SECURITY & COMPLIANCE · Active Directory/Entra ID

Microsoft Entra: Tenant Governance und erweiterte Security-Administrator-Rolle

Du hast mehr Tenants, als du glaubst, und deine Security-Admins dürfen bald mehr, als du ihnen bewusst gegeben hast. Zwei Neuerungen, ein gemeinsamer Nenner: Wer jetzt nicht aufräumt, räumt später im Incident-Call auf. Mit Publikum.

Executive Summary

Microsoft hat im August 2026 **Entra Tenant Governance** allgemein verfügbar gemacht. Das Paket löst ein Problem, das jede größere Organisation hat und kaum eine zugibt: Irgendwo existieren Tenants, die niemand verwaltet. Der Test-Tenant aus dem Pilotprojekt 2019. Der Tenant, den das Marketing für ein Event „kurz mal" angelegt hat. Der Tenant der übernommenen Tochterfirma, dessen letzter Admin inzwischen bei der Konkurrenz Karriere macht. Tenant Governance findet solche Tenants anhand von Signalen, baut kontrollierte Admin-Beziehungen auf und überwacht die Konfiguration gegen eine Soll-Baseline in Entra, Intune, Exchange Online, Teams, Purview und Defender.

Parallel dazu erweitert Microsoft die eingebaute Rolle **Security Administrator**. Bis Ende September 2026 kommen vier Reaktionsrechte dazu: Konto deaktivieren, Konto wieder aktivieren, Sessions widerrufen und Passwort-Reset erzwingen, jeweils gegen nicht privilegierte Konten. Klingt nach Bequemlichkeit für das SOC, ist aber vor allem eines: eine stille Rechteausweitung für jede bestehende Zuweisung. Genau deshalb gehört die Rolle auf die Tagesordnung deines nächsten Least-Privilege-Reviews.

> **★ Wichtig: Das Wichtigste in drei Sätzen**
>
> Tenant Governance ist seit 10. August 2026 GA und zeigt dir Schatten-Tenants, Beziehungen und Konfigurations-Drift.
>
> Security Administrator kann ab Ende September 2026 nicht privilegierte Konten sperren, entsperren, abmelden und deren Passwort zurücksetzen.
>
> Beides verlangt eine Entscheidung von dir, bevor ein Angreifer oder ein Auditor sie für dich trifft.

Worum geht es im Detail?

Der Hintergrund zuerst. Multi-Tenant ist in Konzernen der Normalzustand, nicht die Ausnahme. Fusionen, abgeschottete Umgebungen für sensible Workloads, Entwicklungs- und Test-Tenants: Alles legitim. Das Problem ist der Teil, den die zentrale IT nicht kennt. Einen Tenant anzulegen kostet einen Nutzer genau eine Kreditkarte und zehn Minuten. Ihn wieder loszuwerden kostet im Zweifel ein Support-Ticket, drei Nachweise und die Geduld eines Mönchs. Bisher hattest du keinen offiziellen Weg, solche Tenants systematisch zu finden, geschweige denn deren Konfiguration zu prüfen.

Tenant Governance besteht aus vier Bausteinen, die aufeinander aufbauen:

- **Related Tenants:** Entra erkennt verwandte Tenants automatisch über drei Signale. Das B2B-Signal misst ein- und ausgehende Gastzugriffe, B2B-Registrierungen und B2B-Adminzugriffe. Das Multitenant-App-Signal findet Apps fremder Tenants mit Rechten bei dir und umgekehrt. Das Billing-Signal zeigt Tenants, die am selben Commerce-Abrechnungskonto hängen.
- **Governance Relationships:** Per Einladung, Anfrage und Freigabe baust du einen kontrollierten Admin-Zugang zwischen „governing“ und „governed“ Tenant auf. Technisch steckt GDAP dahinter, also granulare delegierte Adminrechte, kombinierbar mit PIM for Groups. Richtlinienvorlagen sorgen dafür, dass du in jedem Tenant dieselben Rechte anfragst.
- **Configuration Management:** Du beschreibst den Soll-Zustand als JSON-Baseline, ziehst bei Bedarf einen Snapshot aus einem sauberen Referenz-Tenant und lässt einen Monitor alle sechs Stunden vergleichen. Über 200 Ressourcentypen in sechs Diensten sind abgedeckt.
- **Secure Tenant Creation:** Neue Add-on-Tenants entstehen über ein MCA-Abonnement, bekommen automatisch eine Governance-Beziehung per Standardvorlage und ein „Microsoft Entra ID Free“-Billing-Asset. Das Asset belegt die kommerzielle Eigentümerschaft und hilft dem Support, dir den Zugang zurückzugeben, falls der letzte Admin geht oder ein Angreifer den Tenant übernimmt.

