

Defender for Cloud Apps im Mittelstand

Es gibt eine Sorte Lizenzgespräch, die immer gleich abläuft. Jemand hat Microsoft 365 E5 gekauft, weil das Paket rechnerisch günstiger war als die Einzelteile, und irgendwann fällt auf, dass darin noch etwas namens Defender for Cloud Apps liegt. Ungenutzt. Seit zwei Jahren. Wie ein Fitnessvertrag, den man aus Prinzip weiterzahlt.

Dann wird das Ding eingeschaltet, und drei Tage später steht in einem Report, dass in deinem Unternehmen 600 Cloud-Apps im Einsatz sind. Sechshundert. Bei 200 Nutzern. Der Geschäftsführer bekommt große Augen, die IT bekommt Blutdruck, und niemand merkt, dass davon 480 Einträge Werbenetzwerke, Schriftarten-Hoster und Update-Server sind, die nie ein Mensch bewusst aufgerufen hat.

Defender for Cloud Apps ist ein gutes Werkzeug. Es ist auch ein Werkzeug, das für Konzerne mit 40.000 Mitarbeiterinnen und Mitarbeitern und einem Security-Operations-Team gebaut wurde. Wenn du 200 Nutzer hast und die IT aus zweieinhalb Personen besteht, von denen eine hauptsächlich Drucker repariert, dann brauchst du eine ehrliche Einordnung: Was davon zahlt sich aus, was ist netter Beifang, und was ist schlicht Beschäftigungstherapie mit Enterprise-Anstrich.

Genau das liefert dieser Beitrag. Er gehört zur Serie [Microsoft 365 Security](#) und behandelt Handlungsfeld B: Cloud Discovery über Defender for Endpoint, den Schatten-IT-Report, App-Governance für OAuth-Apps, Sitzungsrichtlinien mit Conditional Access App Control und die Anomalie-Erkennung. Am Ende steht eine Empfehlung, die du nicht auf jeder Herstellerfolie findest: Zwei dieser fünf Bausteine solltest du bei 200 Nutzern bewusst liegen lassen.

FAKTEN · Was hinter dem Produktnamen steckt

Defender for Cloud Apps ist Microsofts CASB – Cloud Access Security Broker. Der Cloud-App-Katalog umfasst **über 31.000 Cloud-Apps**, die anhand von **über 90 Risikofaktoren** bewertet werden. Discovery-Daten werden viermal täglich neu analysiert. Das Produkt ist Bestandteil von Microsoft Defender XDR und wird im Defender-Portal unter "Cloud Apps" bedient – eine eigene Portaladresse gibt es seit dem Zusammenzug der Konsolen nicht mehr.

Erst die Lizenz, dann die Begeisterung

Bevor du irgendetwas einschaltest: Prüfe, ob du es überhaupt darfst. Diese Reihenfolge klingt banal, wird aber regelmäßig umgedreht, und dann steht am Ende des Proof of Concept die Frage, warum die Hälfte der Menüpunkte grau ist.

Die Lizenzlage, unbeschönigt

Defender for Cloud Apps ist kein Bestandteil von Microsoft 365 Business Premium. Das ist der Punkt, an dem die meisten mittelständischen Planungen kippen, denn Business Premium ist im Segment bis 300 Nutzer das mit Abstand beliebteste Paket. Business Premium enthält Defender for Business – also die Endpunkt-Seite, die für die Discovery-Signale gebraucht wird – aber nicht den CASB selbst. Du kannst die Lücke mit einer Zusatzlizenz schließen, das funktioniert sauber, kostet aber eben extra.

Lizenz	Cloud Discovery	Anomalie-Erkennung	OAuth-Governance	Sitzungsrichtlinien
Microsoft 365 Business	nein (nur mit	nein	nein	nein

Premium	Zusatzlizenz)			
Microsoft 365 E3 / EMS E3 / Entra ID P1	ja, als "Cloud App Discovery"	nein	nein	nein
Microsoft 365 E5 / E5 Security	voll	voll	voll	voll
EMS E5	voll	voll	voll	voll
Defender for Cloud Apps eigenständig	voll	voll	voll	voll

Die zweite Zeile verdient einen zweiten Blick. In Microsoft 365 E3, EMS E3 und Entra ID P1 steckt ohne Aufpreis "Cloud App Discovery" – eine echte Teilmenge von Defender for Cloud Apps. Du bekommst denselben Katalog mit über 31.000 Apps, dieselbe Risikobewertung, dieselben Nutzungsauswertungen pro App, Benutzer und IP-Adresse, und du darfst eigene Discovery-Richtlinien anlegen. Was fehlt: die Anomalie-Erkennung für entdeckte Apps, die OAuth-Verwaltung samt Widerruf, die Sitzungsrichtlinien, die Aktivitätsrichtlinien und der SIEM-Konnektor.

TIPP · Der günstigste sinnvolle Einstieg

Wenn du E3 hast und über E5 nachdenkst: Fang mit Cloud App Discovery an. Du siehst deine Schatten-IT vollständig, ohne einen Cent mehr auszugeben. Wenn der Report nach vier Wochen zeigt, dass niemand außerhalb der genehmigten Werkzeuge arbeitet, hast du ein Argument gegen das Upgrade. Zeigt er drei unbekannte Dateiablagen mit Gigabyte-Uploads, hast du eines dafür. Beides ist mehr wert als eine Bauchentscheidung. Wie du solche Entscheidungen sauber priorisierst, steht im Beitrag [Secure Score: sinnvoll nutzen statt Punktejagd](#).

Zwei Termine, die du im Kalender haben solltest

Das Produkt bewegt sich. Zwei Änderungen betreffen dich direkt, wenn du jetzt einsteigst. Erstens: Die Dateirichtlinien von Defender for Cloud Apps werden zum 6. Januar 2027 eingestellt. Dateibasierter Datenschutz wandert vollständig zu Microsoft Purview. Wenn dir also jemand empfiehlt, Inhaltsprüfungen über MDCA-Dateirichtlinien zu bauen, ist das eine Investition mit Ablaufdatum. Baue das gleich als Purview-DLP oder als automatische Klassifizierung.

Das ist kein Detail am Rand: Wer heute Dateirichtlinien aufsetzt, migriert sie in gut einem Jahr wieder. Der [Kompetenzbereich Microsoft Purview](#) zeigt, wo diese Funktionen künftig leben. Zweitens ist seit August 2026 die einheitliche rollenbasierte Zugriffssteuerung von Microsoft Defender für neue Kunden standardmäßig aktiv. Für dich heißt das: Berechtigungen vergibst du zentral im Defender-Portal, nicht mehr in einer produktspezifischen Nische. Bestehende Tenants aktivieren das manuell.

