SECURITY & COMPLIANCE

Defender: Neues RBAC-Berechtigungsmodell wird automatisch aktiviert (Prüfung bis 02.12.2026)

Executive Summary

Kurz und schmerzhaft: Du hast **28 Tage**. Laut Microsoft-Ankündigung MC1537494 wird das einheitliche Berechtigungsmodell Defender RBAC (bei Microsoft auch „Unified RBAC“ oder URBAC) zum einzigen Zugriffsmodell für alle Funktionen im Defender-Portal, Microsoft Sentinel eingeschlossen. Microsoft importiert deine bestehenden Rollen automatisch, zeigt im Portal einen Banner und schaltet das neue Modell rund 30 Tage später ohne weitere Rückfrage scharf. Microsoft nennt den 02.12.2026 als Termin, bis zu dem du die importierten Rollen geprüft haben solltest. Der Rollout der Banner beginnt Anfang Dezember und soll Ende Januar 2027 abgeschlossen sein, die Meldung läuft bis zum 02.03.2027.

Was freundlich als „erweiterte Möglichkeiten“ verpackt ist, ist in Wahrheit eine Abkündigung: Die bisherigen Einzelmodelle, also die Rollen von Defender for Endpoint, die Email-&-collaboration-Berechtigungen für Defender for Office 365, die MDI-Rollen, die lokalen Rollen von Defender for Cloud Apps und die Azure-Rollen für Sentinel im Defender-Portal, verlieren ihre Rolle als maßgebliche Rechtequelle. Nach der Aktivierung entscheidet nur noch Defender RBAC, wer im Portal was sehen und tun darf. Wer die Importliste nicht prüft, erfährt im Ernstfall um drei Uhr nachts, dass die Rufbereitschaft keine Geräte mehr isolieren kann. Das ist die Art Überraschung, auf die ein SOC gut verzichten kann.

Fakten: Das Wichtigste auf einen Blick

- **Was:** Defender RBAC wird für Defender- und Sentinel-Funktionen im Defender-Portal automatisch aktiviert, je Workload, rund 30 Tage nach dem Banner.
- **Termine:** Meldung seit 03.11.2026, Prüfung laut Microsoft bis 02.12.2026, Banner-Rollout Anfang Dezember bis Ende Januar 2027, Meldung endet am 02.03.2027.
- **Unverändert:** Purview, Exchange Online, Entra-Verzeichnisrollen, PIM und Azure RBAC für Azure-Ressourcen. PowerShell für Defender for Office 365 funktioniert weiter wie bisher.
- **Rückweg:** Nach der Aktivierung lässt sich jeder Workload über die Workload-Einstellungen sofort auf das alte Modell zurückschalten. Ein Opt-out vor der Aktivierung sieht die Meldung nicht vor.
- **Lizenz:** Keine Zusatzkosten. Für Defender for Office 365 gilt die Umstellung nur mit Plan 2, etwa über Microsoft 365 E5.

Worum geht es im Detail?

Zum Hintergrund: Das Defender-Portal ist über Jahre aus einzelnen Produkten zusammengewachsen, und jedes Produkt hat sein eigenes Rechtemodell mitgebracht wie ein Gast seine eigene Hausordnung. Defender for Endpoint kennt Rollen und Gerätegruppen, Defender for

Office 365 nutzt die Email-&-collaboration-Rollengruppen plus Exchange-Rollen, Defender for Identity hat MDI Admin, User und Viewer, Defender for Cloud Apps eigene lokale Administratoren, und Sentinel wird über Azure RBAC am Workspace gesteuert. Wer wissen wollte, wer im Haus einen Rechner isolieren oder eine Mail aus allen Postfächern löschen darf, brauchte fünf Browser-Tabs, viel Kaffee und eine gewisse Leidensfähigkeit.

Defender RBAC fasst das in ein Modell mit vier Berechtigungsgruppen zusammen: **Security operations** (Sicherheitsdaten, Alerts, Response, Live Response), **Security posture** (Schwachstellen, Exposure Management, Secure Score), **Authorization and settings** (Rollen verwalten, Sicherheits- und Systemeinstellungen) und **Data operations** für Sentinel-Daten. Jede Rollenzuweisung lässt sich zusätzlich einschränken: auf Gerätegruppen wie bisher, und neu auf Cloud-, Identity- und Sentinel-Scopes. Sentinel-Scopes sind laut Microsoft Learn eine echte zeilenbasierte Zugriffssteuerung: Datenzeilen werden bei der Aufnahme mit einem Scope-Tag versehen, bis zu 100 Scopes je Tenant sind möglich. Microsoft verkauft das Ganze außerdem als „zukunftssicher“, weil Zuweisungen künftige Berechtigungen und Workloads einschließen können, und als Voraussetzung für neue Angebote wie Perception. Übersetzt: Wer nicht mitzieht, bekommt die neuen Spielzeuge nicht.