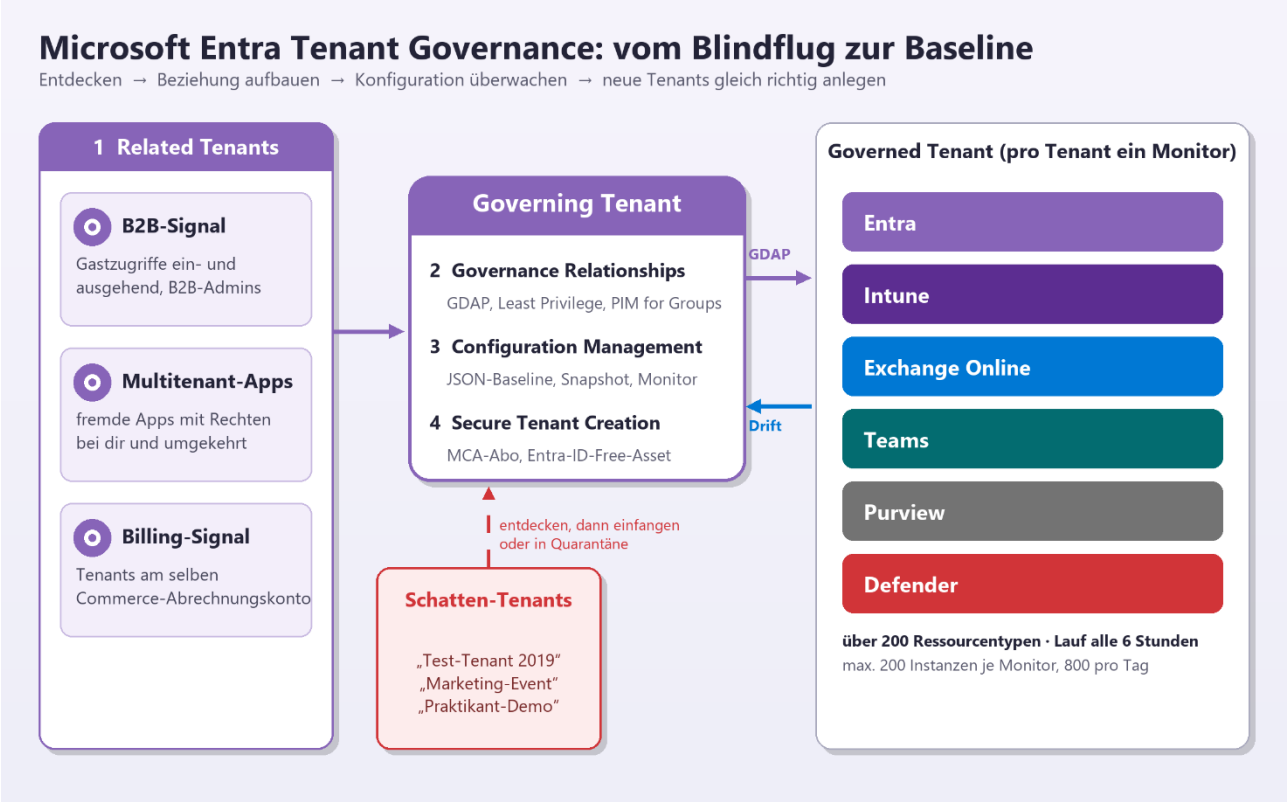

Abbildung 1: Die vier Bausteine von Entra Tenant Governance im Zusammenspiel

Die Grenzen solltest du kennen, bevor du Versprechen machst. Ein Monitor darf maximal 200 Ressourceninstanzen enthalten, pro Tenant sind 800 Instanzen am Tag drin. Wer darüber hinaus will, bekommt keinen Fehler zur Laufzeit, sondern schon beim Anlegen. Mehrstufige Beziehungen gibt es nicht: Ein Tenant ist entweder Regierung oder Untertan, nie beides. Und wer als Partner bereits eine GDAP-Beziehung über das Partner Center zu einem Kunden-Tenant pflegt, muss diese erst entfernen, bevor eine Tenant-Governance-Beziehung zum selben Tenant möglich ist.

