

Purview Network DLP wird GA – blockiert Uploads von KI-Agenten

Endlich ein Türsteher, der auch Roboter nach dem Ausweis fragt. Was die allgemeine Verfügbarkeit von Purview Network DLP für dich bedeutet, was sie kann, wo sie blind ist und was du bis Weihnachten erledigt haben solltest.

Executive Summary

Microsoft hat im Security-Roundup für September 2026 die Netzwerk-DLP von Purview für allgemein verfügbar erklärt. Der Rollout läuft seit Ende September und soll Ende Oktober 2026 durch sein. Der Clou: Purview klebt nicht mehr nur am Endpunkt, in Exchange oder in SharePoint, sondern sitzt über Entra Internet Access (Teil von Global Secure Access) direkt im Netzwerkpfad. Jeder Upload, jeder Prompt, jede Datei, die zu einer nicht verwalteten Cloud- oder KI-App wandert, kann inline geprüft und abgewürgt werden.

Und das gilt nicht nur für Menschen. Auch KI-Agenten, die im Auftrag eines Nutzers unterwegs sind (On-behalf-of, kurz OBO), laufen durch dieselbe Kontrolle. Wenn dein fleißiger Agent also beschließt, die Gehaltsliste „mal eben“ an ein kostenloses Zusammenfassungs-Tool im Netz zu schicken, macht Purview jetzt genau das, was dein Datenschutzbeauftragter seit zwei Jahren nachts im Traum tut: Es sagt Nein.

Gleichzeitig fällt mit MC1478970 eine lästige Hürde: Für die Microsoft-eigene Integration über Entra Internet Access brauchst du kein Pay-as-you-go-Abo mehr. Die Lizenzierung läuft über Microsoft 365 E7 oder über Purview E5 plus Entra Internet Access. Wer Copilot und Agenten produktiv fährt, bekommt hier den zentralen Kontrollpunkt gegen Datenabfluss in Schatten-KI. Wer es ignoriert, bekommt irgendwann einen Termin bei der Aufsichtsbehörde.

i Fakten: Die harten Zahlen auf einen Blick

GA-Rollout: Ende September bis Ende Oktober 2026, weltweit. Public Preview lief seit November 2025, der ursprüngliche GA-Termin wurde verschoben.

Abdeckung: über 35.000 Apps aus dem Cloud-App-Katalog von Defender for Cloud Apps, dazu adaptive Scopes wie „Alle nicht verwalteten KI-Apps“.

Aktionen: „Nur überwachen“ und „Blockieren“. Kein Warnen mit Begründung, kein Augenzwinkern.

Prüfgrenzen: Text bis 4 MB, Dateien bis 3 MB pro Anfrage.

Worum geht es im Detail?

Klassische DLP hatte immer ein Problem mit der Geografie. Endpoint-DLP sieht, was auf verwalteten Windows- und macOS-Geräten passiert, solange der Browser mitspielt. Exchange-DLP sieht Mails, SharePoint-DLP sieht Dateien in SharePoint. Aber der Mitarbeiter, der seinen Vertragsentwurf per Desktop-App in irgendein KI-Tool kippt, oder das Office-Add-in, das

Tabelleninhalte an eine fremde API schickt, fiel gern durch alle Raster. Genau diese Lücke adressiert die Netzwerk-DLP: Sie ist egal gegenüber Browser, App oder Add-in, weil sie dort ansetzt, wo alles vorbeikommen muss, nämlich auf der Leitung.

Technisch funktioniert das so: Auf dem Entra-joined Gerät läuft der Global-Secure-Access-Client. Er leitet den Internet-Traffic über Entra Internet Access, Microsofts Secure Web Gateway im SASE-Baukasten. Dort wird der TLS-Verkehr aufgebrochen, denn ohne TLS-Inspektion sieht auch der beste Inspektor nur verschlüsselten Zeichensalat. Eine Content-Policy mit der Aktion „Scan with Purview“ schickt die relevanten Inhalte in Echtzeit an Purview. Purview klassifiziert mit denselben Sensitive Info Types, Vertraulichkeitslabels und Klassifizierern, die du ohnehin schon gepflegt hast (oder zumindest pflegen wolltest), und liefert ein Urteil zurück: durchlassen oder blocken.

