus:

- Desktop versions of Microsoft 365 apps with premium features
- Easily host webinars
- Attendee registration and reporting tools
- Manage customer appointments

Recommended

Microsoft 365 Business Premium

AU$30.20 user/month

(Annual subscription–auto renews)[1]
Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Get started

Try free for one month[2]

Everything in Business Standard, plus:

- Advanced security
- Access and data control
- Cyberthreat protection

Microsoft 365 Apps for business

AU$12.00 user/month

(Annual subscription–auto renews)[1]
Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Get started

Try free for one month[2]

- Desktop versions of Microsoft 365 apps with premium features
- 1 TB of cloud storage per user
- Standard security
- Anytime phone and web support

***Off set cost of antivirus if you are using Microsoft Defender**

POST EVENT SURVEY

Please fill out our survey

before you leave today.

Thank you for attending

SECURITY IN PRACTICE:

Is Microsoft 365 Business Premium worth it?

Do more with less - SMB.

myrtec

Microsoft

@myrtec