SECURITY & COMPLIANCE

Entra ID: Verbesserte Conditional Access Policies

CONSULTING BRIEFING · 17. SEPTEMBER 2026 · BODDENBERG.DE

Executive Summary

Falls du glaubst, deine Conditional-Access-Policies von 2023 machen heute noch genau das, was damals im Change-Ticket stand: Microsoft hat 2026 eine Nachricht für dich, und die lautet nein. Conditional Access ist in diesem Jahr an drei Stellen gleichzeitig feiner geworden – und feiner heißt in diesem Fall auch: Es greift an Stellen, an denen du es bisher nie gesehen hast.

Erstens hat Microsoft am 15. Juni 2026 ein Loch geschlossen, das jahrelang als Feature verkauft wurde: Wer eine Policy auf „Alle Ressourcen“ gebaut und eine einzige App ausgenommen hat, dessen Baseline-Scopes liefen bisher an der Prüfung vorbei. Jetzt nicht mehr. Zweitens gilt Conditional Access seit dem 6. bis 13. Juli 2026 auch während der Registrierung von Windows Hello for Business und macOS Platform SSO – der Moment, in dem ein Angreifer auf einem frisch kompromittierten Endgerät gern seine eigene passwortlose Anmeldung einrichtet. Drittens sind KI-Agenten zu vollwertigen Identitäten geworden, mit eigenen Risiko-Signalen, eigenen Policy-Zielen und einer eigenen Lizenzzeile.

Für Betreiber kritischer Infrastruktur ist das eine gute Nachricht mit Hausaufgabe. Das NIS2UmsuCG ist seit dem 6. Dezember 2025 in Kraft, die Registrierungsfrist beim BSI lief zum 6. März 2026 mit Nachfrist bis zum 31. Juli 2026, und die geschätzt 29.500 betroffenen Einrichtungen in Deutschland müssen Zugriffskontrolle und Mehrfaktor-Authentifizierung nicht nur wollen, sondern nachweisen. Conditional Access plus Anmeldeprotokolle ist dafür der pragmatischste Nachweis, den der Microsoft-Stack hergibt.

Der Handlungsauftrag in einem Satz: Prüfe deine „Alle Ressourcen“-Policies auf Ausnahmen, hebe MFA auf Authentifizierungsstärken an, und kläre, wer bei dir eigentlich für die Konten der Agenten zuständig ist. Letzteres wird die unangenehmste der drei Fragen.

FAKTEN: Die Zahl, die jedes Budgetgespräch beendet

Microsoft verarbeitet nach eigenen Angaben über 100 Billionen Sicherheitssignale pro Tag und beziffert die Risikoreduktion durch Mehrfaktor-Authentifizierung auf über 99 Prozent. Mehr als 99 Prozent der beobachteten Password-Spray-Angriffe laufen über Legacy-Authentifizierung – also über Protokolle, die du mit einer einzigen Policy abschalten kannst.

Worum geht es im Detail?

Conditional Access ist im Kern eine Wenn-dann-Maschine: Wenn Benutzer, Ressource und Bedingungen passen, dann greifen Gewährungs- und Sitzungssteuerungen. Ausgewertet wird das nicht bei der Erstanmeldung, sondern jedes Mal, wenn Entra ID ein Token ausstellt oder erneuert. Genau daraus ergeben sich die Verbesserungen des Jahres 2026 – und die Nebenwirkungen.

Baseline-Scopes: das Loch, das nie eines sein sollte. Bisher galt: Fordert eine App nur ein paar harmlose Scopes an – openid, profile, email, offline_access, User.Read, People.Read und ein

paar Verwandte – und ist irgendeine Ressource aus deiner „Alle Ressourcen“-Policy ausgenommen, dann wurde gar nicht geprüft. Die Begründung war nachvollziehbar: Fast jede App liest beim Anmelden das eigene Benutzerprofil, und niemand wollte Outlook damit abschießen. Der Nebeneffekt war weniger nachvollziehbar: Azure CLI fordert nur User.Read an, der VS-Code-Desktopclient nur openid und profile. Beide sind bisher ohne MFA-Prompt durchmarschiert. Seit dem 15. Juni 2026 werden diese Baseline-Scopes als Verzeichniszugriff gewertet und auf die Ressource „Windows Azure Active Directory“ gemappt – und damit von deiner Policy erfasst. Wer nichts tut, bekommt das Verhalten automatisch über mehrere Wochen ausgerollt.

