

SECURITY & COMPLIANCE

Purview integriert Global Secure Access für Netzwerk-Ebene-DLP bei KI-Nutzung

Executive Summary

Jahrelang lief dein Data-Loss-Prevention-Konzept nach einem simplen Prinzip: Du schützt, was Microsoft gehört. SharePoint, Exchange, OneDrive, Teams, dazu Endpoint DLP auf den verwalteten Windows-Geräten und für die Gewissenhaften noch eine Browser-Erweiterung im Edge. Alles ordentlich, alles auditierbar, alles nutzlos in genau dem Moment, in dem ein Kollege den Quartalsbericht markiert, Strg+C drückt und ihn in ein Chatfenster kippt, das in keiner deiner Richtlinien vorkommt.

Genau diese Lücke schließt Microsoft jetzt. Purview Network Data Security klinkt sich über Entra Global Secure Access direkt in den Datenstrom ein. Der GSA-Edge bricht die TLS-Verbindung auf, eine Content Policy mit der Aktion „Scan with Purview“ reicht den Inhalt an die Klassifizierung weiter, und Purview entscheidet in Echtzeit: durchlassen oder blocken. Der entscheidende Punkt steckt im Kleingedruckten: Die Durchsetzung hängt nicht mehr daran, dass das Ziel eine verwaltete Microsoft-Anwendung ist. Sie hängt nur noch daran, dass der Traffic durch deinen Tunnel läuft.

Der Reifegrad ist ordentlich, aber noch nicht fertig: Die Roadmap-ID 566528 nennt den Preview-Start für Anfang Juli 2026, die allgemeine Verfügbarkeit beginnt Ende September 2026 und soll Ende Oktober abgeschlossen sein. Du bist also mitten im Übergang. Zwei Dinge solltest du dabei nüchtern einplanen. Erstens: Das Feature ist nicht in E5 enthalten, sondern läuft über Pay-as-you-go mit Azure-Abo, abgerechnet je Request. Zweitens: Ohne TLS-Inspektion passiert gar nichts, und TLS-Inspektion ist kein technisches Thema, sondern ein politisches.

FAKTEN: Die drei Zahlen, die du im Kopf haben solltest

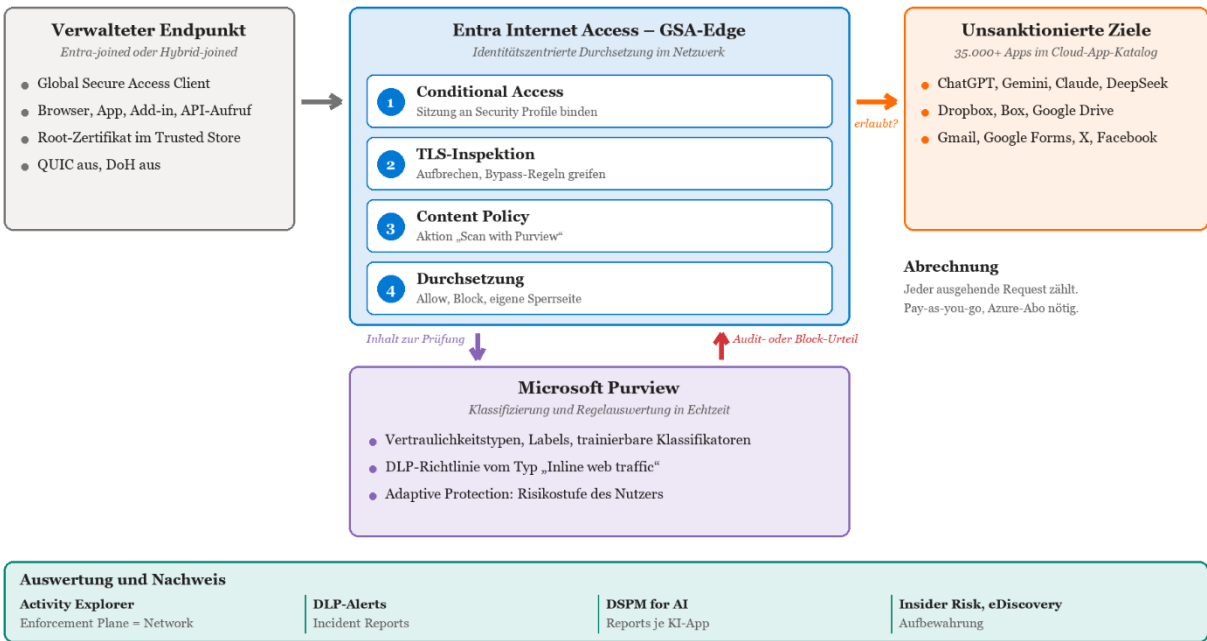
Roadmap-ID 566528. GA-Fenster Ende September bis Ende Oktober 2026. Abrechnung über Pay-as-you-go zum Listenpreis von rund 0,50 US-Dollar je 10.000 inspizierten Requests. Während der Public Preview fallen für die Durchsetzung über Global Secure Access keine zusätzlichen Gebühren an — das ändert sich mit der GA.