> **ℹ Fakten: Eckdaten Tenant Governance**
>
> GA seit 10. August 2026. Lizenzstufen: kostenlos, Basic und Premium; der governing Tenant braucht eine Tenant-Governance-Lizenz.
>
> Höhere Limits für Monitore und Snapshots gibt es mit ID Governance, Entra Suite oder Microsoft E7.
>
> Monitor-Intervall sechs Stunden, erster Lauf bis zu sechs Stunden nach Anlage. Verwaltung auch per Microsoft Graph.

Und jetzt zur Rolle. Security Administrator war bisher die Rolle für Leute, die Sicherheit konfigurieren: Conditional Access, Identity Protection, PIM-Einstellungen, Security-Reports. Was fehlte, war der rote Knopf. Wenn im SOC um 3 Uhr nachts ein kompromittiertes Konto auffiel, musste jemand mit User- oder Helpdesk-Admin-Rechten geweckt werden. Microsoft schließt diese Lücke jetzt, indem die Rolle vier Aktionen dazubekommt. Die Zahl der Directory-Aktionen der Rolle steigt damit von 82 auf 86. Wichtig: Die Aktionen greifen nur gegen nicht privilegierte Konten. Einen Global Administrator sperrt der Security Administrator also weiterhin nicht, und das ist auch gut so.

Bereits im Juni 2026 hat Microsoft die neue Rolle **Entra SOC Identity Responder** eingeführt. Sie kann nicht privilegierte Konten deaktivieren und aktivieren, Refresh-Tokens ungültig machen, Passwörter von Cloud-only-Konten zurücksetzen und einzelne Authentifizierungsmethoden löschen, lässt sich auf Administrative Units beschränken und hat sonst keine Konfigurationsrechte. Sie ist also das Skalpell, während Security Administrator mit den neuen Rechten eher das Schweizer Taschenmesser mit eingebauter Kettensäge wird.

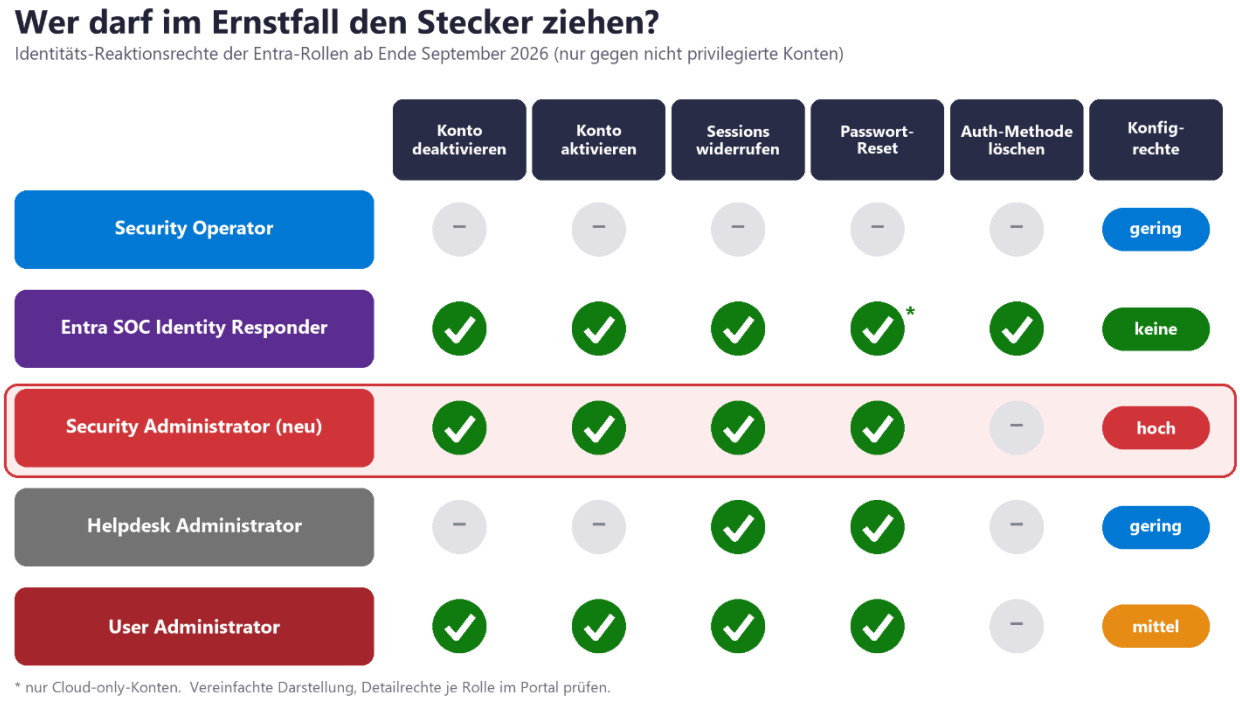

Abbildung 2: Reaktionsrechte der relevanten Entra-Rollen im Vergleich (vereinfacht)

Was sind Chancen? Was sind Risiken?

