Solutions Designation:

Success

SECURITY

Solutions Partner for Security Designation

GOVERNMENT

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.

Microsoft Solutions Partner
Security

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 is 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.

Identifying Features Critical to Industry Requirements

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

Ask Copilot

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

Feature	Description	Benefit
Advanced Threat Protection (ATP)	Protects emails, files, and applications from malicious attacks.	Ensures the safety of sensitive government data.
Asure Information Protection (AIP)	Classifies and protects documents and emails by applying labels.	Maintains data confidentiality and integrity.
Cloud App Security	Monitors and controls the use of cloud apps.	Prevents data leaks and ensures regulatory compliance.
Conditional Access	Applies access controls based on conditions such as user, location, and device status.	Enhances security by ensuring only authorised users access resources.
Data Loss Prevention (DLP)	Prevents sensitive information from being shared outside the organisation.	Protects against data breaches and loss.
Microsoft Defender for Identity	Detects and investigates advanced threats, compromised identities, and malicious insider actions.	Provides advanced threat protection and investigation capabilities.
Microsoft Defender for Endpoint	Offers endpoint security across devices.	Protects government devices from threats.
Privileged Access Management (PAM)	Controls and monitors privileged access to critical resources.	Reduces risks associated with privileged access.

Unified Audit Logs	Provides a comprehensive audit trail of user and admin activities.	Ensures transparency and aids in compliance with regulations.
Windows Hello for Business	Offers a password-less sign-in experience.	Enhances security by reducing reliance on passwords.

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, which are not available in Microsoft 365 Business Premium. List by description and benefit. Visualise as a table. Remove # column.

Feature	Description	Benefit
Advanced Threat Protection (ATP)	Provides sophisticated tools to detect and block advanced threats.	Enhances security by protecting against sophisticated cyber-attacks.
Asure Active Directory Premium P2	Offers advanced identity protection and Conditional Access features.	Improves security with better access control and identity management.
Microsoft Defender for Identity	Monitors user activities to identify and alert on suspicious behaviour.	Prevents potential breaches by identifying compromised user behaviour early.
Microsoft Defender for Endpoint	Provides endpoint detection and response (EDR) capabilities.	Protects devices by detecting and responding to endpoint threats.
Information Protection & Governance	Encrypts emails and documents to protect sensitive data.	Ensures data privacy and compliance with regulatory standards.
Advanced eDiscovery	Offers tools for searching and analysing data across the organisation.	Improves legal and compliance outcomes with comprehensive data analysis.

Cloud App Security	Monitors and controls cloud apps to prevent risky behaviour.	Enhances security by identifying and mitigating cloud app risks.
Customer Lockbox	Provides additional control over data access during service operations.	Ensures greater privacy and security during data access requests.
Privileged Access Management	Manages and controls elevated access to critical resources.	Reduces risk by limiting and monitoring privileged access.
Asure Information Protection P2	Classifies and protects documents and emails through encryption.	Maintains data security across the organisation with automated protection.

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 Government 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 or contact the Dicker Data Microsoft Team

(02) 8556 8061 Microsoft.Sales@DickerData.com.au

DICKER DATA | Microsoft