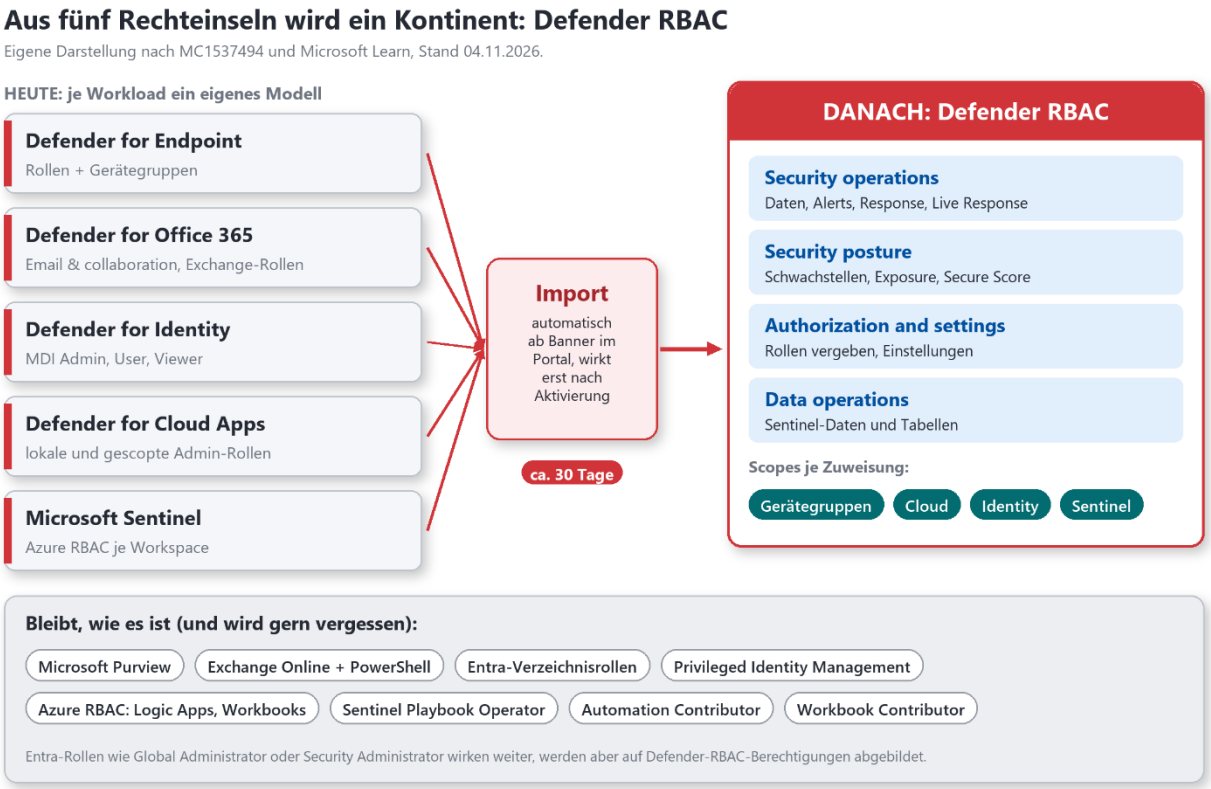


Abbildung 1: Die fünf bisherigen Rechtemodelle werden importiert und nach rund 30 Tagen durch Defender RBAC ersetzt. Purview, Exchange, Entra, PIM und Azure RBAC bleiben außen vor.