Fangen wir mit einer Geschichte an, die so oder ähnlich in fast jedem Konzern spielt. Ein Maschinenbauer mit rund 9.000 Mitarbeitern, drei Zukäufe in fünf Jahren. Auf die Frage, wie viele

Tenants es gibt, antwortet der Architekt mit fester Stimme: „Vier." Die ersten Discovery-Ergebnisse zeigen 23. Darunter ein Tenant mit dem schönen Namen „contoso-test-alt-2018", angelegt 2018, mit einer Multitenant-App, die bis heute Lesezugriff auf Mailboxen im Produktiv-Tenant hat. Der Ersteller hat das Unternehmen 2020 verlassen. Die App ist noch da. Die Berechtigung auch. Nur der Mut, das dem CISO zu erzählen, war kurzzeitig weg.

Aspekt	Chance	Risiko
Schatten-Tenants	Erstmals systematische Sicht über B2B-, App- und Billing-Signale	Discovery bedeutet nicht Eigentum; unbekannte Tenants verweigern die Beziehung
Konfigurations-Drift	Soll-Ist-Vergleich über sechs Dienste, auditfähige Snapshots	Kein Auto-Remediate; widersprüchliche Baselines melden fröhlich gegensätzliche Drifts
Admin-Zugriff	Least Privilege per GDAP und PIM for Groups statt B2B-Gastadmins	Konflikt mit bestehenden Partner-Center-GDAP-Beziehungen, keine Mehrstufigkeit
Tenant-Erstellung	Neue Tenants automatisch unter Governance, Wiederherstellung über Billing-Asset	Nur mit MCA-Abo; ohne Standardvorlage entsteht keine Beziehung
Security Administrator	SOC kann sofort containen, ohne zweite Rolle	Stille Rechteausweitung für alle aktiven und berechtigten Zuweisungen
SOC Identity Responder	Minimalrolle nur für Containment, auf AUs beschränkbar	Wird ignoriert, weil Security Administrator „eh schon alles kann"

Die Chance bei Tenant Governance ist handfest: Du bekommst eine belastbare Inventur, eine saubere Admin-Struktur ohne B2B-Gastkonten-Wildwuchs und einen Drift-Monitor, der dir sagt, wann jemand „nur mal eben" eine Conditional-Access-Richtlinie entschärft hat. Für Revisionen sind Snapshots Gold wert, weil du den Konfigurationsstand zu einem Stichtag belegen kannst.

Für Partner und Konzern-IT gleichermaßen interessant ist das Zusammenspiel mit bestehenden Admin-Modellen. Viele Unternehmen verwalten Tochter-Tenants heute über B2B-Gastkonten, denen in jedem Tenant einzeln Rollen zugewiesen werden. Das funktioniert, bis jemand das Unternehmen verlässt und in sieben Tenants noch als Global Administrator herumgeistert, wie ein Gespenst mit Schreibrechten. Governance Relationships bündeln diese Zugriffe zentral, und PIM for Groups sorgt dafür, dass die Rechte erst bei Bedarf aktiv werden. MSPs und MSSPs können dieselben Mechanismen für Kunden-Tenants nutzen, müssen aber den Konflikt mit bestehenden Partner-Center-Beziehungen sauber auflösen.