WARNUNG: Die Woche, in der dein Helpdesk dich hasst

Ein Kunde aus der Energieversorgung hatte genau eine Ausnahme in der Tenant-MFA-Policy: einen alten Leitstand-Webclient, der App-Schutzrichtlinien nicht kann. Vier Zeilen Dokumentation, seit 2022 unangetastet. Nach dem Enforcement-Rollout standen am Montagmorgen 40 Ingenieure vor MFA-Prompts in der Azure CLI – aus Deployment-Skripten heraus, die keine Oberfläche haben und Challenges deshalb nicht beantworten können. Der Build lief nicht, die Ursache stand in keinem Change-Protokoll. Suche solche Ausnahmen, bevor sie dich suchen.

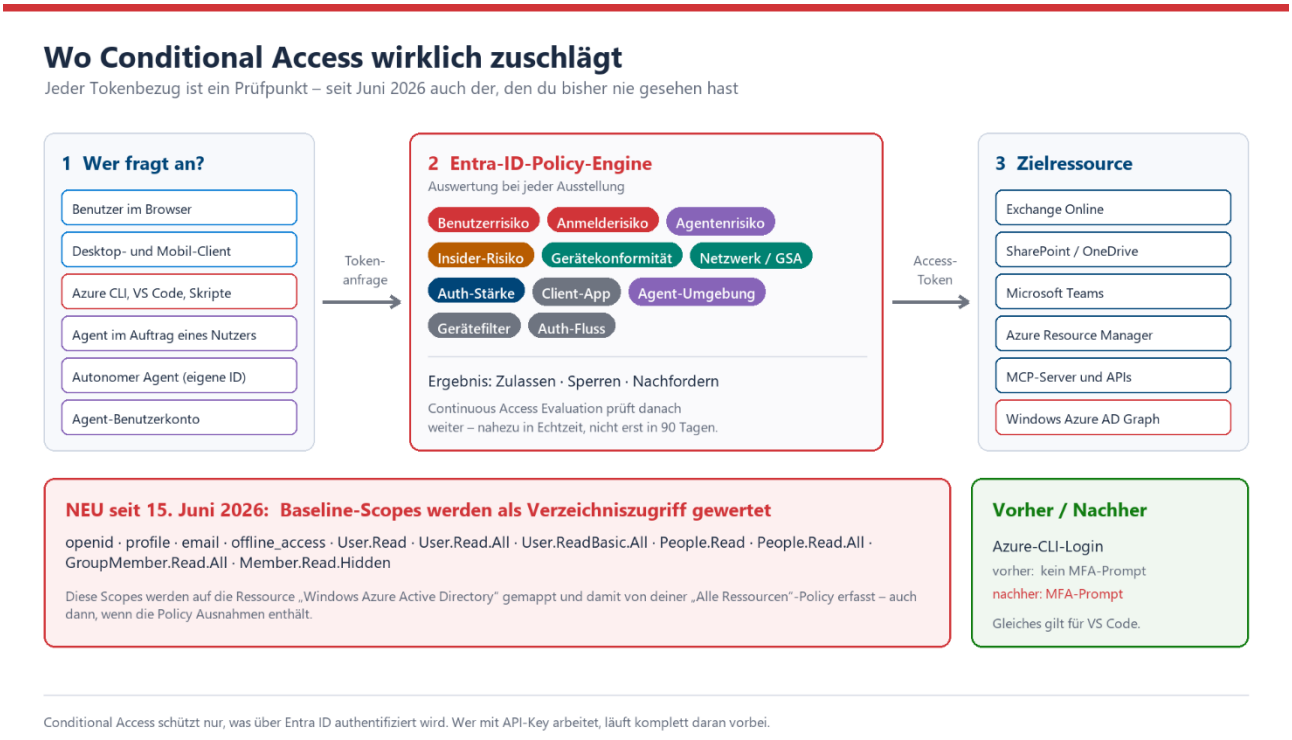

Abbildung 1: Jeder Tokenbezug ist ein Prüfpunkt. Rot markiert ist der Pfad, der bis Juni 2026 an der Auswertung vorbeilief.