Neu ist dabei nicht das Modell selbst. Für neue Tenants von Defender for Endpoint und Defender for Identity ist Defender RBAC schon seit 2025 Standard, für neue Organisationen mit Defender for Office 365 Plan 2 seit Juli 2026. Wer sich bisher bewusst für das alte Modell entschieden hat oder schlicht nie umgeschaltet hat, wird jetzt umgezogen. Der Ablauf laut MC1537494: Zuerst erscheint im Defender-Portal auf der Seite für Berechtigungen und Rollen ein Banner, gleichzeitig importiert Microsoft die alten Rollen. Dieser Import hat noch keine operative Wirkung. Nach rund 30 Tagen wird der jeweilige Workload aktiviert, und ab dann gelten nur noch die neuen Rollen. Die Workloads und Termine je Tenant zeigt das Portal selbst an.

Die vollständige Zuordnung jeder Altrolle zu den neuen Berechtigungen findest du im Learn-Artikel Zuordnen von Berechtigungen in Microsoft Defender Unified RBAC, den Gesamtüberblick unter Microsoft Defender Unified RBAC.

Bereich	Bisher maßgeblich	Nach der Aktivierung
Defender for Endpoint	MDE-Rollen, Gerätegruppen	Defender RBAC, Gerätegruppen als Scope
Defender for Office 365 (P2)	Email & collaboration, Exchange-Rollen	Defender RBAC; Exchange-Rollen nur noch für Exchange und Purview
Defender for Identity	MDI Admin, User, Viewer	Defender RBAC, Identity-Scopes
Defender for Cloud Apps	lokale Admin-Rollen	Defender RBAC; vier gescopte Rollen entfallen
Sentinel im Defender-Portal	Azure RBAC je Workspace	Defender RBAC, Sentinel-Scopes; Sync zurück nach Azure
Entra-Rollen	Global Admin, Security Admin/Operator/Reader	wirken weiter, abgebildet auf RBAC-Rechte

Wichtig: Standardmäßig aktiv: was ohne dein Zutun passiert

Tust du nichts, aktiviert Microsoft Defender RBAC für die im Portal genannten Workloads automatisch, rund 30 Tage nach dem Banner. Ab dann zählen nur noch die importierten und von dir bearbeiteten Rollen. Steuern kannst du im Defender-Portal unter System, Berechtigungen, Microsoft Defender XDR, Rollen: Dort prüfst und änderst du die importierten Rollen, startest den Import bei Bedarf erneut und schaltest über „Workload settings“ einzelne Workloads selbst ein oder nach der Aktivierung wieder aus. Für Sentinel geht das je Workspace. Wer Rollen per Skript verwaltet, muss auf die Rollenverwaltung der Microsoft Graph API (derzeit Beta) umsteigen.

Was sind Chancen? Was sind Risiken?

Die Chance ist real: ein Ort, an dem du sehen kannst, wer was darf. Für jeden, der schon einmal eine ISO-27001-Auditorin durch fünf Rechtemodelle führen musste, ist das ungefähr so befreiend wie der Moment, in dem der letzte Fileserver ausgeschaltet wird. Dazu kommt echte Granularität: Live Response Basic für die erste Analyseebene, Advanced Live Response nur für die zweite. Ein Konzern mit Standorten in Deutschland und Spanien kann über Sentinel-Scopes dafür sorgen, dass das Team in Madrid die Logs aus Madrid sieht und nicht die Anmeldedaten der deutschen Personalabteilung. Für NIS2, KRITIS-Dachgesetz und BSI-Grundschutz (Baustein ORP.4, Identitäts- und Berechtigungsmanagement) ist ein zentrales, dokumentierbares Rechtemodell ein handfestes Argument.

Die Risiken stecken im Kleingedruckten des Imports, und zwar zuverlässig dort, wo niemand hinschaut. Erstens: Rollen, denen Konten oder Gruppen zugewiesen sind, die es in Entra ID nicht mehr gibt, landen in der Liste „Roles not eligible for import“. Sie werden schlicht nicht übernommen. Ein Maschinenbauer aus Ostwestfalen hatte genau so einen Fall in einer Testumgebung: Die MDE-Rolle für die Rufbereitschaft enthielt noch das Konto eines Werkstudenten, der vor anderthalb Jahren gegangen war. Folge: Die Rolle wurde nicht importiert, nach der Aktivierung konnte die Rufbereitschaft keine Geräte mehr isolieren. Der Werkstudent hat also noch lange nach seinem Abschied für Ausfälle gesorgt. Respekt.

