

Defender for Endpoint: Onboarding ohne Drama

Es gibt einen Satz, der in Projektbesprechungen erstaunlich oft fällt: „Defender ist doch schon drin, das läuft.“ Meistens stimmt der erste Teil. Der zweite fast nie. Auf den Geräten läuft Microsoft Defender Antivirus, weil Windows das seit Jahren mitbringt. Onboardet an den Dienst ist deshalb noch gar nichts. Im Defender-Portal steht eine leere Geräteinventur, und das einzige, was tatsächlich läuft, ist die Zeit.

Das ist die gute Nachricht an dieser Baustelle: Du musst nichts kaufen, was du nicht schon hast, und du musst nichts installieren. Du musst zwei Dienste miteinander bekannt machen, eine Richtlinie zuweisen und danach eine Handvoll Schalter in der richtigen Reihenfolge umlegen. Das Drama entsteht nicht beim Onboarding. Es entsteht danach — wenn jemand alle ASR-Regeln gleichzeitig auf Block dreht, weil das im Testtenant mit vier virtuellen Maschinen so schön unauffällig war, und am nächsten Morgen die Warenwirtschaft nicht mehr startet.

Dieser Beitrag beschreibt den Weg von der Lizenzfrage bis zur ersten belastbaren Betriebsaussage: welche Produktvariante was kann, wie das Onboarding über Intune abläuft, welche Schutzschalter in welcher Reihenfolge scharf gestellt werden, wie du ASR-Regeln einführst, ohne die Belegschaft gegen dich aufzubringen, und was du vorher festgelegt haben musst, damit im Ernstfall jemand ein Gerät isolieren darf. Er gehört in die Reihe [Microsoft 365 Security](#), in der die einzelnen Bausteine einer Microsoft-365-Absicherung zusammenlaufen.

Eine Warnung vorweg, damit die Erwartung stimmt: Der Endpunkt ist die letzte Verteidigungslinie, nicht die erste. Wenn Identitäten ungeschützt sind und die Mandantenkonfiguration löchrig ist, rettet dich auch ein perfekt konfigurierter Defender nicht. Die Grundlagen stehen in [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — dieser Beitrag setzt sie voraus.

Erst die Lizenz, dann der Klick

Die häufigste Ursache für ein gescheitertes Defender-Projekt ist nicht die Technik, sondern eine falsche Annahme über den eigenen Vertrag. Es gibt drei Produktvarianten, sie heißen ähnlich, sie sehen im Portal ähnlich aus, und sie können deutlich Unterschiedliches. Wer das vorher klärt, spart sich die Diskussion darüber, warum eine Funktion aus dem Handbuch im eigenen Tenant nicht existiert.

Plan 1, Plan 2 und Defender for Business

Defender for Endpoint Plan 1 ist die Präventionsvariante: Next-Generation-Schutz, alle ASR-Funktionen, Network Protection, Web Protection und Webinhaltsfilterung, Device Control, Anwendungssteuerung, Firewall — und ein überraschend brauchbarer Satz manueller Reaktionsmöglichkeiten, zu dem auch die Geräteisolation gehört. Plan 1 steckt in Microsoft 365 E3.

Plan 2 legt das dazu, was aus Prävention eine Ermittlungsfähigkeit macht: EDR, automatisierte Untersuchung und Behebung, Advanced Hunting mit sechs Monaten Datenhaltung, Threat Analytics, die Sandbox-Tiefenanalyse und das Schwachstellenmanagement. Plan 2 steckt in Microsoft 365 E5. Der praktische Unterschied im Alltag: Mit Plan 1 siehst du, dass etwas geblockt wurde. Mit Plan 2 siehst du, was der Angreifer davor und danach getan hat.

Defender for Business ist die Variante für Organisationen bis 300 Nutzer, unter anderem in Microsoft 365 Business Premium enthalten. Sie liefert Next-Generation-Schutz, ASR-Funktionen,

EDR und automatisierte Untersuchung mit deutlich vereinfachter Konfiguration. Fünf Clientgeräte je Nutzerlizenz sind abgedeckt; Server brauchen ein eigenes Add-on. Auffällig sind die kleinen Grenzen: Es gibt genau eine Webinhaltsfilter-Richtlinie pro Organisation, eigene ASR-Regeln lassen sich nicht anlegen, und für ASR-Regeln sowie überwachten Ordnerzugriff brauchst du trotzdem Intune.