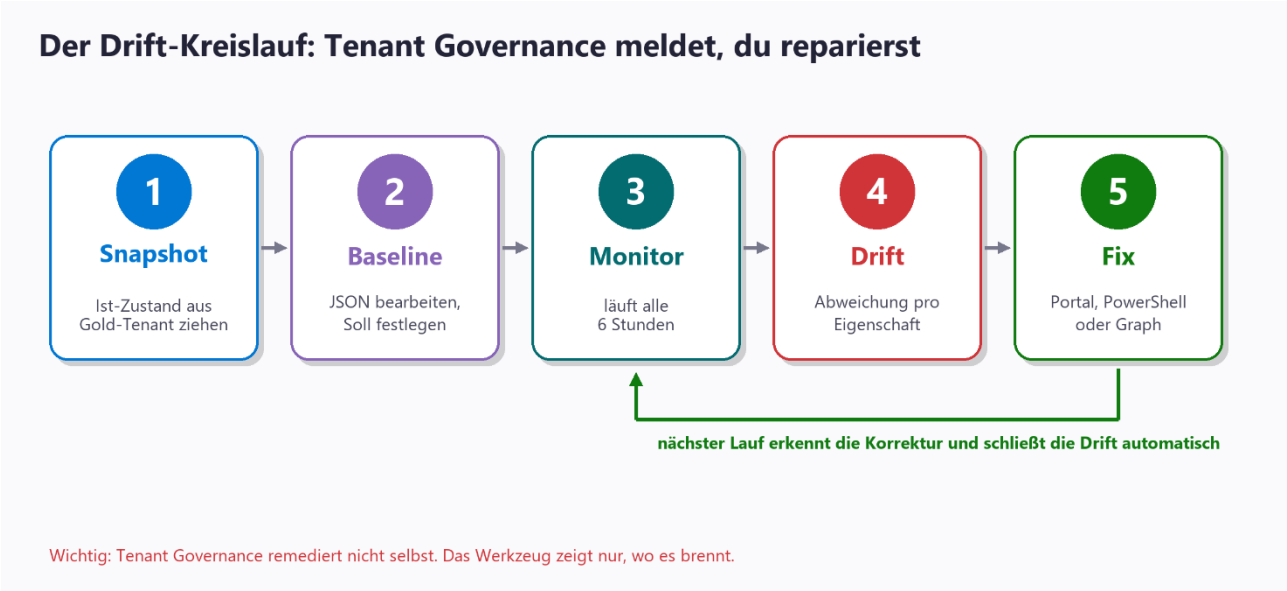

Abbildung 3: So läuft der Drift-Kreislauf im Betrieb

Das Risiko liegt weniger im Werkzeug als in der Erwartung. Tenant Governance repariert nichts. Es meldet. Wenn niemand die Drift-Meldungen liest, hast du ein sehr teures Alarmsystem ohne Feuerwehr. Und bei der Security-Administrator-Rolle ist die Gefahr noch banaler: Jemand hat die Rolle vor drei Jahren dauerhaft bekommen, weil er „nur Reports sehen" sollte. Ab Ende September kann genau dieses Konto nun auch Konten sperren und Passwörter zurücksetzen. Wird es kompromittiert, hat der Angreifer ein prima Werkzeug für Sabotage: Er sperrt deine Belegschaft aus, während du noch den Incident-Call organisierst. Ransomware-Gruppen lieben so etwas, weil es die Reaktion lähmt.

> **⚠ Warnung: Die Rolle wächst, dein Rollenkonzept nicht**
>
> Microsoft fragt dich nicht, ob deine bestehenden Security-Administrator-Zuweisungen die neuen Rechte bekommen sollen. Sie bekommen sie einfach.
>
> Wer die Rolle als „Lesezugriff mit Extras" verteilt hat, verteilt jetzt einen Sperrhebel für tausende Konten. Glückwunsch, du hast ein neues Tier-0-nahes Risiko, ohne einen einzigen Klick gemacht zu haben.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Nichts davon ist Raketenwissenschaft. Die schlechte: Es ist Fleißarbeit, und Fleißarbeit wird bekanntlich immer auf „nach dem Rollout" verschoben. Also bis zum Incident. Hier die Reihenfolge, die sich in Projekten bewährt hat:

Schritt	Was konkret	Wer
1. Rollen-Review	Alle aktiven und berechtigten Security-Administrator-Zuweisungen exportieren, begründen oder entfernen	IAM-Team, CISO
2. PIM erzwingen	Security Administrator nur noch eligible mit Freigabe, MFA und kurzer Aktivierungsdauer	IAM-Team

Schritt	Was konkret	Wer
3. SOC-Rolle schneiden	Analysten auf Entra SOC Identity Responder umstellen, bei Bedarf per AU begrenzen	SOC-Leitung
4. Audit-Alerts	Alarme auf Konto-Deaktivierungen und Passwort-Resets durch Security-Rollen einrichten	SOC, SIEM-Team
5. Discovery starten	Related Tenants auswerten, Billing-Signal zuerst, Owner je Tenant ermitteln	Cloud-Governance
6. Einfangen oder isolieren	Governance-Anfrage stellen, bei Ablehnung Quarantäne-Workflow nutzen	Cloud-Governance, Legal
7. Gold-Baseline	Snapshot aus Referenz-Tenant ziehen, zu JSON-Baseline veredeln, Monitor anlegen	Plattform-Team
8. Tenant-Erstellung	Standard-Governance-Vorlage definieren, Anlage nur noch über MCA-Weg	Cloud-Governance, Einkauf

✓ Tipp: Klein anfangen, dann skalieren

Starte die Baseline nicht mit „alles“. Nimm die zehn Conditional-Access-Richtlinien, Authentifizierungsmethoden und die Defender-Grundeinstellungen. Das passt locker in 200 Instanzen und liefert sofort Nutzen.

