Copilot für Microsoft 365 – Sicherheit und Compliance

	Szenario	Microsoft 365 für Business (1-300 Mitarbeiter)		Microsoft 365 für Enterprise		
		Business Standard	Business Premium	Office 365 E3	Microsoft 365 E3	Microsoft 365 E5
Identitäts- und Zugriffsmanagement	Anmelden bei Copilot für Microsoft 365 mit einer einzigen Identität	✓	✓	✓	✓	✓
	Erzwingen von MFA beim Zugriff auf Microsoft 365 zur Verwendung von Copilot	✓	✓	Basic MFA	✓	✓
	Ermöglichen für End-user das Passwort zurückzusetzen und zu ändern, und entsperren beim Zugriff auf Microsoft 365	Cloud only	✓	Cloud only	✓	✓
	Implementieren von Richtlinien für bedingten Zugriff basierend auf Identität, Gerät und Standort beim Zugriff auf Microsoft 365 zur Verwendung von Copilot		✓		✓	✓
	Ermöglichen der Durchsetzung von Zugriffsrichtlinien nahezu in Echtzeit, auswerten von kritischen Ereignissen und sofortiges widerrufen des Zugriff auf Microsoft 365		✓		✓	✓
	Kontrollieren des Zugriffs von Cloud-Apps (Microsoft 365 und Drittanbieter)					✓
	Überprüfen, wer Zugriff auf Inhalte in Microsoft 365 Copilot hat - Reduzierung von Oversharing					✓
	Managen von just-enough und just-in-time Genehmigung für Admin-Rollen, die den Zugriff auf Copilot-Apps verwalten können					✓
Endpoint management	Push/deploy Microsoft 365 Apps auf Geräte und Copilot Zugriff gewähren		✓		✓	✓
	Verwalten von Microsoft 365 Apps-Updates		✓		✓	✓
	Beschränken der Verwendung der Microsoft 365-Apps und Teams – sowie von Copilot in diesen Apps – auf persönlichen Geräten.		✓		✓	✓
	Verhindern, dass Dateien, einschließlich der von Copilot generierten, in ungeschützten Apps gespeichert werden		✓		✓	✓
	Löschen aller Arbeitsinhalte, einschließlich der von Copilot generierten Inhalte, wenn ein Gerät verloren geht.	✓	✓		✓	✓
	Widerrufen des Arbeitszugriffs auf nicht konformen Geräten	Except windows	✓		✓	✓
Datensicherheit und Compliance	Suchen nach von Copilot generierten Daten, nach Inhalten, suchen nach Schlüsselwörtern, anwenden der gesetzlichen Aufbewahrungspflicht und exportieren von Suchergebnissen. Untersuchung von Vorfällen im Zusammenhang mit Copilot und Reaktion auf Rechtsstreitigkeiten	Content search	eDiscovery (standard)	eDiscovery (Standard)	eDiscovery (Standard)	eDiscovery (Premium)
	Audit-Protokolle für Copilot-Interaktionen	Audit (Standard)	Audit (Standard)	Audit (Standard)	Audit (Standard)	Audit (Premium)
	Anwenden einer Aufbewahrungsrichtlinie für Copilot-Interaktionen	Standard	Standard	Standard	Standard	Automatisiert
	Richtlinien zur Verhinderung von Datenverlust zum Schutz sensibler Daten, die von Copilot generiert und an Microsoft 365-Standorten gespeichert werden, vor Exfiltration		Dateien & E-Mails	Dateien & E-Mails	Dateien & E-Mails	+ Endpunkt, Teams
	Vererben von Vertraulichkeitsbezeichnungen und Zitieren von Vertraulichkeitsbezeichnungen in der Ausgabe und in Referenzen in Copilot		✓	✓	✓	✓
	Copilot verbieten, Daten, für die Benutzer keine Extraktionsberechtigungen haben, zusammenzufassen oder in die Antwortnachrichten für diese Benutzer aufzunehmen	✓	✓	✓	✓	✓
	Vertrauliche Dateien, für die Benutzer keine Anzeigeberechtigung haben, von der Verarbeitung durch Copilot für diese Benutzer ausschließen	✓	✓	✓	✓	✓
	Kennzeichnen und Schützen von Microsoft 365-Inhalten, die von Copilot verwendet werden		Manuell, Dateien und E-Mail	Office only, Manuell	Manuell	Automatisiert
	Erkennen von Verstößen gegen den Geschäfts- oder Verhaltenskodex für Copilot-Aufforderungen und -Antworten					✓
	Verhindern des Zugriffs von Copilot auf Inhalte, die mit Double Key Encryption verschlüsselt wurden					✓
	Verwenden Sie gebrauchsfertige, trainierbare Klassifikatoren für maschinelles Lernen, um vertrauliche Informationen zu identifizieren und benutzerdefinierte Klassifikatoren zu erstellen					✓
Threat protect	Erkennung und Risikobewertung von 400+ KI-Apps in einem Unternehmen					✓
	Möglichkeit, die Verwendung einer erkannten KI-App in der Organisation zu blockieren					✓

Immer up to Date!

mit Microsoft 365 & neuen Funktionen im Detail