Was in welcher Variante steckt

Defender for Business	Defender for Endpoint P1	Defender for Endpoint P2
bis 300 Nutzer	in Microsoft 365 E3	in Microsoft 365 E5
- Next-Generation-Schutz - ASR-Funktionen (vereinfacht) - EDR - Automated Investigation - vereinfachte Einrichtung - eine Webfilter-Richtlinie 5 Clients je Lizenz - Server nur als Add-on	- Next-Generation-Schutz - ASR-Regeln vollständig - Network Protection - Web Protection und Filter - Device Control - App Control und Firewall - manuelle Reaktionen - Geräteisolation	- alles aus Plan 1 - EDR mit Blockmodus - Automated Investigation - Advanced Hunting 6 Monate Datenhaltung - Threat Analytics - Deep Analysis / Sandbox - Vulnerability Management

Mischlizenzierung wird nicht unterstützt: Wer Defender for Business und Plan 2 im selben Tenant hat, bekommt für alle das Defender-for-Business-Erlebnis. Der Wechsel geht erst nach Volllizenzierung — und nur über den Microsoft-Support.

ASR-Regeln laufen technisch auf jeder Windows-Edition mit Microsoft Defender Antivirus. Was die Lizenz kauft, ist die zentrale Auswertung: Berichte, Alarmer und Advanced Hunting.

Skizze 1: Die drei Produktvarianten und ihre Grenzen. Plan 2 enthält Plan 1 vollständig.

Fähigkeit	Defender for Business	Plan 1	Plan 2
Next-Generation-Schutz	ja	ja	ja
ASR-Regeln zentral verwalten	ja, ohne eigene Regeln	ja	ja
Network Protection	ja	ja	ja
Manuelle Reaktionen, Geräteisolation	ja	ja	ja
EDR	ja	nein	ja
EDR im Blockmodus	nein	nein	ja
Automated Investigation and Response	ja	nein	ja
Advanced Hunting, 6 Monate Historie	nein	nein	ja
Threat Analytics, Tiefenanalyse	nein	nein	ja
Schwachstellenmanagement	nein	Grundumfang	ja
Nutzerobergrenze	300	keine	keine

Tabelle 1: Der Vergleich in der Kurzfassung. Maßgeblich sind immer die aktuellen Produktbedingungen.

Die Mischlizenz-Falle

Hier verunglücken erstaunlich viele Projekte. Microsoft unterstützt keine gemischte Endpunktsicherheits-Lizenzierung. Wer 80 Nutzer mit Business Premium hat und für 30 davon Microsoft 365 E5 Security dazukaft, bekommt nicht für 30 Nutzer die Plan-2-Oberfläche — der gesamte Tenant bleibt im Defender-for-Business-Erlebnis. Um auf Plan 2 zu wechseln, musst du alle Nutzer entsprechend lizenzieren und den Wechsel anschließend beim Microsoft-Support beantragen. Das ist kein Schalter im Portal, und es passiert nicht über Nacht.

Ähnlich gelagert ist die Serverfrage. Für Defender-for-Business-Organisationen gibt es ein Server-Add-on, das pro Serverinstanz abgerechnet wird. Ab etwa 60 Servern verweist Microsoft auf die Enterprise-Modelle, also Defender for Endpoint Server oder Defender for Servers aus Defender for Cloud. Wer Server ohne passende Lizenz onboardet, hat kein technisches Problem, sondern ein vertragliches — und die fallen bekanntlich später auf, dafür aber teurer.

WARNUNG — Drei Sätze, die dich Geld kosten

„Wir kaufen E5 erst mal für die Admins.“ — In einem Tenant mit Defender for Business bringt das niemandem die Plan-2-Funktionen, sondern nur eine Rechnung.

„Server nehmen wir einfach mit rein.“ — Onboarding funktioniert, die Lizenzpflicht bleibt.

„Wir starten mit Plan 1 und schauen dann.“ — Legitim, aber dann fehlen dir EDR-Blockmodus, automatisierte Untersuchung und die gesamte Hunting-Historie. Plane das ein, statt es zu entdecken.