WARNUNG · Der Klassiker beim Rollenmodell

Die Rolle "Cloud App Security Administrator" darf App-Governance **einschalten**, aber danach nichts darin sehen oder verwalten. Wer die Funktion betreiben soll, braucht zusätzlich Sicherheitsadministrator, Sicherheitsoperator oder Sicherheitsleseberechtigung. Das kostet erfahrungsgemäß eine halbe Stunde Ratlosigkeit, wenn man es nicht vorher weiß.

Cloud Discovery über Defender for Endpoint

Es gibt drei Wege, an Discovery-Daten zu kommen: manuelle Log-Uploads aus der Firewall, ein Log-Collector als Docker-Container, der Syslog oder FTP entgegennimmt, und die eingebaute Integration mit Defender for Endpoint. Für den Mittelstand ist der dritte Weg der einzige, der auf Dauer funktioniert. Die anderen beiden erwähne ich nur, damit du weißt, warum du sie nicht nimmst.

Warum Log-Collector und Firewall-Export im Mittelstand scheitern

Der manuelle Upload liefert eine Momentaufnahme. Du exportierst einen Wochenlog aus der Firewall, lädst ihn hoch, bekommst einen Bericht. Beim ersten Mal ist das spannend. Beim vierten Mal macht es niemand mehr, weil derjenige, der es macht, krank ist, gekündigt hat oder inzwischen weiß, dass der Bericht ohnehin dasselbe sagt wie letztes Mal.

Der Log-Collector automatisiert das, verlangt aber einen Docker-Host, eine Syslog-Konfiguration auf dem Netzwerkgerät, Zertifikatspflege und die Beobachtung eines weiteren Dienstes, der still ausfallen kann. Vor allem aber hat er ein konzeptionelles Problem: Er sieht nur Traffic, der durch dein Netzwerk läuft. Seit dem Homeoffice ist das ein Bruchteil. Und Firewall-Logs kennen keinen Gerätekontext – du siehst, dass eine IP-Adresse etwas getan hat, nicht welches Notebook.

Die Integration mit Defender for Endpoint löst beide Probleme in einem Schritt. Der Sensor sitzt auf dem Endgerät und meldet Netzwerkaktivität mit Benutzer- und Gerätekontext, unabhängig davon, ob das Gerät im Büro, im Zug oder am Küchentisch steht. Kein Routing, kein Spiegelport, kein zusätzlicher Server.

Datenfluss Cloud Discovery über Defender for Endpoint

Hinweg: vom Endgerät zum Schatten-IT-Report



Rückweg: von der Entscheidung zur Blockade



Was hier fehlt und niemand vermisst: Log-Collector, Syslog-Export, Firewall-Regelpflege, wöchentliche CSV-Uploads.

Skizze 1: Datenfluss der Cloud Discovery – Hinweg vom Endgerät zum Report, Rückweg von der Entscheidung zur Blockade auf demselben Gerät.

Voraussetzungen und der eine Schalter

Die Anforderungsliste ist überschaubar und in fast jedem halbwegs gepflegten Tenant bereits erfüllt.

Voraussetzung	Details	Typischer Stolperstein
Lizenz Defender for Cloud Apps	eigenständig oder in E5 / EMS E5	Business Premium reicht nicht

Endpunktschutz	Defender for Endpoint Plan 2 oder Defender for Business	Plan 1 genügt nicht
Geräte onboarded	Windows 10 ab Version 1709 mit aktuellem Patchstand, Windows 11	unmanaged Geräte liefern gar nichts
macOS	Defender-for-Endpoint-Version 20.123072.25.0 oder neuer	Netzwerkschutz muss aktiv sein, UDP wird nicht erfasst
Defender Antivirus	Echtzeitschutz, Cloudschutz, Netzwerkschutz im Blockmodus	empfohlen, nicht zwingend – ohne ihn sind die Daten dünner

Eingeschaltet wird das im Defender-Portal unter Einstellungen > Endpunkte > Allgemein > Erweiterte Features, mit einem Schalter namens "Microsoft Defender for Cloud Apps". Danach dauert es bis zu zwei Stunden, bis die ersten Daten auftauchen. Wenn deine Geräte noch gar nicht angebunden sind, ist das der vorgelagerte Schritt – [Defender for Endpoint: Onboarding ohne Drama](#) beschreibt ihn im Detail.

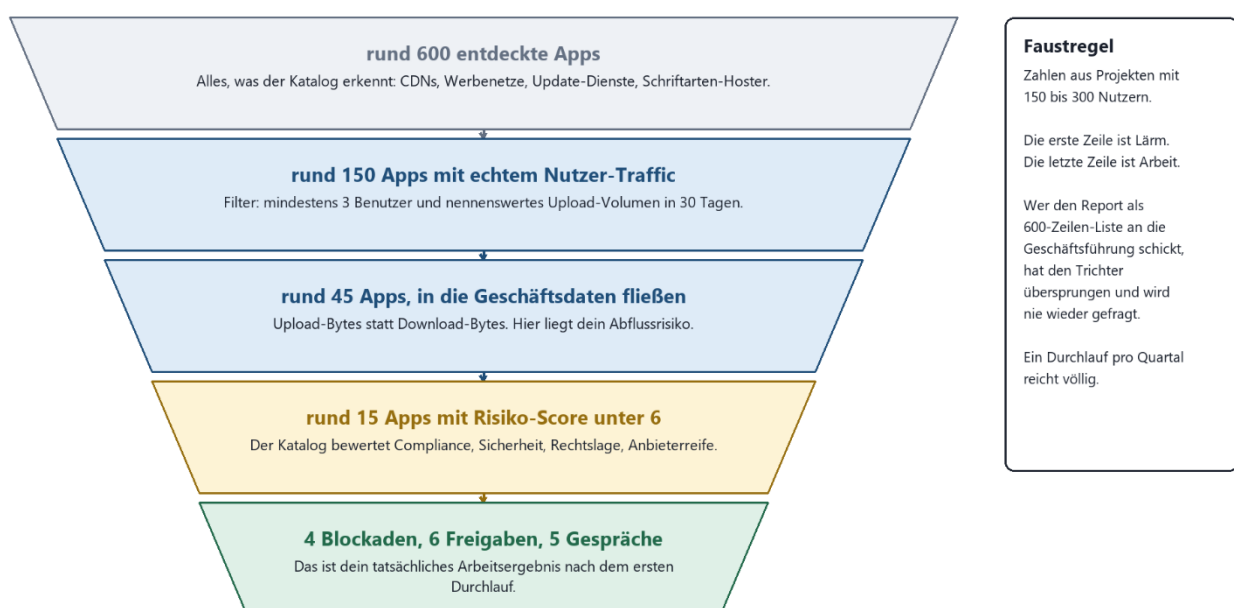
WARNUNG · Bevor du den Schalter umlegst: Mitbestimmung klären