Authentifizierungsstärken statt „irgendein MFA“. Die zweite Verbesserung ist die, die am meisten Sicherheit pro Aufwand bringt. „Mehrfaktor-Authentifizierung erforderlich“ ist ein grober Hebel – er akzeptiert das Einmalkennwort per SMS genauso wie den FIDO2-Stick. Authentifizierungsstärken erlauben stattdessen, pro Szenario festzulegen, welche Methodenkombinationen zählen. Es gibt drei eingebaute Stufen und beliebige eigene. Der wichtigste Stolperstein steht im Kleingedruckten: Policies werden erst nach der Erstauthentifizierung ausgewertet. Die Stärke verhindert also nicht, dass jemand sein Kennwort eintippt – sie verhindert nur, dass er damit weiterkommt. Und wer sich mit Kennwort anmeldet,

während die Policy Windows Hello verlangt, wird nicht automatisch umgeleitet, sondern muss die Sitzung neu starten und die Anmeldeoption von Hand wählen.

Methodenkombination	MFA	Passwortlos	Phishing-resistent
FIDO2-Sicherheitsschlüssel	ja	ja	ja
Windows Hello for Business / Plattform-Anmeldeinformation	ja	ja	ja
Zertifikatbasiert (mehrstufig)	ja	ja	ja
Authenticator (Telefonanmeldung)	ja	ja	nein
Temporary Access Pass	ja	nein	nein
Kennwort plus Besitzfaktor (SMS, Anruf, Push, OATH)	ja	nein	nein
Föderiert mehrstufig	ja	nein	nein
Kennwort allein, SMS-Anmeldung, QR-Code	nein	nein	nein

Token Protection gegen Wiedergabeangriffe. Token Protection bindet die Anmeldesitzung kryptografisch an das Gerät. Ein gestohlenes Token nützt dem Angreifer auf seiner Maschine dann exakt nichts. Für native Anwendungen ist das auf Windows, iOS, iPadOS und macOS allgemein verfügbar, durchgesetzt wird es für Exchange Online, SharePoint Online und Teams, auf Windows zusätzlich für Azure Virtual Desktop und Windows 365. Browserbasierte Anwendungen sind noch Vorschau und derzeit auf ausgewählte Webanwendungen begrenzt, die auf Azure Resource Manager zugreifen. Also: hervorragender Baustein, aber kein Ersatz für eine Gesamtstrategie gegen Tokendiebstahl.

Registrierung ist jetzt auch ein Tor. Bisher haben die Registrierungsflüsse für Windows Hello for Business und macOS Platform SSO deine auf „Sicherheitsinformationen registrieren“ gerichteten Policies schlicht ignoriert. MFA war zwar immer verlangt, aber Standort, Gerätekonformität oder Authentifizierungsstärke eben nicht. Seit dem 6. Juli 2026 – abgeschlossen für alle Tenants am 13. Juli – gelten deine Gewährungssteuerungen auch hier. Das schließt den Zeitpunkt, an dem ein Angreifer auf einem übernommenen Endgerät gern eine eigene passwortlose Anmeldeinformation anlegt. Die Kehrseite: Wenn deine Registrierungs-Policy einen vertrauenswürdigen Standort verlangt, kann niemand mehr Hello im Homeoffice einrichten. Das ist kein Fehler, das ist deine Policy.

Mehr Bedingungen, weniger Pauschalurteile. Unterhalb der Schlagzeilen ist der Bedingungskatalog gewachsen. Insider-Risiko zieht Signale aus der adaptiven Schutzfunktion von Microsoft Purview in die Zugriffsentscheidung – also Verhaltensmuster, historische Auffälligkeiten und Anomalien statt nur Anmeldedaten. Die Netzwerkbedingung kann verlangen, dass der Zugriff über Global Secure Access läuft, und die neue Bedingung für Authentifizierungsflüsse regelt in der Vorschau Übertragungsverfahren wie Gerätecodefluss und Authentifizierungsübertragung. Dazu kommt ein kleines, aber im Alltag wirksames Detail aus dem Mai 2026: Privileged Identity Management kann die erneute Authentifizierung bei der Rollenaktivierung jetzt über Conditional Access und Authentifizierungskontexte konfigurieren. Damit lässt sich die harte Anforderung

genau dort aufhängen, wo sie hingehört – an der Rechteerhöhung und nicht an jeder Portalanmeldung.