> **Warnung: Verwaiste Konten sind tödlich für den Import**
>
> Ein einziges gelöschtes Konto in einer Altrolle blockiert den Import der ganzen Rolle. Prüfe die Liste der nicht importierbaren Rollen, entferne die Leichen im alten Modell und starte den Import neu. Achtung: Wer dieselbe Rolle zweimal importiert, erzeugt laut Microsoft Learn ein Duplikat. Also erst die alte Kopie löschen, dann neu importieren.

Zweitens: Für Defender for Office 365 importiert Microsoft nur Rollen und Rollengruppen, die mindestens einer Person aktiv zugewiesen sind. Und das Mapping fördert Dinge zutage, die vorher niemand sehen wollte. Die Rolle „Preview“ steckt standardmäßig in Purview-Rollengruppen wie eDiscovery Manager oder Data Investigator und wird auf „Email & collaboration content: All Emails (read)“ abgebildet, also Lesezugriff auf den Inhalt aller E-Mails. Das Recht war vorher auch schon da, nur versteckt. Jetzt steht es schwarz auf weiß in deiner Rollenliste, und der Datenschutzbeauftragte wird fragen, warum die Kollegin aus dem Rechtsbereich Mails der Geschäftsführung lesen darf.

Drittens Sentinel, das Lieblingsthema aller Infrastruktur-als-Code-Freunde. Nach der Aktivierung ist Defender RBAC die Rechtequelle, Zuweisungen werden nach Azure RBAC zurücksynchronisiert. Wer danach weiter per Terraform oder Bicep Rollen am Workspace setzt, riskiert laut Microsoft Learn Sync-Fehler. Service Principals lassen sich in Defender RBAC nicht berechtigen, und die Rollen Playbook Operator, Automation Contributor und Workbook Contributor bleiben in Azure. Pikant: Ein Global Administrator hat in Defender RBAC nicht automatisch Rechte auf Sentinel-Workspaces, er darf sie sich nur selbst geben. Und weil Sentinel im Defender-Portal zusätzlich weiterhin Azure-Rollen respektiert, sieht jemand mit üppigen Azure-Rechten unter Umständen mehr, als die schöne neue Rolle vermuten lässt. Least Privilege ist also erst erreicht, wenn auch Azure aufgeräumt ist.

Viertens Defender for Cloud Apps: Mit der Aktivierung entfallen die gescopten Rollen App/instance admin, User group admin, Cloud Discovery global admin und Cloud Discovery report admin. Ersatz gibt es nur über eigene Rollen in Defender RBAC. Das ist die eigentliche Abkündigung in dieser Meldung, und sie steht dort nicht einmal drin.

Thema	Chance	Risiko
Ein Rechtemodell	Ein Ort für Audit und Rezertifizierung	Importlücken bei verwaisten Konten
Neue Scopes	Standort- oder Teamtrennung, auch in Sentinel	Falsch gesetzte Scopes blenden Alarme aus
Automatischer Import	Kein Neubau nötig, Mapping vorgegeben	Breite Altrechte wandern ungeprüft mit
Sentinel in RBAC	Zeilenbasierte Rechte, Sync nach Azure	IaC-Konflikte, keine Service Principals
Opt-out nach Aktivierung	Schneller Rückweg im Störfall	Verleitet zum Aussitzen statt Aufräumen

Was müssen wir jetzt schon vorbereiten?

Meine klare Empfehlung: Warte nicht, bis Microsoft den Schalter umlegt. Aktiviere Defender RBAC selbst, Workload für Workload, in einem Wartungsfenster deiner Wahl, mit Testkonten je Rolle und dem SOC am Telefon. Das Opt-out nach der Aktivierung ist dein Notausgang, nicht dein

Plan. Microsoft nennt kein Datum, bis zu dem dieser Notausgang offen bleibt, und die Richtung ist eindeutig: Das alte Modell ist ein Auslaufmodell, das Ende ist nur noch nicht datiert. Wer jetzt zurückschaltet, schiebt dieselbe Arbeit in ein Quartal, in dem garantiert noch weniger Zeit ist.