Cloud Discovery über Defender for Endpoint erzeugt eine Datenbasis, aus der hervorgeht, welcher benannte Mensch von welchem Gerät aus welchen Dienst aufgerufen hat. Das ist in Deutschland eine Verhaltens- und Leistungskontrolle im Sinne des Betriebsverfassungsgesetzes, und zwar unabhängig davon, ob du sie so nutzen willst. Defender for Cloud Apps kann Benutzernamen in Discovery-Berichten anonymisieren – nutze das, solange keine Vereinbarung steht. Wie du das Gespräch führst, ohne dass es eskaliert, steht in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Der Schatten-IT-Report und was du wirklich damit machst

Jetzt kommt der Teil, an dem die meisten Projekte einschlafen. Der Report ist da, er ist beeindruckend lang, und dann passiert nichts, weil niemand weiß, wo er anfangen soll. Die Antwort ist ein Trichter, und der wichtigste Schritt ist der erste: aggressiv filtern.

Vom Schatten-IT-Report zur Entscheidung: der Trichter



Skizze 2: Vom Rohbericht zur Entscheidung – realistische Größenordnungen aus Projekten mit 150 bis 300 Nutzern.

Die Reihenfolge der Filter ist nicht beliebig. Sortiere zuerst nach hochgeladenen Bytes, nicht nach Zugriffszahlen. Ein Dienst, den 80 Leute einmal im Monat lesend aufrufen, ist harmlos. Ein Dienst, in den drei Leute täglich Daten schieben, ist deine Baustelle. Danach schau auf den Risiko-Score, aber behandle ihn als Gesprächseinstieg, nicht als Urteil – der Score bewertet Anbietereigenschaften wie Zertifizierungen, Datenhaltung und Rechtslage, nicht deine konkrete Nutzung.

Für jede App, die durch den Trichter fällt, triffst du genau eine von drei Entscheidungen. Und nur eine davon hat technische Folgen.

Status	Was er bewirkt	Wann du ihn setzt
Sanktioniert	reine Dokumentation, kein technischer Effekt	der Dienst ist genehmigt, es gibt einen Vertrag, jemand ist zuständig
Geduldet (kein Status)	nichts – die App bleibt sichtbar und erlaubt	geschäftlich irrelevant oder unklar, kein Handlungsdruck
Nicht sanktioniert	Domänen werden als Custom-URL-Indikatoren nach Defender for Endpoint übertragen, Netzwerkschutz blockiert	der Dienst ist ein echtes Risiko und du hast eine Alternative anzubieten

Die Blockade ist bemerkenswert unaufwendig. Du markierst eine App als "nicht sanktioniert", die zugehörigen Domänen werden meist binnen weniger Minuten nach Defender for Endpoint synchronisiert, und der Netzwerkschutz auf dem Endgerät zeigt dem Nutzer eine Blockmeldung. Es gibt keine Firewall-Regel zu pflegen und keinen Proxy zu konfigurieren. Seit Mai 2026 lässt sich außerdem der informative Alarm abschalten, den jeder Blockversuch erzeugt – ein Schalter, den du am zweiten Tag suchen wirst, wenn du einen populären Dienst gesperrt hast.

WICHTIG · Blockieren ohne Ersatzangebot ist Sabotage

Wenn du den privaten Dateiaustauschdienst sperrst, mit dem die Vertriebsabteilung seit vier Jahren 300-Megabyte-Angebote an Kunden schickt, dann sperrst du nicht Schatten-IT. Du sperrst einen Geschäftsprozess. Die Abteilung wird binnen einer Woche einen Weg drumherum finden, und der wird schlechter sein als der vorherige. Kläre vorher, was stattdessen gilt: eine SharePoint-Freigabe, ein Gastzugang, ein Link mit Ablaufdatum. Der Beitrag [Gastzugriff und externe Freigaben härten](#) zeigt, wie das sauber geht.

App-Governance: der OAuth-Bestand, den niemand kennt

Wenn ich in einem mittelständischen Tenant genau eine Sache anschauen dürfte, wäre es die Liste der OAuth-Anwendungen. Nicht weil sie besonders spannend ist, sondern weil sie zuverlässig Dinge enthält, von denen niemand im Haus etwas weiß. Ein Kalender-Synchronisierer, den jemand 2021 für ein Projekt zugelassen hat. Ein Newsletter-Werkzeug einer Agentur, die seit zwei Jahren nicht mehr für euch arbeitet. Eine KI-Notizhilfe, die sich Zugriff auf alle Teams-Besprechungen geholt hat, weil das Häkchen so freundlich formuliert war.

Warum OAuth-Missbrauch die unangenehmste Angriffsform ist

Der klassische Phishing-Angriff stiehlt ein Passwort. Dagegen hilft MFA, und dagegen hilft ein Passwortwechsel. Der Consent-Angriff stiehlt kein Passwort. Er bringt den Benutzer dazu, einer Anwendung Berechtigungen zu erteilen – auf einer echten Microsoft-Anmeldeseite, mit korrektem Zertifikat, ohne jede Fälschung. Was der Angreifer danach hat, ist ein legitim ausgestelltes Token, das sich selbst erneuert und mit dem Passwort nichts zu tun hat.

Die OAuth-Consent-Kette – warum ein Passwortwechsel nicht hilft



Skizze 3: Ablauf eines Consent-Angriffs. Der Passwortwechsel am Ende ändert nichts, weil nie ein Passwort im Spiel war.

Die vorbeugende Seite dieses Themas – wer im Tenant überhaupt zustimmen darf, wie der Administratoren-Genehmigungsworkflow aussieht und welche Berechtigungen du grundsätzlich nie freigeben solltest – ist ausführlich in [App-Registrierungen und Consent-Governance](#) beschrieben. Hier geht es um die andere Hälfte: um Erkennung und Aufräumen im laufenden Betrieb.