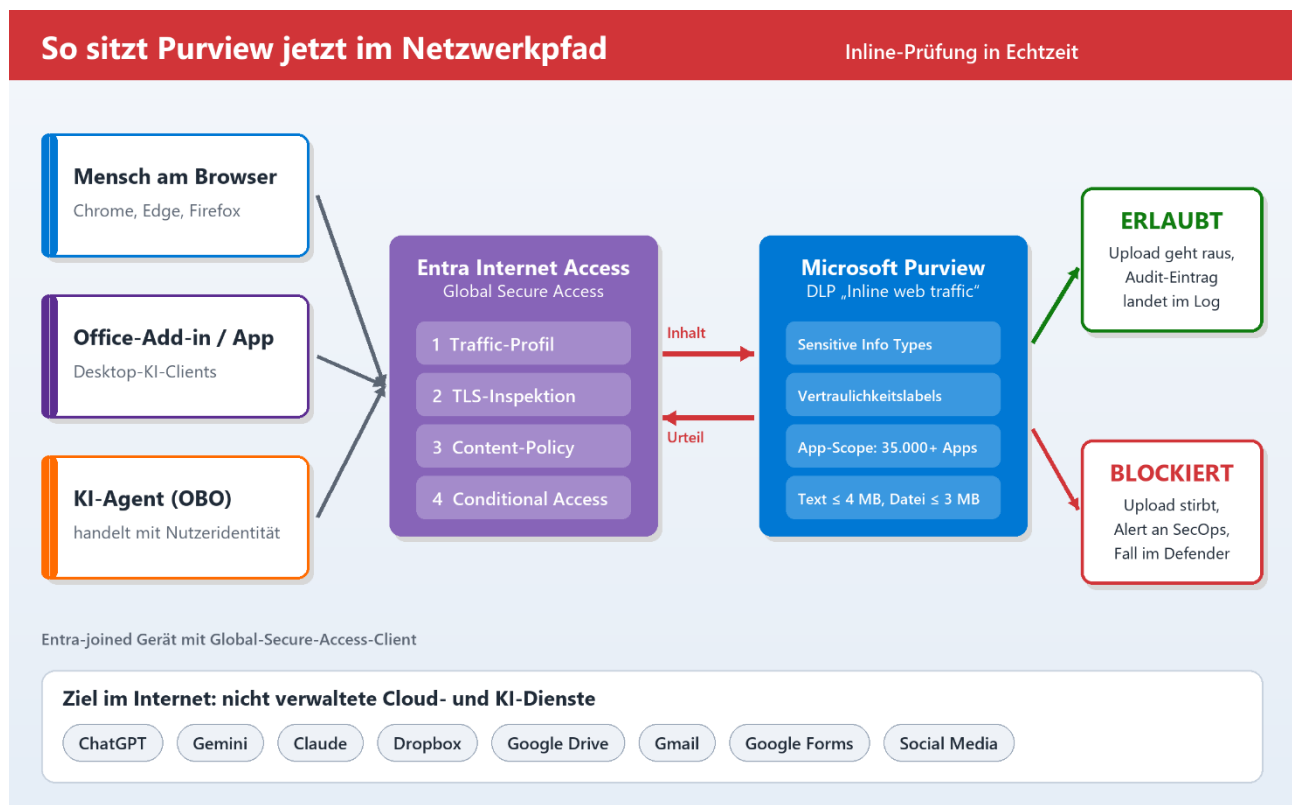


Abbildung 1: Der Weg eines Uploads vom Gerät über Entra Internet Access und Purview bis zum Ziel

In Purview heißt das neue Szenario „Inline web traffic“. Du legst eine DLP-Richtlinie an, wählst als Ziel etwa den adaptiven Scope „Alle nicht verwalteten KI-Apps“, schaltest den Durchsetzungsort „Netzwerk und nicht-Microsoft-Secure-Browser“ ein und definierst Bedingungen und Aktionen. Überwacht werden vier Aktivitäten: Text an eine Cloud- oder KI-App senden, Datei hochladen, Text empfangen und Datei herunterladen. Entra Internet Access unterstützt alle vier, bei Drittanbietern hängt es vom Partner ab. Treffer landen im Activity Explorer (Filter „Enforcement plane: network“), in DSPM for AI und bei konfigurierten Alerts in Purview und Defender.