Worum geht es im Detail?

Technisch besteht die Lösung aus zwei Hälften, die sich gegenseitig brauchen und getrennt konfiguriert werden. Das ist der häufigste Stolperstein, deshalb gleich vorweg: Wer nur eine der beiden Hälften baut, bekommt kein halbes Ergebnis, sondern gar keines.

Netzwerk-DLP: Wer inspiziert was, und wer entscheidet?

Datenpfad einer Eingabe in einen nicht sanktionierten KI-Dienst – vom Endpunkt bis zur Block-Entscheidung



Grafik 1: Der Datenpfad einer KI-Eingabe. Global Secure Access sieht den Traffic, Purview fällt das Urteil, Global Secure Access setzt es durch.

Die erste Hälfte lebt in Entra. Du aktivierst das Internet-Access-Traffic-Profil, rollst den Global Secure Access Client auf Entra-joined oder Hybrid-joined Geräte aus und richtest eine TLS-Inspektionsrichtlinie ein. Danach legst du unter „Global Secure Access > Secure > Content policies“ eine Inhaltsrichtlinie an. In deren Regel wählst du als Aktion nicht Allow oder Block, sondern „Scan with Purview“ — und genau hier beginnt der interessante Teil. Diese Content Policy verknüpfst du mit einem Security Profile, und das Security Profile bindest du über eine Conditional-Access-Richtlinie an Nutzer und Sitzung. Das ist der Unterschied zu klassischen Proxy-Ansätzen: Die Entscheidung ist identitätszentriert. Der Praktikant und der Vorstand laufen durch dieselbe Leitung und bekommen trotzdem unterschiedliche Antworten.

Die zweite Hälfte lebt in Purview. Dort legst du eine DLP-Richtlinie vom Typ „Inline web traffic“ an. Wichtig: Du kannst keine bestehende Richtlinie umwidmen, dieser Typ wird bei der Erstellung festgelegt und lässt sich nicht nachrüsten. Als Datenquelle wählst du entweder einzelne Cloud-Apps aus dem Katalog von Defender for Cloud Apps — über 35.000 Einträge — oder du greifst zu einem Adaptive App Scope wie „All unmanaged AI apps“. Unter „Choose where to enforce the policy“ muss „Network and non-Microsoft secure browsers“ aktiv sein. Als Aktion gibt es genau eine: „Restrict browser and network activities“, wahlweise auf Audit oder Block, für vier Aktivitäten.

Was Purview an der Netzwerkebene tatsächlich sieht und tun kann

Aktivität	Bedeutung im Alltag	Verfügbare Aktion
Text gesendet	Prompt, Formularinhalt, E-Mail-Text, JSON an eine API	Audit oder Block
Datei hochgeladen	PDF, Office-Datei, Quellcode, Archiv, Bild	Audit oder Block

Aktivität	Bedeutung im Alltag	Verfügbare Aktion
Text empfangen	Antwort des KI-Dienstes zurück an den Nutzer	Audit oder Block
Datei heruntergeladen	Rückfluss aus der unsanktionierten App auf das Gerät	Audit oder Block

Als Bedingungen stehen dir die Klassifikatoren zur Verfügung, die du ohnehin schon gepflegt hast: Vertraulichkeitstypen, Vertraulichkeitsbezeichnungen, trainierbare Klassifikatoren, dazu Dateieigenschaften und — der eigentlich spannende Hebel — die Risikostufe aus Adaptive Protection. Damit kannst du eine Regel bauen, die für die Belegschaft nur protokolliert und ausgerechnet bei dem Kollegen blockt, der seit drei Wochen auffällig viel exportiert und seit gestern eine Kündigungsfrist hat. Das ist keine Schikane, das ist Verhältnismäßigkeit.