Was App-Governance dir zeigt

App-Governance ist der Teil von Defender for Cloud Apps, der sich um OAuth-fähige Anwendungen kümmert, die in Entra ID registriert sind – seit den Erweiterungen vom Juni 2026 zusätzlich auch um Salesforce Connected Apps und External Client Apps. Du schaltest es im Defender-Portal unter Einstellungen > Cloud Apps > App-Governance ein. Danach dauert es bis zu zehn Stunden, bis die Funktion nutzbar ist. Die Region deiner Rechnungsadresse spielt eine Rolle: Einige Länder sind noch ausgenommen, Deutschland gehört nicht dazu.

Signal	Was es bedeutet	Deine typische Reaktion
Hochprivilegierte App	die App hat mehr Berechtigungen, als sie tatsächlich nutzt	Berechtigungen kürzen oder App ersetzen
Ungenutzte App	seit längerer Zeit keine Aktivität, Zustimmung besteht aber fort	Zustimmung widerrufen – der schnellste Sicherheitsgewinn überhaupt
Neue App mit vielen Zustimmungen in kurzer Zeit	klassisches Muster einer Consent-Phishing-Welle	sofort deaktivieren, dann untersuchen
Verdächtige Downloadaktivität einer OAuth-App	die App lädt untypisch viele Dateien aus SharePoint oder OneDrive	als Vorfall behandeln, Token widerrufen
Aktivität von unbekanntem Anbieter	die App verbindet sich aus einem ungewöhnlichen Netz	prüfen, ob der Hersteller den Betrieb verlagert hat

Das Signal "ungenutzte App" ist seit Dezember 2025 für nahezu alle kommerziellen Kunden verfügbar und unterschätzt. Jede zugestimmte Anwendung, die seit einem halben Jahr nichts tut,

ist ein offenstehendes Fenster ohne Nutzen. Der Widerruf kostet dich einen Klick und erzeugt keine Diskussion, weil niemand vermisst, was niemand benutzt. Ich habe noch kein Projekt erlebt, in dem dieser Durchgang weniger als ein Dutzend Einträge ergeben hätte.

TIPP · Verbinde den Microsoft-365-Konnektor

App-Governance zeigt deutlich mehr, wenn zusätzlich der Microsoft-365-Konnektor eingerichtet ist. Erst dann siehst du in der erweiterten Suche, welche konkreten Ressourcen eine OAuth-App tatsächlich angefasst hat. Ohne den Konnektor weißt du, dass eine App Berechtigungen hat; mit ihm weißt du, was sie damit gemacht hat. Für die Untersuchung eines Vorfalls ist das der Unterschied zwischen Vermutung und Beweis – siehe auch [Kompromittiertes Konto erkennen und aufräumen](#).

WICHTIG · Die Reihenfolge im Ernstfall

App im Portal deaktivieren, dann Token und Sitzungen widerrufen, dann Postfachregeln und Weiterleitungen prüfen, dann erst das Passwort zurücksetzen. Wer mit dem Passwort anfängt, verschafft dem Angreifer nur Zeit. Der komplette Ablauf steht in [Incident-Response-Plan für Microsoft 365](#).

Sitzungsrichtlinien mit Conditional Access App Control

Und jetzt der Teil, bei dem ich dir vermutlich die Vorfriede verderbe. Conditional Access App Control ist technisch die eleganteste Funktion im ganzen Produkt. Sie ist auch die, die du bei 200 Nutzern mit hoher Wahrscheinlichkeit nicht brauchst.

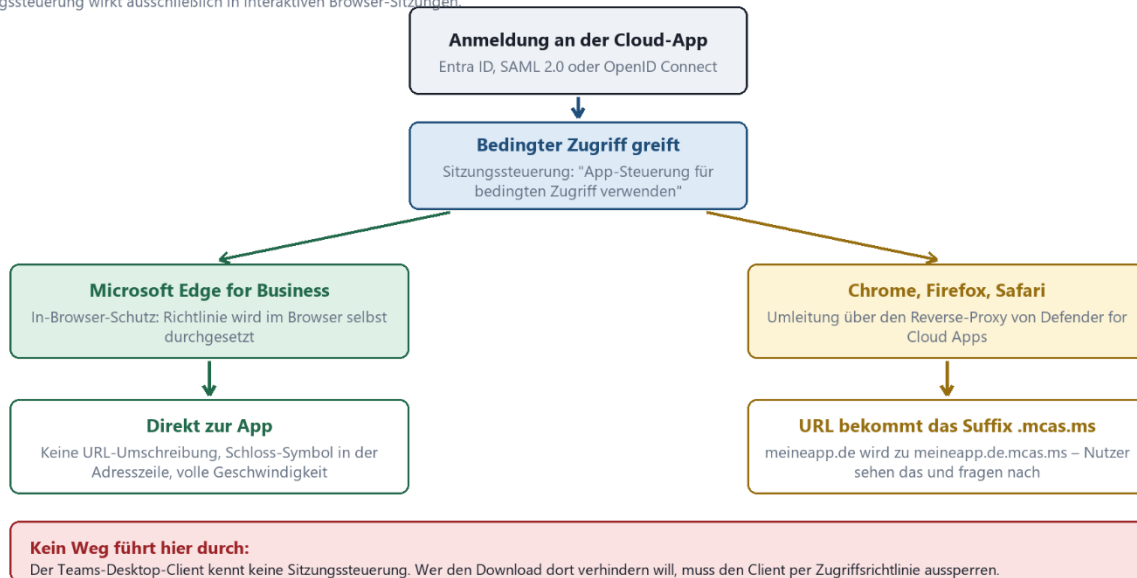
Wie es funktioniert

Der bedingte Zugriff in Entra ID kann eine Anmeldung nicht nur erlauben oder verweigern, sondern auch mit einer Sitzungssteuerung versehen. Die reicht die Sitzung an Defender for Cloud Apps weiter, und dort greifen Zugriffs- und Sitzungsrichtlinien: Download blockieren, Ausschneiden und Kopieren unterbinden, Drucken verhindern, Upload unklassifizierter Dateien stoppen, beim Herunterladen automatisch ein Vertraulichkeitslabel setzen, bei einer heiklen Aktion mitten in der Sitzung erneut eine mehrstufige Authentifizierung verlangen.