Jetzt zum spannenden Teil, den KI-Agenten. Ein OBO-Agent arbeitet mit der Identität des Nutzers. Aus Netzwerksicht ist sein Traffic also Traffic dieses Nutzers auf diesem Gerät, und genau deshalb greift dieselbe Richtlinie. Das ist der eigentliche Paradigmenwechsel: Du musst nicht für jeden Agenten ein eigenes Regelwerk erfinden, sondern der Agent erbt die Leitplanken seines Menschen. Der Agent ist ab sofort so eingeschränkt wie der Praktikant, in dessen Namen er arbeitet. Das klingt banal, ist aber der Unterschied zwischen Governance und Hoffnung.

Warum gerade jetzt? Weil sich die Angriffsfläche verschoben hat. Früher war Datenabfluss ein USB-Stick in der Jackentasche oder eine Mail an die private Adresse. Heute ist es ein Prompt. Jeder Kopiervorgang in ein Chatfenster ist technisch ein Upload an einen Dritten, nur fühlt er sich nicht so an. Dazu kommen Agenten, die ohne Mittagspause Dateien lesen, zusammenfassen und weiterreichen. Kein Mensch schaut jedem dieser Schritte zu. Genau deshalb verlagert Microsoft die Kontrolle dorthin, wo niemand vorbeischieben kann, und macht Purview zum Zöllner an der Grenze, statt es nur in den Häusern patrouillieren zu lassen.

Szenario	Vor Network DLP	Mit Network DLP (GA)
Prompt im Browser an ChatGPT	Endpoint-DLP, nur mit unterstütztem Browser	Inline geprüft, egal welcher Browser
Datei-Upload per Desktop-KI-App	Meist unsichtbar	Prüfung auf der Leitung, Block möglich
Office-Add-in schickt Daten an API	Blinder Fleck	Wird als Text oder Datei erkannt
KI-Agent (OBO) lädt Dokument hoch	Keine zentrale Kontrolle	Gleiche Policy wie beim Nutzer
B2B-Gastbenutzer	Außen vor	Weiterhin außen vor

★ Wichtig: Microsoft 365 Copilot ist nicht das Ziel

Die Regeln für nicht verwaltete Apps betreffen nur die Consumer-Version von Microsoft Copilot. Microsoft 365 Copilot mit Enterprise Data Protection ist ein verwalteter Dienst und wird über die bekannten Purview-Mechanismen geschützt. Network DLP ist der Zaun um die Wildnis, nicht um den eigenen Garten.

Was sind Chancen? Was sind Risiken?

Die größte Chance ist Ehrlichkeit. Jede Organisation, die behauptet, sie habe keine Schatten-KI, hat entweder keine Mitarbeiter oder kein Logging. Mit einer Audit-Policy siehst du zum ersten Mal schwarz auf weiß, wer welche sensiblen Inhalte an welche Dienste schickt. Ein Kunde aus dem Maschinenbau war sich sicher, dass „bei uns niemand ChatGPT benutzt“. Nach zwei Wochen Audit-Modus hatten wir 1.400 Treffer, darunter komplette Angebotskalkulationen und eine Stückliste mit dem freundlichen Label „Streng vertraulich“. Der Geschäftsführer hat die Liste schweigend gelesen und dann gefragt, ob man die KI auch abmahnen kann.