Der Mehrwert wird erst im Vergleich mit den bestehenden Ebenen richtig sichtbar. Du hast heute in aller Regel zwei Durchsetzungspunkte, und beide haben denselben blinden Fleck: Sie brauchen etwas, das du kontrollierst — ein onboardetes Gerät oder einen bestimmten Browser.

Die drei Durchsetzungsebenen im direkten Vergleich

Ebene	Greift bei	Braucht	Typische Lücke
Endpoint DLP	Windows- und macOS-Geräte im Browser	Onboarding, Purview-Browsererweiterung	Nicht onboardete Geräte, Nicht-Browser-Clients
Browser-DLP (Edge)	Edge for Business	Edge als Pflichtbrowser	Chrome, Firefox, Desktop-Apps, API-Aufrufe
Netzwerk-DLP (GSA)	Allem, was durch den Tunnel läuft	Entra Internet Access, TLS-Inspektion, Pay-as-you-go	QUIC, Nicht-HTTP, Geräte ohne GSA-Client

WARNUNG: TLS-Inspektion ist ein Betriebsrats-Thema, kein Firewall-Thema

Du brichst per Definition verschlüsselte Verbindungen deiner Belegschaft auf und liest den Klartext mit. Microsoft legt beim Anlegen der Richtlinie automatisch eine empfohlene Bypass-Regel für die Kategorien Bildung, Finanzen, Behörden sowie Gesundheit und Medizin an — und das ist kein Zufall, sondern eine juristische Schutzhaltung. Nimm diese Bypass-Liste ernst, erweitere sie um alles, was nach Arztportal, Gewerkschaft, Bewerbung oder Online-Banking riecht, und dokumentiere die Entscheidung sauber. Wenn das Onlinebanking eines Kollegen in deinem Mitschnitt landet, hilft dir kein Roadmap-Eintrag mehr.

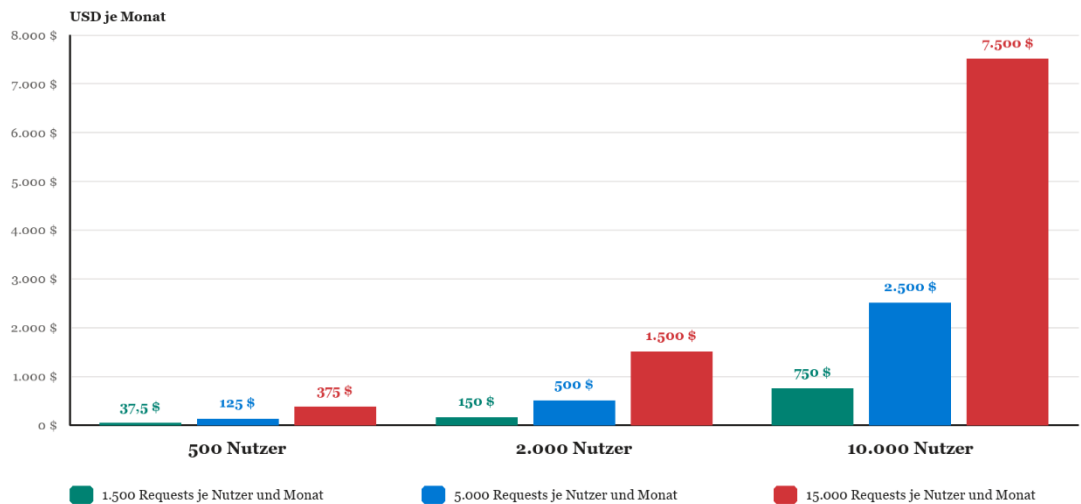
Was sind Chancen? Was sind Risiken?