Onboarding über Intune: der eigentliche Vorgang

Das Onboarding selbst ist unspektakulär, und das ist eine gute Eigenschaft. Es besteht aus einer Dienst-zu-Dienst-Verbindung, ein paar Schaltern und einer Richtlinie. Es gibt keinen Agenten zu verteilen, keinen Reboot zu planen und keine Softwareverteilung anzufassen. Ein Gerät wird genau einmal onboardet und bleibt es dann.

Schritt eins: der Connector

Zuerst müssen Intune und Defender for Endpoint voneinander wissen. Der Schalter dafür liegt nicht in Intune, sondern im Defender-Portal unter den erweiterten Features: „Intune-Verbindung“ auf Ein, speichern. Danach zeigt Intune unter Endpunktsicherheit den Verbindungsstatus „Aktiviert“ an — allerdings mit bis zu 15 Minuten Verzögerung. Wer in dieser Zeit dreimal hin- und herklickt und dabei etwas anderes verstellt, hat den ersten selbstgebauten Fehler schon eingebaut.

Für den Aufbau brauchst du zwei Berechtigungen an zwei Stellen: in Intune die Rolle „Endpoint Security Manager“ oder gleichwertige Rechte, im Defender-Portal die Rolle „Sicherheitsadministrator“ aus Microsoft Entra ID. Für neue Defender-for-Endpoint-Kunden gilt seit dem 16. Februar 2025 ausschließlich das vereinheitlichte rollenbasierte Zugriffsmodell; bestehende Tenants behalten ihre gewachsenen Rollen. Das ist ein Detail, das genau dann auffällt, wenn du eine Anleitung aus dem Jahr 2023 nachklickst und der beschriebene Menüpunkt nicht existiert.