Zweite Chance: Du kannst KI erlauben, statt sie zu verbieten. Wer weiß, dass Kreditkartennummern und als vertraulich gelabelte Dokumente an der Leitung hängen bleiben, kann der Belegschaft mehr Freiheit bei den Werkzeugen lassen. Das ist deutlich angenehmer als die klassische Methode, bei der die IT alles sperrt und die Leute dann eben über ihr privates Smartphone arbeiten, wo niemand mehr irgendwas sieht.

Die Risiken sind allerdings real, und manche davon beißen. TLS-Inspektion ist ein Eingriff mit Nebenwirkungen: Zertifikats-Pinning, Banking-Seiten, Gesundheitsportale und Betriebsrat wollen berücksichtigt werden. Die Prüfgrenzen von 4 MB Text und 3 MB pro Datei bedeuten, dass die 80-MB-PowerPoint mit der Übernahmestrategie nicht inhaltlich bewertet wird. Einige KI-Dienste wie Runway oder Meta AI schicken Inhalte laut Microsoft zeitweise kodiert an dynamisch erzeugte Endpunkte, was die Durchsetzung stören kann. Und B2B-Gäste sind komplett ausgenommen.

Und dann ist da noch das Thema Fehlalarme. Sensitive Info Types sind keine Hellseher. Eine Artikelnummer, die zufällig wie eine Kreditkartennummer aussieht, reicht für einen Block. Ein Kunde aus der Logistik hat das erlebt, als plötzlich keine Sendungsnummern mehr ins Tracking-Portal eines Partners gingen. Die Lösung war kein Zauberwerk, sondern Feinarbeit an den Schwellenwerten. Aber sie kostete drei Tage und einen sehr schlecht gelaunten Versandleiter.

Chancen	Risiken
Sichtbarkeit über Schatten-KI in allen Browsern, Apps und Add-ins	TLS-Inspektion bricht Anwendungen mit Zertifikats-Pinning
Agenten erben die Leitplanken ihres Nutzers	Große Dateien über 3 MB werden nicht inhaltlich geprüft
Wiederverwendung bestehender Klassifizierer und Labels	Kodierte Uploads einzelner KI-Dienste entweichen
Kein Pay-as-you-go mehr für die Entra-Integration	Lizenzfrage: E7 oder Purview E5 plus Internet Access
Alerts zentral in Purview und Defender	Nur Entra-joined Geräte, keine B2B-Gäste

⚠️ Warnung: Die Consumer-Enterprise-Falle

Nutzen Consumer- und Enterprise-Version einer App dieselbe URL, etwa bei ChatGPT, erwischst deine Richtlinie beide. Wer „alle KI-Apps blockieren“ klickt, blockiert also auch das teuer lizenzierte ChatGPT Enterprise der Marketingabteilung. Die Marketingleiterin wird dich finden. Sie findet immer alle.

⚠️ Warnung: Autonome Agenten sind eine andere Baustelle

Die GA-Meldung spricht ausdrücklich von OBO-Traffic, also Agenten mit Nutzeridentität auf dem Gerät. Ein Agent, der mit eigener Identität irgendwo in der Cloud läuft und nie durch deinen GSA-Client muss, fährt an diesem Türsteher schlicht vorbei. Prüfe also genau, wo deine Agenten eigentlich wohnen.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Du musst nichts sofort tun, das Feature kommt von allein in deinen Tenant. Die schlechte: Es tut auch nichts von allein. Ohne GSA-Client, TLS-Inspektion, Content-Policy und

Conditional Access bleibt Network DLP ein hübscher Menüpunkt. Microsoft selbst stuft den Admin-Aufwand als hoch ein, und ausnahmsweise ist das keine Übertreibung.