Die große Chance ist nicht das Blocken. Die große Chance ist, dass du zum ersten Mal belastbar weißt, was eigentlich passiert. Bei einem Kunden aus dem Maschinenbau hatten wir vor der Einführung eine gepflegte Liste mit vier zugelassenen KI-Diensten und einer klaren Betriebsanweisung. Nach zwei Wochen Sammlungsrichtlinie im reinen Audit-Modus lagen 31 verschiedene KI-Dienste im Activity Explorer. Der meistgenutzte war weder Copilot noch ChatGPT, sondern ein kostenloser Übersetzungsdienst, durch den die Vertriebsabteilung sämtliche Angebotstexte für den polnischen Markt geschickt hatte. Inklusive Preisen. Niemand hatte böse Absichten, alle wollten nur schneller fertig werden.

Der zweite Gewinn ist Anschlussfähigkeit. Was an der Netzwerkebene erfasst wird, landet nicht in einem Sonderprotokoll, sondern in genau den Werkzeugen, die deine Leute schon bedienen können: Activity Explorer mit dem Filter „Enforcement Plane = Network“, DLP-Alerts, DSPM for AI, Insider Risk Management, Communication Compliance, eDiscovery und Aufbewahrungsrichtlinien. Wer eine Sammlungsrichtlinie mit aktivierter Inhaltserfassung fährt, hat den vollständigen Dialog zwischen Nutzer und KI-Dienst im Zugriff. Das ist gleichzeitig die größte Chance und das größte Risiko — dazu gleich mehr.

Was die Inspektion kostet, bevor jemand fragt

Monatliche Pay-as-you-go-Kosten bei 0,50 US-Dollar je 10.000 inspizierten Requests



Der Preis je Request ist harmlos. Die Menge der Requests ist es nicht. Sie entscheidet, ob du 40 Dollar oder 7.500 Dollar im Monat zahlst.

Grafik 2: Die Rechnung skaliert nicht mit deiner Nutzerzahl, sondern mit dem Traffic, den du durch die Inspektion schickst. Die Zielauswahl ist damit eine Budgetentscheidung.

Womit wir beim Geld wären. Der Preis wirkt harmlos, und pro Request ist er das auch. Abgerechnet wird jeder ausgehende Netzwerkaufruf vom Gerät zu einer Website oder API — Antworten zählen nicht mit. Das Problem ist die Menge. Eine moderne Webanwendung feuert im Hintergrund Dutzende Requests pro Minute, und wenn du deine Content Policy großzügig auf ganze Webkategorien statt auf konkrete Endpunkte legst, inspizierst du fröhlich Telemetrie und Werbepixel mit. Die Grafik zeigt, wie schnell aus 37 Dollar 7.500 Dollar im Monat werden, ohne dass sich an der Nutzerzahl etwas ändert.

Chancen und Risiken nüchtern gegenübergestellt

Thema	Chance	Risiko
Sichtbarkeit	Echte Schatten-KI-Inventur statt Vermutungen	Du siehst Dinge, die du danach nicht mehr ignorieren darfst
Durchsetzung	Blocken unabhängig von Browser und App	Ein zu strenger Block trifft Geschäftsprozesse, die du nicht kanntest
Kosten	Kein Vorabinvest, Start im kleinen Scope möglich	Requests statt Nutzer als Einheit, Kosten laufen unbemerkt hoch
Recht	Nachweisbare Kontrolle für Audit und Aufsicht	TLS-Aufbruch und Prompt-Mitschnitt brauchen Mitbestimmung

Thema	Chance	Risiko
Betrieb	Bekannte Purview-Werkzeuge, keine neue Konsole	QUIC muss aus, Zertifikat muss überall sitzen, sonst Fehlerbilder

Das unterschätzte Risiko ist nicht technischer, sondern organisatorischer Natur. Netzwerk-DLP produziert in den ersten Wochen sehr viele Treffer, weil deine Klassifikatoren nie für Fließtext in Prompts entworfen wurden. Eine Regel auf Kreditkartennummern trifft zuverlässig auch die Testdaten der Entwicklungsabteilung. Wer in dieser Phase sofort blockt, verbrennt die Akzeptanz für das ganze Vorhaben, und die bekommst du nicht zurück.