Microsoft-verwaltete Policies schalten sich selbst ein. Microsoft legt inzwischen selbst Policies in deinen Tenant. Sie erscheinen im Status „Nur berichten“, und wenn du nichts tust, schaltet Microsoft sie frühestens 30 Tage später scharf – angekündigt per E-Mail und Message Center, zwei Wochen vorher. Im Katalog stehen unter anderem: MFA für alle Benutzer, MFA für Administratoren in den Microsoft-Admin-Portalen, MFA und erneute Authentifizierung bei risikoreichen Anmeldungen, Legacy-Authentifizierung sperren, Gerätecodefluss sperren, Zugriff für Benutzer mit hohem Risiko sperren, Risikobehebung erzwingen und – in der Vorschau – alle Agenten mit hohem Risiko sperren. Umbenennen oder löschen kannst du sie nicht, nur ausschließen, duplizieren oder ausschalten. Trage dein Notfallkonto überall ein, bevor du es brauchst.

TIPP: Der Gerätecodefluss ist der billigste Sicherheitsgewinn des Jahres

Der Gerätecodefluss wird von Kunden fast nie gebraucht, von Angreifern dafür ausgesprochen gern. Genau deshalb gibt es die Managed Policy dafür. Wenn du Teams-Raumsysteme betreibst, nimm sie gezielt aus – die Dokumentation beschreibt dafür einen eigenen Weg – und sperre den Fluss für alle anderen Konten. Zehn Minuten Arbeit, ein ganzer Angriffsvektor weniger.

Agenten als erstklassige Identitäten. Agenten sind 2026 vom Sonderfall zur Identitätsklasse geworden. Conditional Access für Agenten verlangt Entra ID P1 oder P2 plus eine Microsoft-Agent-365-Lizenz pro Benutzer; die Service Plans „Conditional Access for Agents“ und „ID Protection for Agents“ sind ab Juli 2026 in Agent 365 und Microsoft 365 E7 gerollt. Entscheidend für die Praxis ist die Frage, wer im Token als Subjekt steht, denn danach richtet sich, welche Policy überhaupt greift. Dazu kommen zwei neue Zielarten: Agent-Identitäts-Blueprints erfassen eine ganze Klasse von Agenten samt künftiger Exemplare, und benutzerdefinierte Sicherheitsattribute machen Policies attributgesteuert statt handgepflegt. Die Bedingung „Agent-Ausführungsumgebungen“ grenzt endpunktabhängige Steuerungen auf Agenten ein, die überhaupt auf einem Gerät laufen.