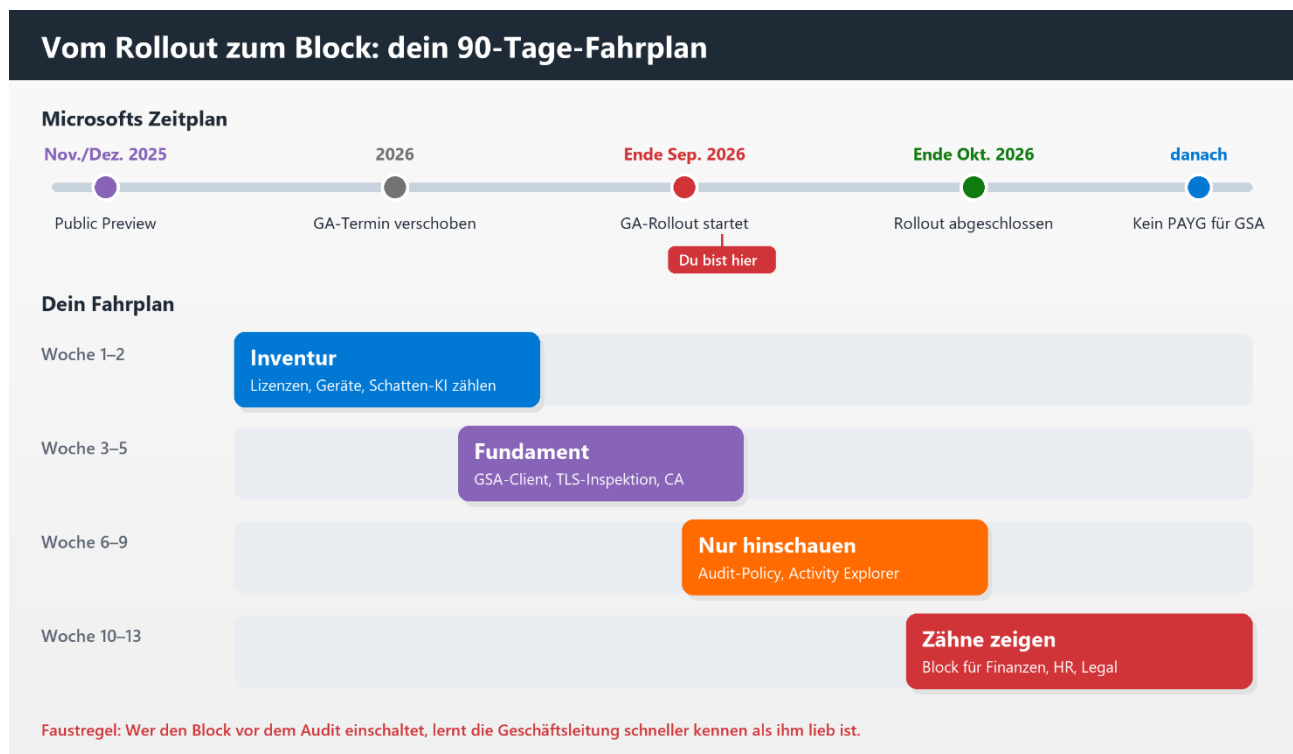


Abbildung 2: Microsofts Zeitplan und ein realistischer 90-Tage-Fahrplan für die Einführung

Fang mit der Inventur an. Kläre, welche Nutzer E7 oder die Kombination aus Purview E5 und Entra Internet Access haben, denn ohne die passende Lizenz gibt es nur Zuschauen von der Tribüne. Prüfe, wie viele Geräte wirklich Entra-joined sind; hybride Altlasten und Privatgeräte fallen raus. Und zieh aus Defender for Cloud Apps die Liste der tatsächlich genutzten KI-Dienste. Die ist in der Regel länger als die Liste der genehmigten, und zwar ungefähr um den Faktor „Oh.“

Danach kommt das Fundament: GSA-Client ausrollen, Internet-Access-Traffic-Profil aktivieren, TLS-Inspektion mit sauberen Ausnahmen konfigurieren, eine Content-Policy mit „Scan with Purview“ anlegen und das Sicherheitsprofil per Conditional Access an die richtigen Gruppen hängen. Plane nach der Integration bis zu 24 Stunden ein, bis Richtlinien verteilt sind und erste Daten auftauchen, und danach bis zu 30 Minuten Verzögerung im Activity Explorer. Wer im Pilot nach fünf Minuten „geht nicht“ ruft, hat einfach zu früh gerufen.