TIPP: Fang beim Ziel an, nicht bei der Regel

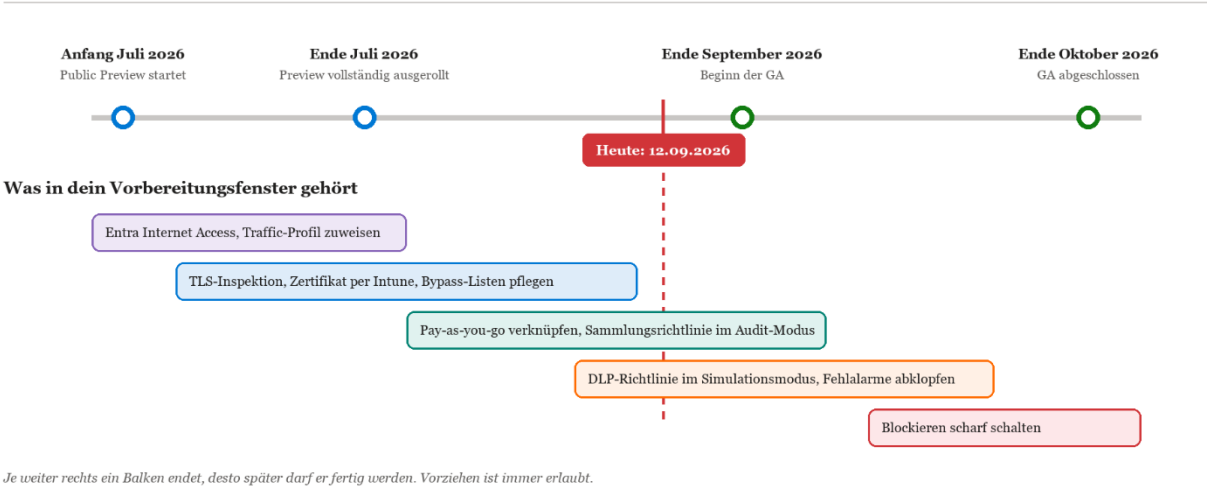
Adressiere in der Content Policy zuerst die konkreten Upload-Endpunkte statt ganzer Domänen. Für ChatGPT sind das beispielsweise die Backend-URLs für den Datei-Upload und die zugehörige Content-Domäne, nicht einfach chatgpt.com. Das findest du in fünf Minuten mit den Entwicklerwerkzeugen des Browsers, es halbiert deine Fehlalarme und deine Rechnung gleich mit. Wildcards auf Top-Level- und Second-Level-Domänen funktionieren ohnehin nicht.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Die meiste Arbeit hat nichts mit dem neuen Feature zu tun. Die schlechte Nachricht: Genau deshalb dauert sie länger, als in deinem Projektplan steht. Wer heute noch kein Entra Internet Access betreibt, baut keine Netzwerk-DLP, sondern zuerst ein SSE-Projekt. Plane das ehrlich ein.

Zeitachse: von der Preview in die Durchsetzung

Roadmap-ID 566528 – und was du parallel dazu erledigt haben solltest



Grafik 3: Der Rollout-Korridor und die Arbeitspakete, die parallel dazu laufen müssen. Der Block ganz rechts ist der einzige, den niemand vorziehen sollte.

Checkliste für die nächsten Wochen

Paket	Was konkret zu tun ist	Wer
-------	------------------------	-----

Paket	Was konkret zu tun ist	Wer
Lizenzen	Purview E5 plus Entra Internet Access oder alternativ Microsoft 365 E7 prüfen	Einkauf, Lizenzmanagement
Abrechnung	Microsoft-365-Tenant mit aktivem Azure-Abo verknüpfen, Pay-as-you-go aktivieren; ohne das lässt sich die Netzwerkdurchsetzung gar nicht erst auswählen	Cloud-Betrieb
Transport	GSA-Client ausrollen, QUIC per Firewallregel auf UDP 443 sperren, DNS over HTTPS abschalten	Client-Management
Zertifikat	Root-Zertifikat für die TLS-Inspektion per Intune in den Trusted Root Store verteilen und Bypass-Regeln für sensible Webkategorien festlegen	PKI, Client-Management
Klassifizierung	Vorhandene Vertraulichkeitstypen auf Prompt-Tauglichkeit prüfen, Schwellwerte schärfen	Information Security
Mitbestimmung	Betriebsvereinbarung zu TLS-Inspektion und Inhaltserfassung verhandeln, Nutzer transparent informieren	Datenschutz, Personalwesen
Pilot	Sammlungsrichtlinie im Audit-Modus auf eine Testgruppe, mindestens zwei Wochen beobachten	Security Operations