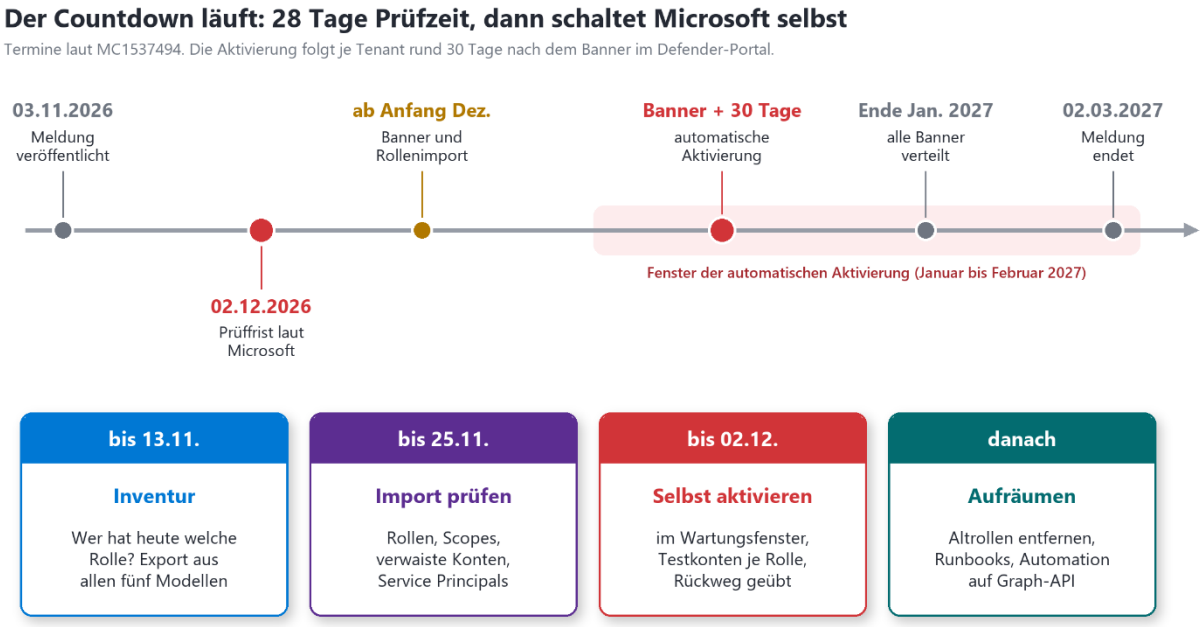


Abbildung 2: Die Prüffrist endet am 02.12.2026, die automatische Aktivierung folgt je Tenant rund 30 Tage nach dem Banner. Wer bis Anfang Dezember selbst umgestellt hat, bestimmt den Zeitpunkt.

Wann	Was	Wer
Bis 13.11.2026	Inventur aller Altrechte: MDE-Rollen und Gerätegruppen, Email-&-collaboration-Rollengruppen, Exchange-Rollen mit Schutzbezug, MDI- und Cloud-Apps-Rollen, Azure-Rollen am Sentinel-Workspace. Skripte und Pipelines finden, die Rollen per API oder IaC setzen.	Security-Administrator, Azure-Team
Bis 20.11.2026	Betriebs- oder Personalrat und Datenschutz informieren: geänderte Rollennamen, neue Scopes, sichtbar gewordene Leserechte auf E-Mail-Inhalte. Anlage „Rollen- und Berechtigungskonzept“ der Betriebs- oder Dienstvereinbarung aktualisieren.	IT-Leitung, Datenschutz
Bis 25.11.2026	Import prüfen oder selbst anstoßen, nicht importierbare Rollen bereinigen, jede Zuweisung gegen die Inventur abgleichen, Rechte auf Least Privilege zuschneiden, Gruppen statt Einzelkonten.	Security-Administrator
Bis 02.12.2026	Selbst aktivieren, Workload für Workload; je Rolle ein Testkonto anmelden lassen; Rückweg über Workload-Einstellungen einmal durchspielen.	Security-Administrator, SOC
Ab Aktivierung	Rollenänderungen nur noch im Defender-Portal, IaC auf Graph-API umstellen, Runbooks und Notfallhandbuch anpassen, Altrollen nach vier Wochen ohne Störung entfernen.	Security-Team, Azure-Team

Tipp: Notfallkonto nicht vergessen

Lege eine eigene Defender-RBAC-Rolle mit der Berechtigung „Authorization“ für eine kleine, über PIM geschützte Gruppe an. Dann musst du für Rollenänderungen im Defender-Portal nicht jedes Mal den Security Administrator in Entra aktivieren, und im Ernstfall kann trotzdem jemand Rechte reparieren, ohne dass der Global Administrator aus dem Tresor geholt werden muss.

