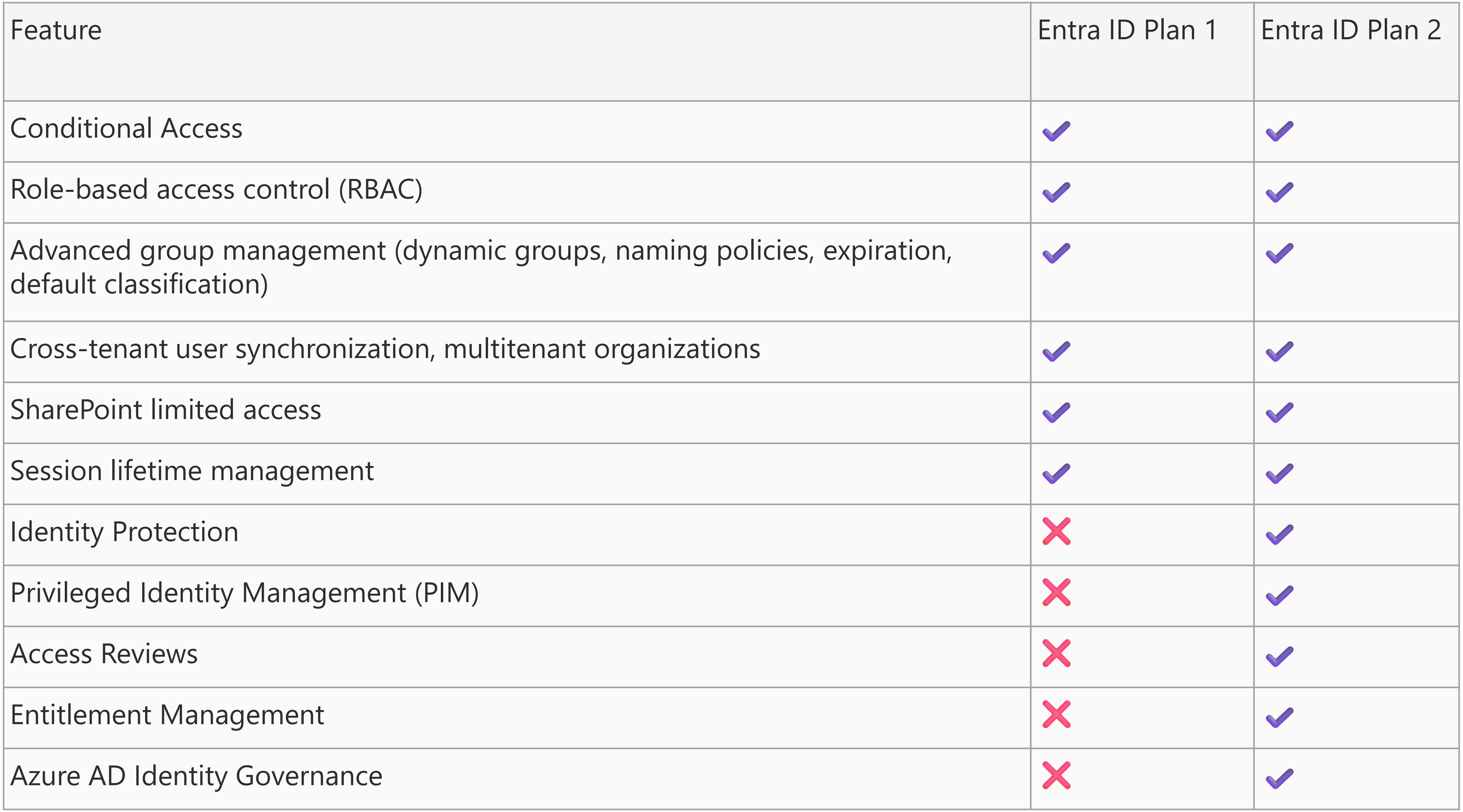
The Microsoft 365 E5 Security add-on enhances the security capabilities of your Microsoft 365 Business Premium subscription by introducing advanced tools and features. Below is a table summarizing the key components and their functionalities:□
By integrating these components, the E5 Security add-on significantly enhances your organization's ability to protect against modern cyber threats and manage security more effectively.□

Component	**Description**
Microsoft Entra ID Plan 2	Provides advanced identity and access management features, including:- **Access Reviews**: Manage group memberships and access to applications.- **Identity Protection**: Detect and remediate identity-based risks.- **Privileged Identity Management (PIM)**: Control and monitor access to sensitive resources with just-in-time access.- **Basic Entitlement Management**: Automate the provisioning and deprovisioning of access for users. □cite□turn0search2□
Microsoft Defender for Office 365 Plan 2	Offers comprehensive protection against phishing, malware, and other threats targeting email and collaboration tools. Features include:- **Safe Attachments**: Scans email attachments in a virtual environment before delivery.- **Safe Links**: Protects users from malicious URLs by verifying links in real-time.- **Threat Explorer**: Provides real-time reports to investigate threats.- **Attack Simulation Training**: Conducts simulated phishing attacks to train employees. □cite□turn0search2□
Microsoft Defender for Endpoint Plan 2	Delivers advanced endpoint protection with capabilities such as:- **Threat Hunting**: Allows proactive hunting for threats across endpoints.- **Automated Investigation and Response (AIR)**: Automates the investigation and remediation of threats.- **Endpoint Detection and Response (EDR)**: Detects and responds to advanced attacks in real-time.- **Threat and Vulnerability Management**: Identifies and prioritizes vulnerabilities on endpoints. □cite□turn0search2□
Microsoft Defender for Identity	Utilizes on-premises Active Directory signals to detect and investigate advanced threats, compromised identities, and malicious insider actions. It helps in identifying suspicious activities and building a comprehensive timeline of detected behaviors. □cite□turn0search2□
Microsoft Defender for Cloud Apps	Acts as a cloud access security broker (CASB) that provides visibility and control over data travel, offers sophisticated analytics to identify and combat cyber threats across all cloud services, and helps in assessing and managing the compliance of cloud applications. □cite□turn0search2□