Ein Detail, das regelmäßig zu Verwirrung führt: Zwischen dem Anlegen der Richtlinien und den ersten sichtbaren Daten liegen bis zu 24 Stunden, bis die Konfiguration an die Netzwerklösung verteilt ist. Danach dauert es noch einmal bis zu 30 Minuten, bis ein einzelner Request im Audit-Log und im Activity Explorer auftaucht. Wenn dein Test also nach zehn Minuten nichts zeigt, ist nicht zwingend etwas kaputt — du bist nur ungeduldig. Prüfe in dieser Wartezeit lieber die Traffic-Logs unter „Global Secure Access > Monitor“, dort siehst du sofort, ob der Verkehr überhaupt durch den Tunnel läuft.

Und noch ein Realitätsabgleich zum Abschluss der Vorbereitung: Netzwerk-DLP ersetzt Endpoint DLP nicht. Sie ergänzt sie. Das Gerät ohne GSA-Client, das private Handy im WLAN des Cafés, der Kollege, der den Screenshot mit dem Handy abfotografiert — all das bleibt außerhalb. Wer die Netzwerkebene als Vollkaskoschutz verkauft, hat in sechs Monaten ein Erklärungsproblem.

WICHTIG: Simulationsmodus ist kein optionaler Luxus

Purview bietet dir beim Anlegen der DLP-Richtlinie ausdrücklich an, sie zunächst im Simulationsmodus laufen zu lassen. Nutze das. Zwei bis vier Wochen Simulation kosten dich nichts außer Geduld und ersparen dir den Anruf des Vertriebsleiters, der seinem wichtigsten Kunden gerade kein Angebot mehr schicken kann. Erst danach schaltest du gezielt einzelne Klassifizierungen auf Block — nicht die ganze Richtlinie auf einmal.

Häufig gestellte Fragen

Brauche ich für Netzwerk-DLP zwingend Microsoft 365 E5?

Nicht zwingend E5 allein, aber eine der beiden gültigen Kombinationen: entweder Microsoft 365 E7 pro Nutzer oder Purview E5 beziehungsweise gleichwertig zusammen mit Lizenzen für Entra Internet Access. Zusätzlich muss in jedem Fall das Pay-as-you-go-Abrechnungsmodell eingerichtet

sein, weil die Inspektion nach Requests abgerechnet wird und nicht über die Nutzerlizenz abgedeckt ist.

Funktioniert die Inspektion auch ohne TLS-Inspektion?

Nein. Eine einfache Inhaltsrichtlinie kann ohne Purview zwar Dateien anhand des MIME-Typs erlauben oder blockieren, aber sobald du Inhalte klassifizieren willst — und erst recht bei Text und Prompts — brauchst du die Aktion „Scan with Purview“, und die setzt eine aktive TLS-Inspektionsrichtlinie voraus. Ohne Aufbrechen der Verschlüsselung sieht der Dienst nur Zieladressen, keinen Inhalt.

Werden auch die Antworten der KI-Dienste geprüft, oder nur meine Eingaben?

Beide Richtungen sind abgedeckt: Text, der an eine Cloud- oder KI-App gesendet wird, Text, der von dort zurückkommt, sowie Datei-Uploads und Datei-Downloads. Für jede dieser vier Aktivitäten kannst du getrennt zwischen Audit und Block entscheiden.

Was passiert mit Gästen und externen Mitarbeitern?

Purview-Richtlinien für Netzwerkdatensicherheit greifen ausdrücklich nicht für B2B-Gastnutzer. Wenn externe Partner mit deinen Daten arbeiten, musst du diesen Weg über andere Mittel absichern, etwa über Vertraulichkeitsbezeichnungen mit Verschlüsselung oder über die Zugriffssteuerung selbst.

Wie verhindere ich, dass die Kosten aus dem Ruder laufen?

Über die Präzision deiner Zielauswahl. Richte die Inhaltsrichtlinie auf konkrete Upload-URLs und FQDNs der relevanten Dienste statt auf breite Webkategorien, beschränke den Pilot auf eine überschaubare Nutzergruppe und beobachte die Request-Zahlen in der Azure-Abrechnung, bevor du den Geltungsbereich erweiterst.