Zu Mitbestimmung und Datenschutz: Die Umstellung selbst ändert nichts an dem, was Defender über die Belegschaft erfasst. Aber in vielen Betriebsvereinbarungen zu Microsoft 365 oder zu Defender ist als Anlage festgelegt, welche Rollen welche Daten sehen dürfen. Wenn sich Rollennamen, Rechtezuschnitt und Scopes ändern, stimmt diese Anlage nicht mehr. Nach § 87 Abs. 1 Nr. 6 BetrVG beziehungsweise dem jeweiligen Personalvertretungsrecht ist das kein neues Mitbestimmungsverfahren, aber eine Informationspflicht, die du ernst nehmen solltest. Für den Datenschutz gilt Art. 32 DSGVO: Ein dokumentiertes, geprüftes Berechtigungskonzept ist eine technische und organisatorische Maßnahme, ein ungeprüfter Automatikimport ist es nicht.

Zur Kommunikation: Die Belegschaft merkt von der Umstellung nichts, Anwenderinnen und Anwender melden sich nicht im Defender-Portal an. Informieren musst du nur die, die es tun: SOC, Rufbereitschaft, externe Dienstleister mit GDAP-Zugriff. Für Letztere bleibt laut MC1537494 die delegierte Verwaltung unverändert, ihre Zuweisungen werden mit importiert. Lass dir trotzdem vom Dienstleister schriftlich bestätigen, dass er nach der Aktivierung noch alles kann, was im Vertrag steht. Sonst stellt ihr das gemeinsam beim nächsten Ransomware-Fall fest, und dann ist die Stimmung erfahrungsgemäß eher gedrückt.

Warnung: Nicht vergessen: Was nicht umzieht

Purview-Funktionen wie DLP und Insider Risk Management bleiben bei den Purview-Rollen, auch wenn sie im Defender-Portal auftauchen. Exchange-Rollen steuern weiter Exchange Online und Purview, werden aber für die Defender-for-Office-365-Oberfläche nicht mehr gebraucht. Wer sie nur dafür vergeben hatte, sollte sie nach der Aktivierung entziehen. Sonst hast du am Ende zwei Rechtemodelle statt einem, und das Ganze war nur ein besonders aufwendiger Umweg zum alten Chaos.

Weiterlesen › Erweiterte Security-Administrator-Rolle in Entra für schnellere Incident-Response

Weiterlesen › NIS2: Defender XDR wird zum zentralen Audit-Werkzeug

Häufig gestellte Fragen

Kann ich die automatische Aktivierung von Defender Unified RBAC verhindern?

Ein Opt-out vor der Aktivierung sieht Microsoft laut MC1537494 nicht vor. Nach der Aktivierung kannst du einzelne Workloads im Defender-Portal unter System, Berechtigungen, Rollen über die Workload-Einstellungen sofort auf das alte Rechtemodell zurückschalten.

Verlieren Global Administrator und Security Administrator nach der Umstellung den Zugriff auf das Defender-Portal?

Nein, die Entra-Rollen Global Administrator, Security Administrator, Security Operator und Security Reader wirken weiter und werden auf Defender-RBAC-Berechtigungen abgebildet. Für Sentinel-Workspaces erhält ein Global Administrator in Defender RBAC allerdings keine automatischen Rechte, er darf sie sich nur selbst zuweisen.

Warum wurde eine meiner Defender-Rollen nicht importiert?

Meist enthält die Rolle Konten oder Gruppen, die in Entra ID nicht mehr existieren, dann erscheint sie unter den nicht importierbaren Rollen. Entferne die verwaisten Zuweisungen im alten Modell und starte den Import erneut; bei Defender for Office 365 werden außerdem nur aktiv zugewiesene Rollen übernommen.

Funktionieren meine PowerShell-Skripte für Defender for Office 365 nach der Umstellung weiter?

Ja, Exchange Online PowerShell und Security & Compliance PowerShell nutzen weiterhin die Exchange- und Email-&-collaboration-Rollen. Nur wer Rollen und Berechtigungen per API konfiguriert, muss auf die Rollenverwaltung der Microsoft Graph API umstellen.

Kostet Defender Unified RBAC zusätzliche Lizenzen?

Nein, Defender RBAC ist ohne Aufpreis Teil der jeweiligen Defender-Lizenzen. Für Defender for Office 365 gilt die Umstellung nur bei Plan 2, etwa über Microsoft 365 E5 oder eine separate Plan-2-Lizenz.