Der Weg dorthin unterscheidet sich je nach Browser. Microsoft Edge for Business setzt die Richtlinie direkt im Browser durch – erkennbar an einem Schloss-Symbol in der Adresszeile. Alle anderen Browser werden über einen Reverse-Proxy umgeleitet, und dabei bekommt die Adresse ein Suffix: Aus der App-Adresse wird die App-Adresse mit angehängtem .mcas.ms. Das funktioniert, aber es fällt auf.

Conditional Access App Control: zwei Wege in dieselbe Sitzung

Sitzungssteuerung wirkt ausschließlich in interaktiven Browser-Sitzungen.



Skizze 4: Zwei Wege durch Conditional Access App Control – In-Browser-Schutz mit Edge, Reverse-Proxy für alle anderen.

Die Grenzen, die selten auf der Folie stehen

Sitzungssteuerung wirkt ausschließlich in interaktiven Browser-Sitzungen. Das ist keine Feinheit, sondern die zentrale Einschränkung. Der Teams-Desktop-Client wird nicht unterstützt – wenn du dort den Download verhindern willst, musst du den Desktop-Client per Zugriffsrichtlinie komplett aussperren und die Leute in den Browser zwingen. Das ist eine Ansage, die du der Belegschaft erklären musst, und zwar mehrfach.

Dazu kommt: Wer den Schutz umgehen will, nimmt einfach die App als Desktop-Anwendung. Deshalb empfiehlt Microsoft ausdrücklich, native Clients per Zugriffsrichtlinie zu blockieren, wenn man auf Sitzungssteuerung setzt. Das ist konsequent, aber es bedeutet, dass du für ein einzelnes Kontrollziel gleich zwei Richtlinien betreibst und eine Client-Landschaft beschneidest.

WARNUNG · Das Support-Ticket, das du vermeiden willst

Wenn eine Anwendung über den Reverse-Proxy läuft und sich unerwartet verhält – eine Schaltfläche reagiert nicht, ein Download bricht ab, ein eingebettetes Fenster bleibt leer – dann diskutierst du das mit dem Hersteller der Anwendung, der die Adresse mit dem .mcas.ms-Suffix noch nie gesehen hat. Rechne diesen Aufwand ein, bevor du eine geschäftskritische Fachanwendung durch den Proxy schickst.

Was für 200 Nutzer die bessere Antwort ist

Fast jedes Ziel, für das im Mittelstand Sitzungsrichtlinien vorgeschlagen werden, lässt sich einfacher erreichen. Nicht ganz so elegant, nicht ganz so fein steuerbar – aber mit einem Bruchteil des Betriebsaufwands und ohne einen Proxy im Pfad deiner Produktivanwendungen.

Dein Ziel	Sitzungsrichtlinie	Die pragmatische Alternative	Empfehlung bei 200 Nutzern
Kein Download auf privaten Geräten	Download blockieren je App und Gerätezustand	App-erzwungene Einschränkungen in SharePoint und Exchange, per bedingtem Zugriff auf nicht konforme	Alternative

		Geräte	
Vertrauliche Dokumente schützen	Beim Download automatisch labeln	Vertraulichkeitslabels mit automatischer Anwendung in Purview – schützt die Datei überall, nicht nur in der Sitzung	Alternative
Externe Zugriffe eindämmen	Zugriff je Gerät und Standort blockieren	Bedingter Zugriff mit Gerätekonformität und Anmelderrisiko	Alternative
Zugriff eines Partners auf eine Fachanwendung überwachen	Sitzung protokollieren, Aktionen einschränken	gibt es so nicht	hier lohnt sich die Sitzungsrichtlinie
Upload von Schadsoftware in SharePoint verhindern	Upload blockieren	Defender for Office 365 und der eingebaute SharePoint-Scan	Alternative

Die einzige Zeile mit einem klaren Ja betrifft Partner und Auftragnehmer, die auf einer Fachanwendung arbeiten, deren Zugriff du nicht über die Geräteverwaltung steuern kannst. Wenn du diesen Fall nicht hast, lass Sitzungsrichtlinien liegen und stecke die Zeit in deine [Conditional Access: Baselines, die nicht nerven](#). Die haben eine deutlich bessere Wirkung pro investierter Stunde.

Anomalie-Erkennung: Impossible Travel, Massen-Download und der Rest

Das ist der Teil, der ohne dein Zutun läuft und deshalb der mit dem besten Verhältnis von Aufwand zu Nutzen ist. Die Anomalie-Erkennungsrichtlinien sind standardmäßig aktiv. Es gibt eine Lernphase von sieben Tagen, in der noch nicht alle Alarme ausgelöst werden. Danach wird jede Sitzung mit dem Verhalten des letzten Monats verglichen – Anmeldezeiten, IP-Adressen, Geräte, Risikobewertung der Aktivitäten. Bewertet wird anhand von über 30 Risikoindikatoren, gruppiert in Faktoren wie riskante IP-Adresse, Anmeldefehler, Administratoraktivität, inaktive Konten, Standort, unmögliche Reise, Gerät und Aktivitätsrate.

Was sich seit Juni 2025 geändert hat

Microsoft hat die Anomalie-Erkennung auf ein dynamisches Modell umgestellt. Die Erkennungslogik passt sich der Bedrohungslage an, ohne dass du Richtlinien pflegen musst. Sichtbare Folge: Eine Reihe klassischer Richtlinien ist deaktiviert und in neue, präzisere Erkennungen überführt worden – darunter "Aktivität von verdächtigen IP-Adressen", "Verdächtige Regeln zur Posteingangsbearbeitung", "Verdächtige E-Mail-Löschaktivität", "Ransomware-Aktivität" und "Aktivität durch ausgeschiedene Benutzer".

FAKTEN · Kein Grund zur Panik in der Richtlinienliste

Wenn du in der Richtlinienverwaltung Einträge siehst, die als deaktiviert markiert sind, ist das kein Konfigurationsfehler und kein Versehen deines Vorgängers. Die Erkennung findet weiterhin statt, nur unter anderem Namen und mit anderer Logik. "Ransomware-Aktivität" heißt jetzt sinngemäß "Ransomware-Zahlungsanweisung in Anwendung hochgeladen", "Aktivität durch ausgeschiedene Benutzer" heißt "Aktivität eines deprovisionierten Benutzers". Es ist nichts auszuschalten und nichts nachzubauen.