Feature	Entra ID Plan 1	Entra ID Plan 2
Conditional Access	✓	✓
Role-based access control (RBAC)	✓	✓
Advanced group management (dynamic groups, naming policies, expiration, default classification)	✓	✓
Cross-tenant user synchronization, multitenant organizations	✓	✓
SharePoint limited access	✓	✓
Session lifetime management	✓	✓
Identity Protection	✗	✓
Privileged Identity Management (PIM)	✗	✓
Access Reviews	✗	✓
Entitlement Management	✗	✓
Azure AD Identity Governance	✗	✓

Feature	Defender for Office 365 Plan 1	Defender for Office 365 Plan 2
Anti-phishing, anti-spam, anti-malware	✓	✓
Safe Links	✓	✓
Safe Attachments	✓	✓
Real-time detection and response	✓	✓
Automated Investigation and Response (AIR)	✗	✓
Attack Simulation Training	✗	✓
Enhanced Reporting & Threat Explorer	✗	✓
Post-breach investigation and hunting	✗	✓
Advanced threat protection for collaboration tools (Teams, OneDrive, SharePoint)	✓	✓
User and admin alerts for phishing attempts	✓	✓
Dynamic end-user training	✗	✓
AI-powered email analysis and filtering	✓	✓
Time-of-click URL filtering	✓	✓

Defender for Office 365 Plan 2 includes all the features of Plan 1, plus additional advanced security features such as Automated Investigation and Response (AIR), Attack Simulation Training, Enhanced Reporting &

Feature	Defender for Business	Defender for Endpoint Plan 2
Next-generation protection (antivirus, antimalware)	✓	✓
Attack surface reduction	✓	✓
Endpoint detection and response (EDR)	✓	✓
Centralized configuration and management	✓	✓
Automated investigation and remediation (AIR)	✗	✓
Threat and vulnerability management	✓	✓ (Advanced)
Advanced hunting	✗	✓
Threat analytics	✗	✓
Sandbox analysis	✗	✓
Microsoft Threat Experts	✗	✓
Attack simulation training	✗	✓
Extended data retention	✗	✓

Defender for Endpoint Plan 2 includes all the features of Defender for Business, plus additional advanced security features such as Automated Investigation and Remediation (AIR), Advanced Hunting, Threat Analytics, Sandbox Analysis, Microsoft Threat Experts, Attack Simulation Training, and Extended Data Retention.

Feature	Description
Identity Protection	Protect user identities and reduce the attack surface by providing insights on identity configurations and security best practices.
Threat Detection	Detect threats using real-time analytics and data intelligence across on-premises Active Directory and cloud identities.
Lateral Movement Paths	Identify and prevent lateral movement paths that attackers could use to compromise sensitive accounts.
Security Assessments	Proactively assess your identity security posture and provide recommendations to improve organizational security.
Suspicious Activity Investigation	Investigate suspicious activities with clear, actionable incident information.
Automatic Response	Respond to attacks using automatic response to compromised identities.
Integration with Microsoft Defender XDR	Fully integrated with Microsoft Defender XDR, leveraging signals from both on-premises and cloud environments.
Advanced Threat Detection	Identify advanced threats, compromised identities, and malicious insider actions targeting the organization.
Hybrid Environment Support	Secure identity monitoring across hybrid environments, including domain controllers, Active Directory Federation Services (AD FS), and Active Directory Certificate Services (AD CS).

These features help organizations secure their identity infrastructure by providing comprehensive threat detection, investigation, and response capabilities

Feature	Microsoft 365 Business Premium	Microsoft 365 E5
Cloud Discovery	✓	✓
App Connectors	✓	✓
Conditional Access App Control	✓	✓
Threat Detection	✓	✓
Information Protection	✓	✓
Shadow IT Discovery	✗	✓
Advanced Threat Protection	✗	✓
Governance Actions	✗	✓
Anomaly Detection Policies	✗	✓
OAuth App Control	✗	✓
Session Control	✗	✓
Cloud App Security Posture Management (CASPM)	✗	✓
Integration with Microsoft Defender for Endpoint	✗	✓

Microsoft 365 E5 includes all the features of Microsoft 365 Business Premium, plus additional advanced security features such as Shadow IT Discovery, Advanced Threat Protection, Governance Actions, Anomaly Detection Policies, OAuth App Control, Session Control, Cloud App Security Posture Management (CASPM),