

Added capabilities vs. Microsoft 365 Business Premium (BP)

Area	What BP already includes	Added by Defender Suite for BP	Added by Purview Suite for BP
Identity & access	Microsoft Entra ID P1 (Conditional Access, self-service password reset, etc.) [2]	Microsoft Entra ID P2: Identity Protection (risk-based policies) + ID Governance (access lifecycle/approvals) [1]	—
Endpoint security	Microsoft Defender for Business (next-gen AV, ASR, TVM, EDR for clients; SMB-optimised) [2] [3]	Defender for Endpoint Plan 2: advanced hunting & custom detections, device-based CA, broader EDR automation/analytics [1]	—
Email & collaboration threat protection	Defender for Office 365 Plan 1 (Safe Links, Safe Attachments, anti-phish for Exchange/SharePoint/OneDrive/Teams) [5] [2]	Defender for Office 365 Plan 2: Attack Simulation Training, Threat Explorer, Automated Investigation & Response (AIR) [2] [1]	Message Encryption and Customer Key options for stricter email privacy & key control (via Purview) [1]
SaaS / app security	(Baseline discovery is limited; no full CASB)	Defender for Cloud Apps (CASB/SaaS security): shadow IT discovery, SaaS posture mgmt, OAuth/app-to-app protection, controls for risky GenAI apps [1]	—
Data classification & labelling	Purview Information Protection (P1): manual sensitivity labels & encryption in Office apps/services [3] [4]	—	Purview Information Protection & Governance (E5 level): broader/automatic labelling & governance across the estate [5]
Data Loss Prevention (DLP)	Core DLP for Exchange, SharePoint, OneDrive (and Teams basics) [10] [5]	—	Expanded DLP coverage and policies across M365 workloads and endpoints with advanced controls and analytics [5]

Records & lifecycle	Basic retention policies; eDiscovery (Standard) [10] [6]	—	Records & Data Lifecycle Management (advanced retention/disposition), eDiscovery (Premium) for legal hold, custodian mgmt, analytics [1] [6]
Insider risk & comms governance	—	—	Insider Risk Management (behaviour analytics for risky activities) and Communication Compliance (monitor/flag inappropriate or risky comms) [1]
Audit & investigations	Audit (Standard) [5]	—	Audit (Premium) (deeper audit logs, longer retention, forensic analytics) + Compliance Manager (score, assessments, improvement actions) [1]
AI data security	—	—	Data Security Posture Management for AI (visibility & policy enforcement for Copilot/AI data interactions; alerts & risk scoring) <i>preview as described by Microsoft</i> [1]

Notes (licensing behaviour)

- **Seat cap:** All three Business Premium add-ons (“Defender Suite”, “Purview Suite”, and the combined **Defender + Purview Suite**) are capped at **300 seats per customer**. [\[1\]](#)
- **Combined bundle:** The **Defender + Purview Suite** bundles everything above for BP at **US\$15 user/month**, with Microsoft positioning it as up to ~68% cheaper than buying the parts separately. [\[1\]](#)
- **Endpoint ‘mixed-licence’ nuance:** If your tenant mixes **Defender for Business** (BP) and **Defender for Endpoint P2** (via the Defender Suite) the **tenant defaults to the Defender for Business experience** unless all users are moved to P2 and you request the switch via Microsoft Support. [\[1\]](#)[\[7\]](#)

References [\[1\] techcommunity.microsoft.com](#), [\[2\] learn.microsoft.com](#), [\[3\] learn.microsoft.com](#), [\[4\] learn.microsoft.com](#), [\[5\] learn.microsoft.com](#), [\[6\] learn.microsoft.com](#), [\[7\] learn.microsoft.com](#)