Impossible Travel richtig verstehen und einstellen

Die Erkennung meldet zwei Aktivitäten desselben Kontos von geografisch weit entfernten Orten in einer Zeitspanne, die für die Strecke nicht reicht. Klingt einfach, ist es nicht, denn drei Details entscheiden über deine Alarmqualität.

Erstens rechnet die Erkennung auf Länder- und Regionsebene. Zwei Aktivitäten innerhalb Deutschlands lösen nie einen Alarm aus, und auch nicht zwischen Deutschland und einem Nachbarland. Wenn dein Außendienst zwischen Aachen und Maastricht pendelt, wirst du hier nichts sehen – was gut ist.

Zweitens gibt es Unterdrückungen. Wenn die IP-Adressen auf beiden Seiten als sicher gelten, etwa weil du sie als Unternehmens-IP markiert hast, wird die Reise als vertrauenswürdig eingestuft und löst keinen Alarm aus – es sei denn, du hast die Empfindlichkeit auf Hoch gestellt. Ist nur eine Seite als sicher eingestuft, greift die Erkennung normal.

Drittens greift die Erkennung nicht bei fehlgeschlagenen und nicht interaktiven Anmeldungen. Das gilt genauso für die Erkennung ungewöhnlicher Länder. Wer also darauf hofft, hier Passwort-Spraying zu sehen, schaut an der falschen Stelle – dafür ist der Identitätsschutz in Entra ID zuständig.

Empfindlichkeit	Unterdrückt	Wirkung	Für wen
Niedrig	System, Tenant und Benutzer	sehr wenige Alarme, hohe Trefferquote, blinde Flecken bei subtilen Fällen	Teams ohne Kapazität für Nachverfolgung
Mittel	System und Benutzer	ausgewogen, der sinnvolle Startwert	der Regelfall im Mittelstand
Hoch	nur System	deutlich mehr Alarme, auch aus vertrauten Regionen	nur mit echtem Betriebsteam oder bei akutem Verdacht

Stell die Empfindlichkeit auf Mittel und lass sie dort. Wenn du eine Person hast, die berufsbedingt ständig zwischen Kontinenten unterwegs ist, nimm sie über die Bereichseinstellung der Richtlinie gezielt heraus, statt die Empfindlichkeit global zu senken. Jede Anomalie-Richtlinie lässt sich einzeln auf Benutzer und Gruppen eingrenzen. Und lege fest, wer die Alarme überhaupt sieht – die Mechanik dafür beschreibt [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Massen-Download: das Signal, auf das es wirklich ankommt

Unter "Ungewöhnliche Aktivitäten (nach Benutzer)" laufen mehrere Erkennungen zusammen, und eine davon ist die wichtigste im ganzen Produkt: ungewöhnlich viele Dateidownloads. Daneben stehen ungewöhnliche Freigabeaktivitäten, ungewöhnliche Löschaktivitäten, ungewöhnliche Identitätswechsel und ungewöhnliche Administratoraktivitäten.

Der Massen-Download ist deshalb so wertvoll, weil er zwei sehr verschiedene Szenarien mit demselben Signal abdeckt. Das eine ist ein übernommenes Konto, aus dem jemand systematisch Daten zieht. Das andere ist die gekündigte Person, die am vorletzten Arbeitstag abends die Projektablage in den Privatorbinder synchronisiert. Beides erzeugt dasselbe Muster: viele Dateien, kurze Zeit, abweichend vom eigenen Normalverhalten.

Eine hohe Rate an Dateiuploads oder -löschungen wiederum kann auf einen laufenden Verschlüsselungsvorgang hindeuten. Diese Signale werden mit Bedrohungsinformationen kombiniert, etwa mit bekannten Dateiendungen von Erpressungssoftware.

Erkennung	Häufigste harmlose Erklärung	Was du zuerst prüfst
-----------	------------------------------	----------------------

Unmögliche Reise	VPN, Reisender, Cloud-Dienst ohne festen Standort	Gerät und Anwendung der zweiten Aktivität
Aktivität aus seltenem Land	Urlaub, Messe, Auslandsprojekt	gab es eine erfolgreiche MFA-Bestätigung
Ungewöhnlich viele Downloads	Projektabschluss, Umzug einer Ablage, Backup-Werkzeug	Gerät, Uhrzeit, Zielordner, Kündigungsstatus
Ungewöhnlich viele Freigaben	neue Zusammenarbeit mit einem Kunden	sind die Empfänger extern und neu
Mehrere fehlgeschlagene Anmeldungen	abgelaufenes Kennwort auf einem Zweitgerät	gleiche IP, gleicher Client, danach Erfolg
Verdächtige Downloads einer OAuth-App	selten harmlos	sofort als Vorfall behandeln

Für Anomalie-Richtlinien lassen sich automatische Governance-Aktionen hinterlegen – Benutzer sperren, Sitzungen beenden, Zustimmung widerrufen. Sei damit im Mittelstand vorsichtig. Eine automatische Kontosperre um 22 Uhr an einem Freitag trifft mit einiger Wahrscheinlichkeit die Geschäftsführung im Hotel und nicht den Angreifer. Fang mit Benachrichtigung an, beobachte drei Monate, automatisiere dann das, was sich als eindeutig erwiesen hat. Wenn du die Alarmer längerfristig aufheben und korrelieren willst, ist das der Punkt, an dem sich ein Blick auf [Microsoft Sentinel anbinden: wann es sich lohnt](#) lohnt.

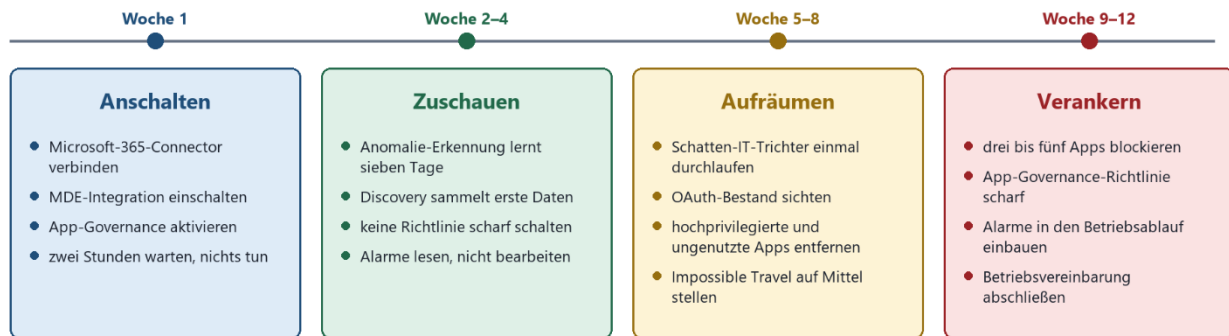
Die ehrliche Priorisierung für 200 Nutzer

Jetzt die Zusammenfassung, die du eigentlich gesucht hast. Nicht alles, was in der Lizenz steckt, verdient deine Zeit. Hier ist meine Einschätzung nach Aufwand, Wirkung und Betriebslast.