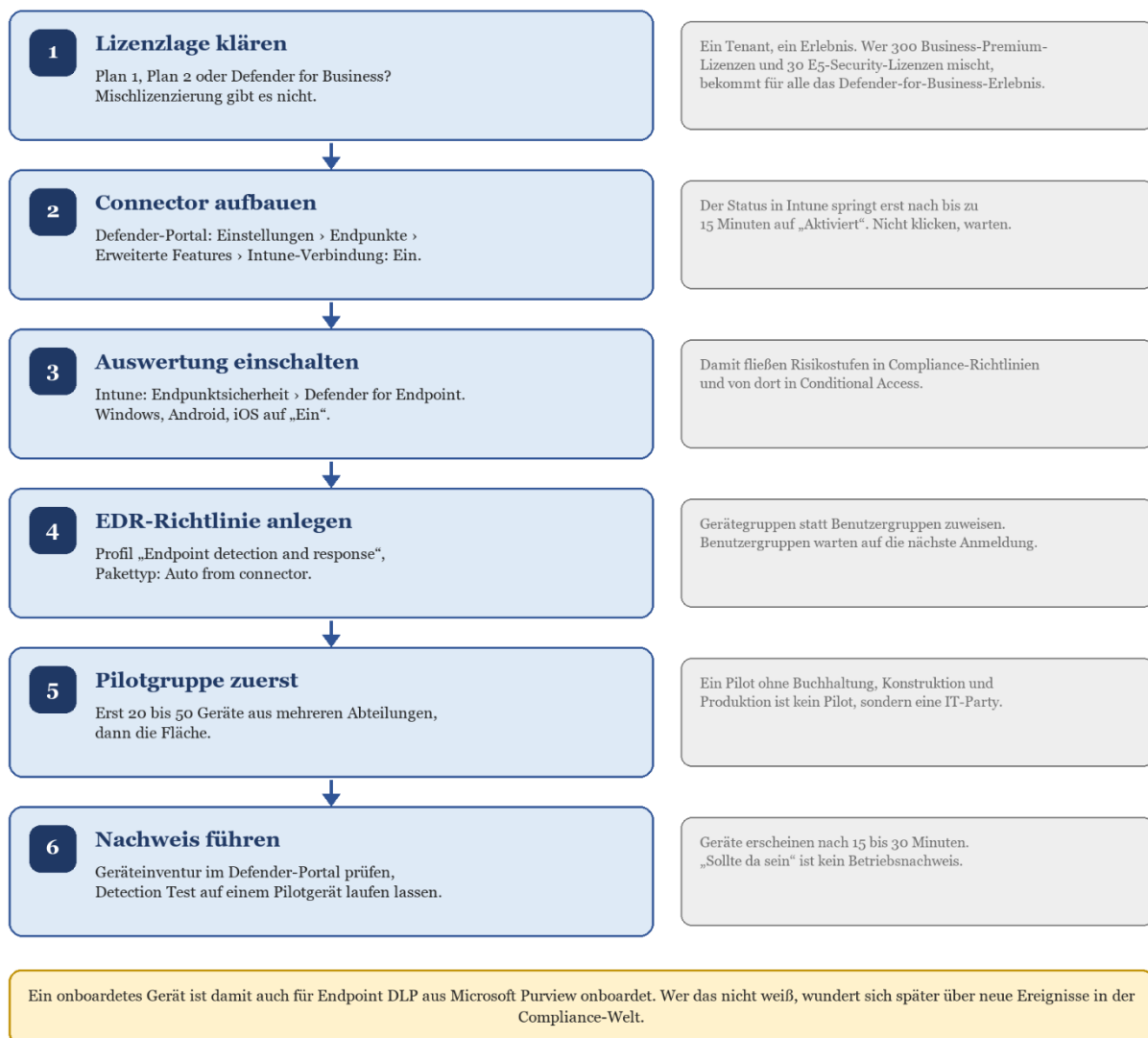
Schritt zwei: die EDR-Richtlinie

Anschließend legst du in Intune unter Endpunktsicherheit eine Richtlinie vom Profiltyp „Endpoint detection and response“ an. Beim Pakettyp wählst du „Auto from connector“ — Intune hat das Onboarding-Paket über die Dienstverbindung bereits erhalten. Den Blob musst du nur dann manuell einfügen, wenn keine Verbindung besteht oder du in einer abgeschotteten Umgebung

arbeitest. Für die Fläche gibt es zusätzlich eine vorkonfigurierte Richtlinie über den Reiter „EDR-Onboardingstatus“, die direkt an alle Windows-Geräte geht.

Zwei Einstellungen verdienen eine bewusste Entscheidung statt eines Reflexes. Erstens das Sample Sharing: „All“ erlaubt die automatische Übermittlung verdächtiger Dateien zur Analyse und verbessert die Erkennung, „None“ schaltet das ab und kostet Erkennungsfähigkeit. Das ist eine Datenschutzfrage, die du dokumentiert beantworten solltest, nicht eine, die du im Assistenten durchklickst. Zweitens die Zuweisung: Nimm Gerätegruppen, keine Benutzergruppen. Bei Benutzergruppen greift die Richtlinie erst, wenn sich jemand anmeldet — und genau die Geräte, die monatelang niemand anfasst, sind selten die unproblematischen.

Onboarding-Ablauf: von der Lizenz bis zum ersten Nachweis



Skizze 2: Der Onboarding-Ablauf mit den Stellen, an denen erfahrungsgemäß etwas hakt.

Schritt drei: nachweisen statt hoffen

Nach 15 bis 30 Minuten sollten die ersten Geräte in der Geräteinventur des Defender-Portals auftauchen. Der Onboardingstatus steht in Intune unter Endpunktsicherheit im Reiter „EDR-Onboardingstatus“. Für den eigentlichen Funktionsnachweis gibt es den Detection Test von Microsoft: ein harmloses Skript, das eine Erkennung auslöst und damit belegt, dass die Kette vom

Gerät bis zur Alarmierung tatsächlich geschlossen ist. Ein Onboarding ohne diesen Test ist ein Onboarding mit Vertrauensvorschuss.

Für den detaillierten Klickpfad — inklusive der Ausbaustufen A1 und A2 mit Screenshots und Zwischenprüfungen — gibt es das [Dossier TerminalFix und der Berlin-Hack](#). Dort ist beschrieben, was in einer realen Umgebung passiert ist, in der genau diese Schritte zu spät kamen.

TIPP — Was du beim Onboarding gleich mitdokumentierst

Wer den Connector aufgebaut hat und wann — inklusive der beiden verwendeten Rollen.