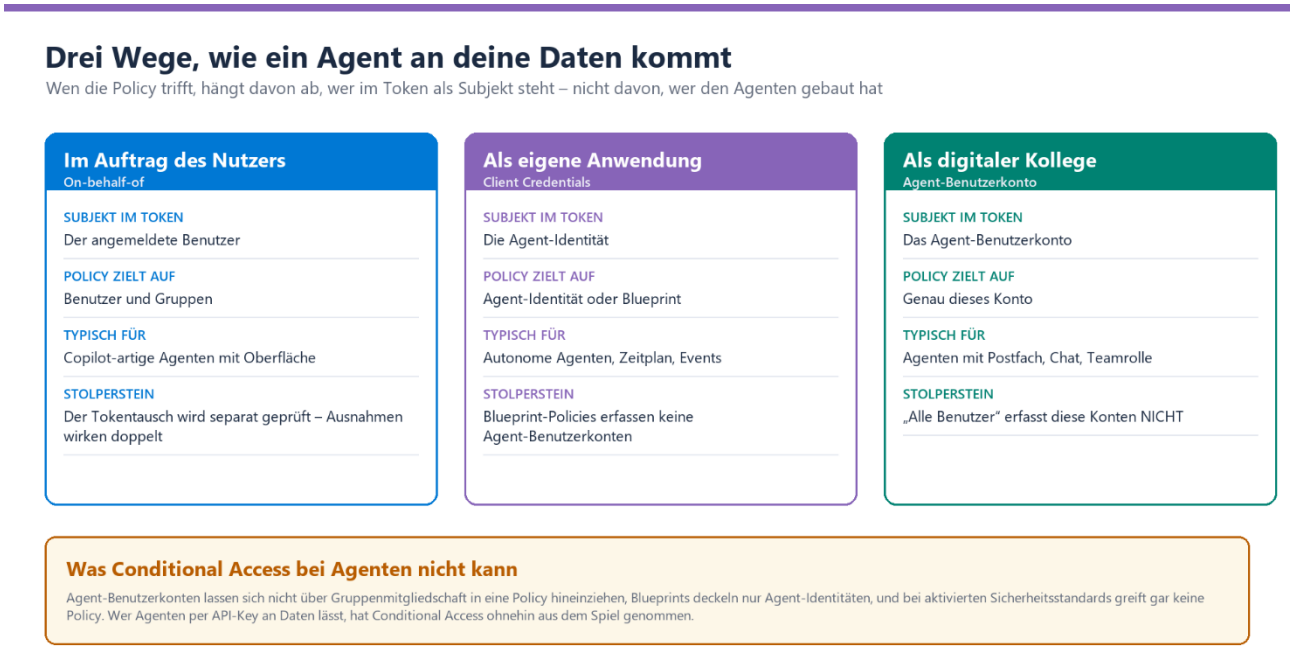

Abbildung 2: Drei Zugriffsmuster, drei völlig verschiedene Policy-Ziele – und ein Stolperstein pro Spalte.

WICHTIG: „Alle Benutzer“ heißt nicht alle Benutzer

Eine Policy, die auf alle Benutzer zielt, erfasst Agent-Benutzerkonten nicht. Diese Konten lassen sich außerdem nicht über Gruppenmitgliedschaft in eine Policy hinein- oder herausnehmen, und eine Policy auf Agent-Identitäten oder Blueprints gilt ebenfalls nicht für sie. Wenn dein digitaler Kollege ein Postfach, einen Teams-Chat und Zugriff auf die Projektablage hat, dann braucht er eine eigene, explizit adressierte Policy. Sonst ist er das einzige Teammitglied ohne Zugangskontrolle.

Der Optimization Agent als Aufräumkraft. Bleibt die Frage, wie du den Überblick behältst. Der Conditional Access Optimization Agent in Security Copilot scannt täglich neue Benutzer, Anwendungen und Agent-Identitäten der letzten 24 Stunden, sucht Abdeckungslücken, schlägt Zusammenlegungen überlappender Policies vor und legt neue Policies grundsätzlich im Modus „Nur berichten“ an. Microsoft berichtet aus der allgemeinen Verfügbarkeit von durchschnittlich 26 gefundenen Lücken pro Kunde und Monat. Die Grenzen solltest du kennen: 300 Benutzer und 150 Anwendungen pro Lauf, 40 Policy-Paare beim Konsolidierungsvergleich, keine Anpassung der Vorschläge – und mindestens eine Security Compute Unit, die monatlich abgerechnet wird, auch wenn der Agent nichts tut.

Änderung	Stand	Was du gewinnst	Was weh tut
Baseline-Scopes-Enforcement	Rollout ab 15.06.2026	Keine stillen Umgehungen mehr über Profil-Scopes	MFA-Prompts in CLI, VS Code und Eigenentwicklungen
CA bei Credential-Registrierung	Abgeschlossen 13.07.2026	Passwortlose Anmeldeinformationen nur unter deinen Bedingungen	Hello-Einrichtung scheitert bei Standort- oder Gerätezwang
Authentifizierungsstärken	Allgemein verfügbar	Phishing-resistente Methoden pro Szenario erzwingbar	Nicht kombinierbar mit „MFA erforderlich“ in derselben Policy
Token Protection	GA nativ, Browser in Vorschau	Gestohlene Token sind auf Fremdgeräten wertlos	Ressourcen- und Plattformgrenzen, Pilot nötig
Microsoft-verwaltete Policies	Laufend, Selbstaktivierung	Sicherer Standard ohne Projektaufwand	Schaltet nach 30 Tagen scharf, ob du willst oder nicht
Conditional Access für Agenten	Service Plans ab Juli 2026	Agenten werden steuerbar wie Benutzer	Agent-365-Lizenz, neue Rollen- und Zuständigkeitsfragen
Optimization Agent	GA, Teilfunktionen Vorschau	Findet Lücken, die im Audit sonst der Prüfer findet	SCU-Kosten, harte Scan-Grenzen, keine eigenen Regeln

Was sind Chancen? Was sind Risiken?