Dann folgt die wichtigste Phase, die am häufigsten übersprungen wird: nur hinschauen. Starte mit der One-Click-Policy aus DSPM for AI („Detect sensitive info shared with AI via network“) oder einer eigenen Audit-Richtlinie. Werte die Treffer aus, korrigiere Fehlalarme, sprich mit Fachbereichen. Erst dann schaltest du Block ein, und zwar zuerst für Finanzen, HR und Rechtsabteilung. Ein Kunde aus dem Handel hat es andersherum gemacht, am Freitagnachmittag, für alle. Am Montag konnte die Buchhaltung keine Rechnungen mehr an einen externen Steuerberater-Upload schicken, weil IBANs im Spiel waren. Der Admin hat überlebt. Knapp.

Aufgabe	Verantwortlich	Bis wann
Lizenzstand E7 bzw. Purview E5 + Entra Internet Access prüfen	Lizenzmanagement	Oktober 2026
Schatten-KI-Inventur aus Defender for Cloud Apps	Security	Oktober 2026
TLS-Inspektion mit Betriebsrat und Datenschutz abstimmen	CISO, DSB, Betriebsrat	November 2026
GSA-Client auf Entra-joined Geräte ausrollen	Endpoint-Team	November 2026
Audit-Policy „Inline web traffic“ aktivieren	Purview-Admin	November 2026
Block-Regeln für sensible Fachbereiche einschalten	Purview-Admin, Fachbereich	Dezember 2026
Agenten-Inventar: OBO oder eigene Identität?	KI-Plattform-Team	Dezember 2026

✓ Tipp: Scopes sauber ziehen

Existiert eine App im Katalog unter mehreren Namen, zum Beispiel QwenAI und Qwen Chat, nimm alle Einträge in die Richtlinie auf. Sonst ist deine Regel so dicht wie ein Nudelsieb mit Designerlabel.

✓ Tipp: Betriebsrat früh ins Boot

TLS-Inspektion plus Inhaltsprüfung plus optionales Content Capture von KI-Konversationen: Das ist mitbestimmungspflichtig, Punkt. Wer den Betriebsrat erst nach dem Rollout informiert, erlebt den Rollback gleich mit.

Häufig gestellte Fragen

Welche Lizenz brauche ich für Purview Network DLP mit Entra Internet Access?

Du brauchst entweder Microsoft 365 E7 oder Purview E5 (oder gleichwertig) pro Benutzer zusammen mit einer Lizenz für Entra Internet Access. Seit dem Rollout ab Ende September 2026 ist für die Microsoft-eigene Integration kein Pay-as-you-go mehr nötig, für Drittanbieter-SASE aber weiterhin.

Kann Purview Network DLP Uploads von KI-Agenten blockieren?

Ja, sofern der Agent im Auftrag eines Nutzers mit dessen Identität arbeitet und sein Traffic über Global Secure Access läuft. Dann greift für den Agenten dieselbe DLP-Richtlinie wie für den Menschen, inklusive Block und Alert.

Funktioniert Purview Network DLP ohne TLS-Inspektion?

Nein. Ohne TLS-Inspektion in Entra Global Secure Access kann der Inhalt verschlüsselter Verbindungen nicht an Purview übergeben und klassifiziert werden, die Inline-Prüfung bleibt dann wirkungslos.

Wie groß dürfen Dateien sein, damit Purview Network DLP sie prüft?

Purview bewertet bei der Inline-Prüfung Dateien bis 3 MB und Textinhalte bis 4 MB pro Anfrage. Größere Inhalte werden nicht vollständig inhaltlich analysiert, deshalb gehören ergänzende Kontrollen wie Endpoint-DLP und Vertraulichkeitslabels weiterhin dazu.

Blockiert Purview Network DLP auch Microsoft 365 Copilot?

Nein, die Regeln für nicht verwaltete Apps gelten nur für die Consumer-Version von Microsoft Copilot. Microsoft 365 Copilot mit Enterprise Data Protection wird über die regulären Purview-Funktionen abgesichert.