Welche Entscheidung beim Sample Sharing getroffen wurde und von wem.

Welche Gerätegruppen zugewiesen sind und welche Geräte bewusst ausgenommen sind (Kassensysteme, Maschinensteuerungen, Altgeräte mit Herstellerfreigabe).

Das Ergebnis des Detection Tests mit Datum. Das ist dein Betriebsnachweis, wenn später jemand fragt, seit wann der Schutz wirkt.

WICHTIG — Onboarding hat einen Nebeneffekt, den viele übersehen

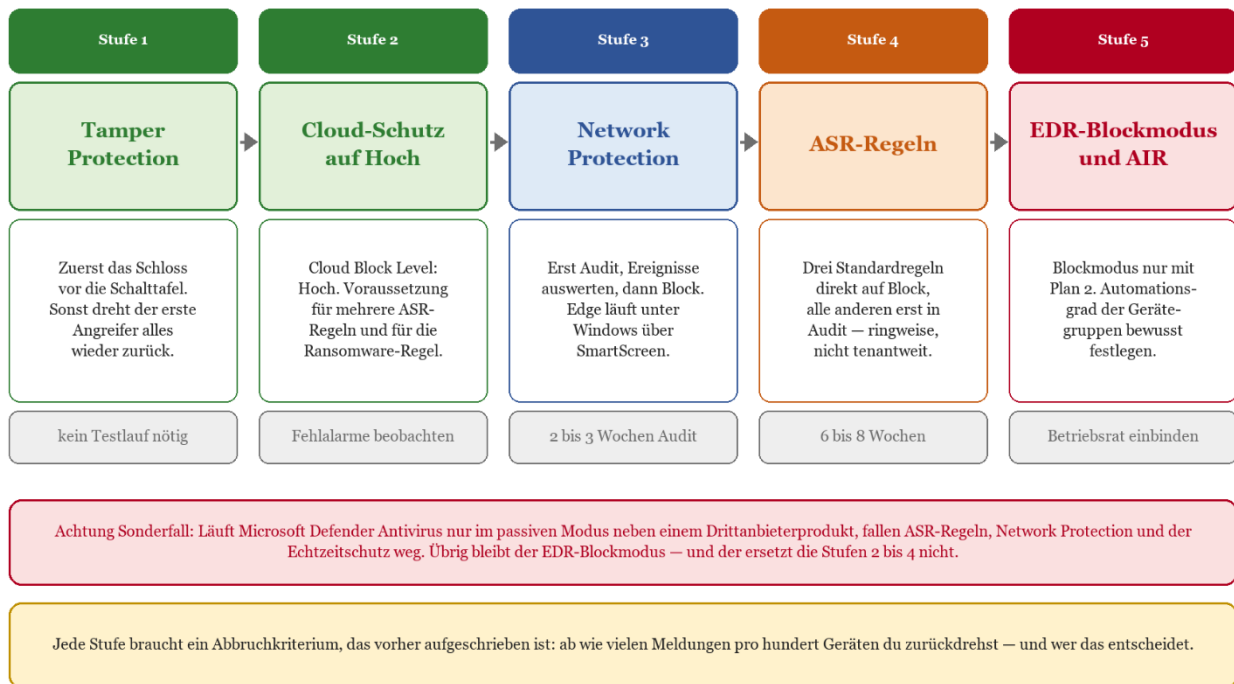
Ein Gerät, das an Defender for Endpoint onboardet wird, ist damit gleichzeitig für Endpoint Data Loss Prevention onboardet. Wenn in eurer Compliance-Welt jemand parallel an DLP-Richtlinien arbeitet, solltet ihr das voneinander wissen — sonst tauchen plötzlich Ereignisse auf, die niemand bestellt hat. Mehr dazu im [Kompetenzbereich Microsoft Purview](#).

Umgekehrt gilt: Onboarding- und Offboarding-Richtlinien dürfen niemals gleichzeitig auf dasselbe Gerät zielen. Das Offboarding-Paket verfällt zudem sieben Tage nach dem Download; abgelaufene Pakete werden abgewiesen.