Die Chance ist strukturell: Du kannst Sicherheit endlich dort ansetzen, wo sie hingehört, statt überall gleich hart zuzuschlagen. Phishing-resistente Authentifizierung nur für den Leitstand und die Administratoren, Standardstärke für die Kantinenplanung, Gerätebindung nur für die drei Anwendungen, in denen die interessanten Daten liegen. Das senkt die Reibung genau dort, wo

Benutzer sonst kreativ werden – und in KRITIS-Umgebungen ist ein Ingenieur, der einen Workaround erfindet, ein größeres Risiko als ein fehlendes Häkchen.

Die zweite Chance ist der Nachweis. Die Risikomanagement-Pflichten des NIS2UmsuCG verlangen Zugriffskontrolle und Mehrfaktor-Authentifizierung, das BSI empfiehlt Richtlinien für bedingten Zugriff ausdrücklich als Teil des IAM-Konzepts. Eine Policy-Landschaft plus Anmelde- und Überwachungsprotokolle ist auditierbar. Ein Satz im Sicherheitskonzept ist es nicht.

Das größte Risiko ist nicht technisch, sondern kalendarisch: Diese Änderungen kommen zu dir, auch wenn dein Projekt anders getaktet ist. Enforcement-Rollouts laufen automatisch, Microsoft-verwaltete Policies aktivieren sich nach 30 Tagen. Wenn dein Change-Prozess sechs Wochen braucht, gewinnt der Rollout.

Das zweitgrößte Risiko heißt Erneuerungsfrequenz. Erneute Authentifizierung bei jedem Zugriff klingt nach Härte, produziert aber MFA-Müdigkeit – und ein Benutzer, der Prompts reflexhaft bestätigt, bestätigt irgendwann auch den des Angreifers. Microsoft warnt zusätzlich vor Anmeldeschleifen, wenn „immer“ ohne Mehrfaktor-Authentifizierung gesetzt wird. Die Voreinstellung von 90 Tagen rollierend ist kein Schlamperei-Erbe, sondern eine bewusste Entscheidung: Jeder Richtlinienverstoß widerruft die Sitzung ohnehin.

Feld	Chance	Risiko
Granularität	Harte Kontrollen nur für harte Fälle, weniger Reibung im Alltag	Policy-Wildwuchs, den in zwei Jahren niemand mehr erklären kann
Automatische Rollouts	Sicherer Standard ohne eigenes Projekt	Termine, die dein Change-Board nicht verhandeln kann
Agenten-Identitäten	Agenten werden prüfbar und abschaltbar	Nicht abgedeckte Agent-Benutzerkonten als blinder Fleck
Sitzungssteuerung	Kurze Lebensdauer für sensible Anwendungen	MFA-Müdigkeit und Anmeldeschleifen bei Übertreibung
Copilot-Unterstützung	Lücken werden gefunden, bevor der Prüfer sie findet	SCU-Kosten und Vertrauen in Vorschläge ohne eigene Prüfung

Was müssen wir jetzt schon vorbereiten?

Fang bei den Ausnahmen an, nicht bei den Policies. Jede Ausnahme in einer „Alle Ressourcen“-Policy ist ab jetzt ein potenzieller Vorfall im Helpdesk. Für die Analyse gibt es einen konkreten Trick: Registriere eine leere Platzhalter-Anwendung, hinterlege sie in den Baseline-Scopes-Einstellungen unter „Verhalten anpassen“ und filtere die Anmeldeprotokolle über Microsoft Graph nach dieser App-ID als Conditional-Access-Zielgruppe. Nach ein paar Tagen hast du eine belastbare Liste aller Clients, die ausschließlich Baseline-Scopes anfordern. Das ist deutlich präziser als Raten.

Danach räumst du die Notfallzugänge auf. Zwei ausgeschlossene Konten ohne Kennwortablauf, überwacht, dokumentiert, in jeder Managed Policy als Ausnahme eingetragen. Wer einmal einen Tenant erlebt hat, in dem eine Risiko-Policy alle Administratoren gleichzeitig ausgesperrt hat, diskutiert diesen Punkt nicht mehr.

Parallel klärst du die Lizenz- und Rollenfrage bei Agenten – und zwar bevor die erste Abteilung ihren eigenen Agenten mit Postfach betreibt. Jede der drei Zugriffsarten braucht eine andere

Policy, und Sicherheitsstandards heben die Wirkung komplett auf. In einem Tenant mit aktivierten Sicherheitsstandards greift für Agenten gar keine Conditional-Access-Policy.