Baustein	Einrichtung	Laufender Aufwand	Wirkung	Urteil
Anomalie-Erkennung	einschalten, sieben Tage warten	Alarmer lesen	hoch	Pflicht
App-Governance für OAuth	ein Schalter, zehn Stunden Wartezeit	vierteljährlich durchsehen	hoch	Pflicht
Cloud Discovery über Defender for Endpoint	ein Schalter, zwei Stunden Wartezeit	ein Trichterdurchlauf pro Quartal	mittel bis hoch	Pflicht
Apps blockieren über Netzwerkschutz	je App ein Klick	Ausnahmen und Rückfragen	mittel	gezielt, nicht flächig
Aktivitätsrichtlinien selbst bauen	Stunden bis Tage	dauerhaftes Nachjustieren	gering ohne Betriebsteam	später, wenn überhaupt
Conditional Access App Control	Tage, plus Tests je Anwendung	hoch, jede App-Änderung kann brechen	punktuell	nur bei konkretem Anlass
Dateirichtlinien in MDCA	Stunden	entfällt ab Januar 2027	wandert nach Purview	gar nicht mehr anfangen

Drei Bausteine sind Pflicht, weil sie im Wesentlichen aus einem Schalter und etwas Geduld bestehen. Zwei sind bewusst wegzulassen. Und einer – die Dateirichtlinien – ist ein Auslaufmodell, in das du keine Minute mehr stecken solltest.

90 Tage Defender for Cloud Apps bei 200 Nutzern



Was in diesem Plan bewusst fehlt: Sitzungsrichtlinien. Die kommen erst, wenn es einen konkreten Anlass gibt – nicht, weil das Lizenzpaket sie hergibt.

Skizze 5: Ein Einführungsplan, der zu einer kleinen IT-Mannschaft passt. Die Wartezeiten sind Teil des Plans, kein Leerlauf.

Auffällig an diesem Plan: In den ersten vier Wochen tust du fast nichts. Das ist kein Versehen. Die Anomalie-Erkennung braucht ihre sieben Tage Lernphase, Discovery braucht Datenvolumen, und jede Richtlinie, die du in dieser Zeit scharf schaltest, arbeitet gegen einen Normalzustand, den das System noch gar nicht kennt. Wer in Woche eins die erste Blockade setzt, produziert vor allem Fehlalarme und verliert das Vertrauen der Belegschaft. Diese Zurückhaltung passt zu der Haltung, die im Beitrag [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) beschrieben ist: Kontrolle dort, wo sie messbar etwas ändert, und nicht überall, wo sie technisch möglich wäre.

TIPP · Der Satz für die Geschäftsführung

"Wir sehen jetzt, welche Cloud-Dienste tatsächlich genutzt werden, wir haben elf alte Zugriffsrechte von externen Anwendungen entfernt, und wir bekommen eine Meldung, wenn ein Konto sich untypisch verhält." Das ist in drei Sätzen der gesamte Nutzen und es ist mehr, als die meisten Unternehmen dieser Größe vorweisen können. Wie du daraus ein Berichtsformat machst, das auch beim vierten Mal noch gelesen wird, steht in [Security-Reporting für die Geschäftsführung](#).

Wenn du bei der Priorisierung oder bei der Frage, ob sich das Lizenz-Upgrade überhaupt rechnet, eine zweite Meinung möchtest: Genau dafür gibt es die [Microsoft-365-Security-Beratung](#). Und wenn dein Team das Defender-Portal souverän bedienen soll, statt sich durch Menüs zu klicken, ist die [Schulung Microsoft 365 Security](#) der schnellere Weg.

FAQ

Brauche ich Defender for Cloud Apps, wenn ich schon Defender for Endpoint habe?

Das sind zwei verschiedene Ebenen. Defender for Endpoint schützt das Gerät und sieht, was darauf passiert. Defender for Cloud Apps schützt die Cloud-Dienste und sieht, was in ihnen passiert – auch dann, wenn der Zugriff von einem Gerät kommt, das dir nicht gehört. Die beiden ergänzen sich: Erst die Kombination liefert dir Schatten-IT-Erkennung mit Gerätekontext. Umgekehrt gilt aber auch: Ohne Defender for Endpoint fehlt dir für die Discovery die Datenquelle, und du landest wieder bei Firewall-Logs.

Reicht Microsoft 365 Business Premium?

Für Defender for Cloud Apps nicht. Business Premium enthält Defender for Business, also die Endpunkt-Seite, aber nicht den CASB. Du kannst Defender for Cloud Apps als Zusatzlizenz erwerben, dann funktioniert die Kombination einschließlich der Discovery-Integration einwandfrei. Rechne das vorher durch: Bei 200 Nutzern ist der Aufpreis eine Position, die in der Budgetplanung sichtbar wird.

Wie lange dauert es, bis ich Daten sehe?

Nach dem Einschalten der Integration mit Defender for Endpoint bis zu zwei Stunden für die ersten Discovery-Daten. App-Governance braucht nach der Aktivierung bis zu zehn Stunden. Die Anomalie-Erkennung hat eine Lernphase von sieben Tagen, in der nicht alle Alarme ausgelöst werden. Discovery-Daten werden danach viermal täglich neu analysiert. Ein belastbares Bild deiner Cloud-Nutzung hast du realistisch nach drei bis vier Wochen.

Muss ich den Betriebsrat beteiligen?

Wenn es einen gibt: ja, sehr wahrscheinlich. Die Discovery erzeugt personenbezogene Nutzungsdaten, die Anomalie-Erkennung bewertet individuelles Verhalten. Das ist eine technische Einrichtung, die zur Verhaltens- und Leistungskontrolle geeignet ist, und damit mitbestimmungspflichtig – unabhängig von deiner Absicht. Der pragmatische Weg: Discovery zunächst mit anonymisierten Benutzernamen betreiben, das Gespräch mit dem Ergebnis führen, dann eine Vereinbarung schließen, die Anlässe und Verfahren für die Deanonymisierung regelt. Details stehen im Beitrag zum Thema Betriebsrat und Monitoring.

