

## SECURITY

# Solutions Partner for Security Designation

## FINANCE

## Build Your Solution

This stage we are defining our solutions technical requirements to determine which Microsoft subscription will become the foundational base of our solution itself.



### What Is the Information Provided?

- Identifying technical features critical to this industry's requirements
- Testing if essential security features are excluded in lower plans?
- What result did our investigation uncover?

### Why Is This Information Important to Understand and Use?

In customer interactions, it's essential to address their concerns within the context of their specific industry, as these are typically the most crucial to meeting their needs. Meeting this brief is crucial for boosting your chances of winning the customer's trust and business.

# How To Use

Once you have identified the industry vertical you would like to know more about, simply search and replace the word Finance for the industry name, Microsoft 365 E5 for what you believe is the best fit Microsoft 365 subscription, Microsoft 365 Business Premium for the subscription you wish to benchmark against

Once complete, ask each of the questions using Copilot (free or paid) and paste into the space required.

Within a few minutes, you will have all those very important technical requirements needed to determine the right subscription base, for the industry you are looking at!

## Identifying Features Critical to Industry Requirements

Based on our findings in in lesson 2, lets assess the criteria recommended to support Finance providers in Australia. Microsoft 365 E5 appears to be the best fit to meeting this industry's needs – but let's confirm this.

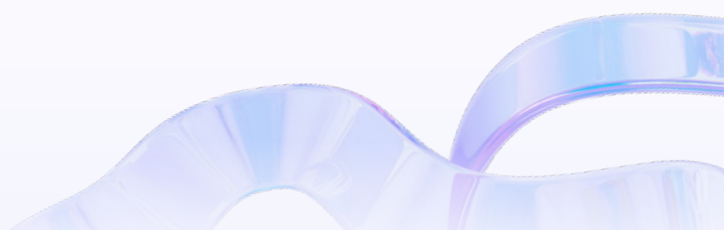


What are the top 10 security features of Microsoft 365 E5 for the Australian Finance Industry, list by feature, description and benefit. Visualise as a table.

Feature	Description	Benefit
Advanced Threat Protection	Provides real-time protection against sophisticated cyber threats, including zero-day attacks.	Ensures the security of sensitive financial data and transactions.
Data Loss Prevention	Monitors and protects sensitive information from unauthorised sharing or leaks.	Maintains compliance with financial regulations and safeguards client information.
Azure Information Protection	Classifies and protects documents and emails by applying labels.	Secures confidential information and ensures it is handled appropriately.
Cloud App Security	Provides comprehensive visibility, control, and threat protection for cloud applications.	Protects against shadow IT and secures financial data in the cloud.
Privileged Access Management	Limits access to critical resources and provides granular control over privileged operations.	Reduces the risk of insider threats and ensures secure access management.

Conditional Access	Applies policies based on user, device, and location factors before granting access.	Helps prevent unauthorised access and strengthens overall security posture.
Identity Protection	Uses machine learning to detect and respond to identity-based threats in real time.	Secures user identities and mitigates risks of identity theft and fraud.
Advanced Compliance	Offers tools to manage and protect data, reduce risk, and meet compliance requirements.	Ensures adherence to financial industry regulations and standards.
Threat Intelligence	Provides insights and analytics on emerging threats and vulnerabilities.	Allows proactive defence strategies to protect against potential cyber threats.
Secure Score	Evaluates and benchmarks the security posture of an organisation based on its configurations.	Provides actionable recommendations to improve security practices and reduce risks.

**Please note:** Benefits in green have all be specifically called for, as industry non-negotiables.



## Are Essential Security Features Excluded in Lower Plans?

The next question is to determine what the base-level subscription should include. For this evaluation, we must balance essential features against desirable ones and ensure we do not compromise the offer, for the sake of price, for example.



### Ask Copilot

What are the top 10 security features of Microsoft 365 E5, by order of importance, that are not available in Microsoft 365 Business Premium. List by description and benefit. Visualise as a table. Remove # column.

Feature	Description	Benefit
Advanced Threat Analytics (ATA)	Monitors user activities, entity behaviours, and detects suspicious activities and known attacks.	Helps identify and protect against advanced threats, compromised identities, and malicious insider actions.
Azure Advanced Threat Protection (ATP)	Provides a cloud-based security solution designed to detect and investigate advanced threats, compromised identities, and malicious insider actions.	Enhances security by protecting user identities and providing real-time attack detection and response.
Microsoft Cloud App Security	Provides visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all cloud services.	Improves the security posture of the organisation by protecting critical information across cloud applications.
Office 365 Advanced Threat Protection	Offers protection for email and collaboration tools by detecting and preventing advanced malware and phishing attacks.	Safeguards communications and collaboration tools against sophisticated cyber threats.
Azure Information Protection Plan 2	Helps classify, label, and protect data based on its sensitivity.	Ensures that sensitive information is properly protected and restricted to authorised users.
Microsoft Defender for Endpoint	Provides endpoint security, endpoint detection and response (EDR), and threat and vulnerability management.	Offers comprehensive protection for endpoints and helps in identifying and mitigating threats.

Microsoft Defender for Identity	Uses on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.	Provides enhanced security for on-premises environments by protecting user identities and detecting advanced threats.
Privileged Access Management	Allows organisations to manage, control, and monitor privileged access to critical resources.	Reduces the risk of privileged account abuse and enhances security by controlling access to sensitive information.
Customer Key	Enables organisations to control their encryption keys and use them to encrypt their Office 365 data at rest.	Provides an added layer of security by allowing organisations to manage the encryption of their data.
Advanced eDiscovery	Provides tools to identify, collect, and review content for legal and compliance purposes.	Enhances the ability to manage and respond to legal requests effectively and efficiently.

**Please note:** Benefits in red have all be specifically called for, as industry non-negotiables.

## What Result Did Our Investigation Uncover?

After examining these requirements, it is determined that Microsoft 365 E5 is the necessary SKU required to meet the needs of the Finance industry.

Based on the number and which crucial features are removed, we cannot consider Microsoft 365 Business Premium for this industry.

**Remember:** If another subscription fit, the information would have shown this.

**Continue on your path to achieving a Microsoft Partner for Security designation.**

Visit [dickerdata.com.au/Microsoft](https://dickerdata.com.au/Microsoft) or contact the Dicker Data Microsoft Team

(02) 8556 8061

[Microsoft.Sales@DickerData.com.au](mailto:Microsoft.Sales@DickerData.com.au)