Abbildung 3: Regulatorische Fristen und Microsoft-Rollouts liegen 2026 im selben Kalender.

Maßnahme	Bis wann	Verantwortlich	Aufwand
Ausnahmen aller „Alle Ressourcen"-Policies inventarisieren	sofort	Identity-Team	1–2 Tage
Platzhalter-App und Graph-Abfrage für betroffene Clients aufsetzen	sofort	Identity-Team	halber Tag
Notfallkonten in allen verwalteten Policies ausschließen	sofort	Identity-Team	2 Stunden
Registrierungs-Policies auf Machbarkeit im Homeoffice prüfen	kurzfristig	Identity + Client	1 Tag
MFA-Anforderungen auf Authentifizierungsstärken umstellen	Q4 2026	Security-Architektur	1–2 Wochen
Token Protection als Pilot im Berichtsmodus fahren	Q4 2026	Client-Management	2 Wochen
Zuständigkeit und Lizenzen für Agent-Identitäten festlegen	Q4 2026	IT-Leitung + Einkauf	Entscheidung

Policy-Nachweise für die BSI-Aufsicht dokumentieren	laufend	Informationssicherheit	laufend

Und ein letzter Rat aus der Praxis: Baue jede neue Policy zuerst im Modus „Nur berichten“, lasse sie lang genug laufen, um einen vollständigen Arbeitszyklus abzudecken – Monatsabschluss, Wartungsfenster, Urlaubsvertretung – und werte interaktive wie nicht interaktive Anmeldungen aus. Der Berichtsmodus kostet dich zwei Wochen. Ein produktiver Fehlschuss in einer Leitstelle kostet dich das Vertrauen des Betriebs, und das bekommst du nicht in zwei Wochen zurück.

Häufig gestellte Fragen

Muss ich beim Baseline-Scopes-Enforcement selbst etwas tun oder passiert das automatisch?

Das neue Verhalten wird seit dem 15. Juni 2026 über mehrere Wochen automatisch für alle Tenants ausgerollt; ohne eigene Konfiguration ist es anschließend der Standard. Du kannst es über die Baseline-Scopes-Einstellungen im Entra-Admin-Center vorher aktivieren, für einzelne Policies über eine Platzhalter-Anwendung beim alten Verhalten bleiben oder es tenantweit abschalten – wobei Letzteres eine Lücke in der Abdeckung zurücklässt.

Wie unterscheidet sich eine Authentifizierungsstärke von „MFA erforderlich“?

„MFA erforderlich“ akzeptiert jede Kombination, die als mehrstufig gilt – inklusive Kennwort plus SMS. Eine Authentifizierungsstärke legt dagegen fest, welche konkreten Methodenkombinationen zählen, etwa nur FIDO2, Windows Hello for Business oder mehrstufige zertifikatbasierte Authentifizierung. Beide Steuerungen lassen sich nicht in derselben Policy kombinieren, weil die eingebaute Stärke „Mehrfaktor-Authentifizierung“ dem alten Schalter entspricht.

Warum greift meine Policy für alle Benutzer nicht bei unseren KI-Agenten?

Weil Policies, die auf alle Benutzer zielen, Agent-Benutzerkonten ausdrücklich nicht einschließen. Diese Konten müssen explizit adressiert werden, und zwar nicht über Gruppenmitgliedschaft, sondern direkt oder über benutzerdefinierte Sicherheitsattribute. Policies auf Agent-Identitäten oder Agent-Identitäts-Blueprints gelten ebenfalls nicht für die Benutzerkonten der Agenten.

Wie oft sollten Benutzer sich neu anmelden müssen?

Die Voreinstellung von Entra ID ist ein rollierendes Fenster von 90 Tagen, und das ist bewusst so gewählt: Kennwortwechsel, Gerätekonformitätsverlust oder eine Kontodeaktivierung widerrufen die Sitzung sofort. Kurze Anmeldehäufigkeiten oder „immer erneut authentifizieren“ gehören nur auf wenige sensible Anwendungen, etwa Rollenaktivierung über Privileged Identity Management, weil häufige Prompts sonst zu MFA-Müdigkeit und damit zu neuen Risiken führen.