Was passiert mit meinen Dateirichtlinien?

Die Dateirichtlinien von Defender for Cloud Apps werden am 6. Januar 2027 eingestellt. Dateibasierte Datenschutzfunktionen wandern zu Microsoft Purview. Wenn du bestehende Richtlinien hast, plane die Migration nach Purview DLP oder auf automatische Klassifizierung rechtzeitig ein. Wenn du noch keine hast: gar nicht erst anfangen, sondern direkt in Purview bauen.

Kann ich Impossible Travel abschalten, wenn es zu viele Fehlalarme gibt?

Kannst du, solltest du aber nicht. Setze stattdessen die Empfindlichkeit auf Niedrig – dann werden zusätzlich Unterdrückungen auf Tenant- und Benutzerebene wirksam. Oder grenze die Richtlinie über die Bereichseinstellung auf die Gruppen ein, bei denen sie sinnvoll ist. Der häufigste Auslöser für Fehlalarme sind übrigens VPN-Dienste und Cloud-Anwendungen ohne festen Standort; wenn deine Unternehmens-IP-Adressen sauber getaggt sind, verschwindet ein guter Teil des Rauschens von selbst.

Blockiert Defender for Cloud Apps auch Apps auf privaten Geräten?

Nein. Die Blockade läuft über den Netzwerkschutz von Defender for Endpoint und wirkt deshalb nur auf verwalteten, angebundenen Geräten – dort allerdings unabhängig vom Standort, also auch im Homeoffice und unterwegs. Für private Geräte brauchst du einen anderen Hebel: bedingten Zugriff mit Gerätekonformität, app-erzwungene Einschränkungen oder eben doch Sitzungsrichtlinien.

Warum sind mehrere Anomalie-Richtlinien in meinem Tenant deaktiviert?

Weil Microsoft sie seit Juni 2025 in ein dynamisches Erkennungsmodell überführt hat. Betroffen sind unter anderem Ransomware-Aktivität, verdächtige Posteingangsregeln, Aktivität von

anonymen IP-Adressen und Aktivität durch ausgeschiedene Benutzer. Die Erkennung läuft unter neuen Namen und mit aktualisierter Logik weiter. Du musst nichts wieder einschalten und nichts nachbauen.

Lohnt sich Conditional Access App Control für uns wirklich nicht?

In den meisten Fällen nicht. Der ehrliche Prüfstein ist eine Frage: Hast du Personen, die auf Unternehmensdaten zugreifen müssen, deren Geräte du aber weder verwaltest noch verwalten wirst – typischerweise Auftragnehmer oder Partnerunternehmen auf einer Fachanwendung? Wenn ja, ist es die richtige Funktion. Wenn nein, erreichst du dieselben Ziele mit bedingtem Zugriff, Gerätekonformität und Vertraulichkeitslabels bei erheblich geringerem Betriebsaufwand.

Was ist der Unterschied zwischen App-Governance und der Consent-Einstellung in Entra ID?

Die Consent-Einstellung ist die Vorbeugung: Sie legt fest, wem Benutzer überhaupt zustimmen dürfen und ab welcher Berechtigung eine Genehmigung nötig ist. App-Governance ist die Beobachtung und das Aufräumen: Sie zeigt dir, welche Anwendungen tatsächlich da sind, was sie tun, welche zu viele Rechte haben und welche seit Monaten nichts mehr tun. Du brauchst beides – die Einstellung verhindert Neuzugänge, die Governance räumt den Altbestand auf.

Fazit

Defender for Cloud Apps ist im Mittelstand kein Projekt, sondern eine Reihenfolge. Drei Schalter, zwei Wartezeiten, ein Quartalsrhythmus – und du hast den größten Teil des Nutzens eingesammelt, ohne dass jemand dafür eine neue Stelle schaffen muss. Cloud Discovery über Defender for Endpoint zeigt dir, was tatsächlich benutzt wird. App-Governance räumt einen Altbestand auf, von dem du bis heute nichts wusstest. Die Anomalie-Erkennung meldet sich, wenn ein Konto sich untypisch verhält. Das läuft weitgehend von allein.

Der Rest ist Fleißarbeit mit fragwürdigem Ertrag. Sitzungsrichtlinien sind eine beeindruckende Technologie für ein Problem, das du bei 200 Nutzern meistens einfacher lösen kannst. Selbst gebaute Aktivitätsrichtlinien brauchen ein Team, das ihre Alarmer auch liest. Und Dateirichtlinien haben ein Ablaufdatum. Der Unterschied zwischen einem funktionierenden und einem gescheiterten CASB-Projekt liegt fast nie an der Technik, sondern daran, ob jemand den Mut hatte, zwei Drittel des Funktionsumfangs bewusst wegzulassen.

Und wenn du nach dem ersten Durchlauf feststellst, dass die Vertriebsabteilung seit drei Jahren Angebote über einen Dienst verschickt, von dem in der IT niemand je gehört hat: Das ist kein Grund für ein Verfahren. Das ist der Grund, warum du das Werkzeug eingeschaltet hast.

WEITER IM THEMA

- › [App-Registrierungen und Consent-Governance](#) – die vorbeugende Seite: wer im Tenant überhaupt zustimmen darf
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) – das Denkmodell hinter der Priorisierung in diesem Beitrag
- › [Defender for Endpoint: Onboarding ohne Drama](#) – die Voraussetzung für Cloud Discovery ohne Log-Collector
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) – bevor du Discovery mit Klarnamen betreibst
- › [Conditional Access: Baselines, die nicht nerven](#) – die Richtlinien, die mehr bringen als Sitzungssteuerung

- › [Kompromittiertes Konto erkennen und aufräumen](#) — *wenn ein Alarm sich als echt herausstellt*
- › [Ransomware-Vorsorge in Microsoft 365](#) — *das Szenario hinter dem Massen-Download-Signal*
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — *die Grundlagen, die vor jedem CASB kommen*
- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — *wenn Nachweispflichten ins Spiel kommen*
- › [MFA in Microsoft 365 richtig einführen](#) — *die Maßnahme mit dem besten Verhältnis von Aufwand zu Wirkung*
- › [Microsoft 365 Security](#) — *die Übersicht über die gesamte Serie*
- › [Dossier TerminalFix und der Berlin-Hack](#) — *wie so etwas in der Praxis abläuft*