Definiere pro Ressource genau einen Soll-Zustand. Zwei Monitore mit widersprüchlichen Vorgaben erzeugen Dauer-Drift und irgendwann Alarmmüdigkeit.

Ein Praxisbeispiel zum Security-Administrator-Thema: Bei einem Handelsunternehmen hatten beim letzten Review 31 Konten die Rolle Security Administrator, davon 19 dauerhaft. Darunter zwei Servicekonten eines längst gekündigten Tools, ein Konto eines externen Beraters, dessen Vertrag 2024 auslief, und ein Shared Account namens „secadmin“, dessen Passwort auf einem Post-it im Serverraum klebte. Nach dem Review blieben vier Personen, alle nur eligible über PIM. Das SOC arbeitet seitdem mit SOC Identity Responder. Der Post-it wurde feierlich geschreddert, mit Protokoll.

⚠ Warnung: Sperren ist schnell, Entsperren ist Politik

Lege vor dem ersten Einsatz fest, wer ein vom SOC gesperrtes Konto wieder freigeben darf und nach welcher Prüfung. Sonst sperrt das SOC um 3 Uhr den Vertriebsvorstand, und um 8 Uhr diskutieren fünf Leute, wer schuld ist, während der Angreifer im Nachbarkonto weitermacht.

Und bei Tenant Governance: Rede früh mit Einkauf und Finanzen. Das Billing-Signal ist oft der schnellste Weg zu vergessenen Tenants, und Secure Tenant Creation hängt am Microsoft Customer Agreement. Wer noch mit alten Vertragsmodellen unterwegs ist, sollte das in die Planung einpreisen. Wichtig auch: Ein governed Tenant kann die Beziehung jederzeit selbst beenden. Das ist kein Kontrollverlust, sondern ein Signal, das du überwachen solltest, denn der governing Tenant bekommt dann eine Benachrichtigung.

Häufig gestellte Fragen

Welche Lizenz brauche ich für Microsoft Entra Tenant Governance?

Tenant Governance gibt es in einer kostenlosen Stufe sowie als Basic und Premium, wobei der governing Tenant eine Tenant-Governance-Lizenz benötigt. Höhere Limits für Monitore und Snapshots sind mit Entra ID Governance, Entra Suite oder Microsoft E7 verfügbar.

Behebt Entra Tenant Governance Konfigurations-Drift automatisch?

Nein, Tenant Governance erkennt und meldet Abweichungen von der JSON-Baseline nur. Die Korrektur erfolgt über das Admin Center, PowerShell oder Microsoft Graph, und der nächste Monitorlauf markiert die Drift dann automatisch als erledigt.

Kann der Security Administrator ab jetzt auch Global Administratoren sperren?

Nein, die neuen Aktionen Deaktivieren, Aktivieren, Sessions widerrufen und Passwort-Reset gelten nur für nicht privilegierte Konten. Für privilegierte Konten bleiben höher eingestufte Rollen wie Privileged Authentication Administrator zuständig.

Was ist der Unterschied zwischen Security Administrator und Entra SOC Identity Responder?

Security Administrator ist eine breite Konfigurationsrolle für Sicherheitsdienste, die jetzt zusätzlich Reaktionsrechte erhält. Entra SOC Identity Responder enthält nur die Containment-Aktionen gegen nicht privilegierte Konten, lässt sich auf Administrative Units beschränken und ist damit die bessere Wahl nach dem Least-Privilege-Prinzip.

Was mache ich, wenn ein entdeckter Tenant die Governance-Anfrage ablehnt?

Dann isolierst du ihn über den Quarantäne-Workflow für nicht genehmigte Tenants, der Nutzer und Apps dieses Tenants vom Zugriff auf deine Ressourcen aussperrt. Häufig hilft es auch, B2B-Zugriffe oder die Abrechnung über dein Konto zu stoppen, damit die Gegenseite ihre Haltung überdenkt.