Die Schalter, die tatsächlich etwas bewirken

Nach dem Onboarding ist ein Gerät sichtbar, aber noch nicht besonders gut geschützt. Die Standardeinstellungen sind ein vernünftiger Kompromiss für ein Betriebssystem, das auf Millionen sehr unterschiedlichen Rechnern läuft. Für ein verwaltetes Unternehmensgerät sind sie zu zurückhaltend. Vier Schalter machen den Unterschied — und sie gehören in dieser Reihenfolge umgelegt.

In welcher Reihenfolge du die Schalter umlegst



Skizze 3: Die Reihenfolge ist kein Geschmacksurteil. Jede Stufe setzt die vorherige voraus.

Tamper Protection zuerst

Manipulationsschutz kommt vor allem anderen. Er sorgt dafür, dass Echtzeitschutz, Verhaltensüberwachung, Cloud-Schutz, Signaturupdates und die automatischen Aktionen auf erkannte Bedrohungen nicht abgeschaltet werden können — auch nicht von einem lokalen Administrator und auch nicht von Schadsoftware, die es als Erstes genau darauf abgesehen hat. Selbst die Antiviren-Ausschlüsse lassen sich unter bestimmten Voraussetzungen gegen Manipulation absichern. Für Unternehmenskunden ist der Manipulationsschutz im Rahmen des integrierten Schutzes standardmäßig eingeschaltet; prüfen solltest du es trotzdem.

Zwei Eigenheiten musst du kennen. Erstens: Bei aktivem Manipulationsschutz werden Änderungen an geschützten Einstellungen über Gruppenrichtlinien schlicht ignoriert. Sie sehen im GPO richtig aus und wirken nicht. Wer noch mit Gruppenrichtlinien für Defender-Einstellungen arbeitet, verwaltet ab hier eine Illusion. Zweitens: Wenn du an einem Gerät wirklich etwas ändern musst, gibt es den Problembehandlungsmodus, der den Schutz vorübergehend aussetzt — danach werden die Einstellungen auf den konfigurierten Stand zurückgesetzt. Ob der Schutz aktiv ist, verrät lokal das Cmdlet Get-MpComputerStatus im Feld IsTamperProtected.

Microsoft baut diese Funktion gerade aus: Der bisherige Manipulationsschutz wird in den Verwaltungsoberflächen in „Controlled Configuration“ umbenannt. An bestehenden Bereitstellungen ändert sich dadurch nichts, und die erweiterten Schutzwirkungen bekommst du nicht automatisch — dafür brauchst du eine eigene Richtlinie über Intune oder die Sicherheitseinstellungsverwaltung. Ein Umbenennen ist kein Upgrade.

Cloud-Schutz auf Hoch

Der Cloud-Schutz ist der Grund, warum moderne Erkennung überhaupt funktioniert: Statt auf die nächste Signaturlieferung zu warten, fragt der Client bei jeder unklaren Datei die Microsoft-

Dienste. Er ist standardmäßig aktiv, aber die Blockierstufe steht ab Werk auf „Nicht konfiguriert“. In Intune findest du sie in der Antivirus-Richtlinie unter „Cloud Block Level“ mit den Werten Hoch, Hoch Plus und Nulltoleranz.

Für produktive Clientflotten ist „Hoch“ die vernünftige Einstellung: starke Erkennung bei optimierter Clientleistung, zum Preis von etwas mehr Fehlalarmen. „Hoch Plus“ kostet spürbar Leistung, „Nulltoleranz“ blockiert schlicht jede unbekannte ausführbare Datei — das ist eine Einstellung für Kioskrechner und Steuerungsterminals, nicht für die Entwicklungsabteilung, es sei denn, du willst dort ein Volksfest auslösen.

FAKTEN — Warum „Hoch“ mehr ist als eine Geschmacksfrage

Drei ASR-Regeln liefern EDR-Alarme überhaupt erst ab der Cloud-Stufe „Hoch Plus“ oder „Nulltoleranz“: Adobe Reader ohne Kindprozesse, ausführbare Inhalte aus E-Mail und Webmail sowie JavaScript und VBScript als Downloader.

Für die Benutzer-Pop-ups derselben Regeln genügt die Stufe „Hoch“. Wer bei „Nicht konfiguriert“ bleibt, hat die Regeln aktiv, aber weder Alarm noch sichtbaren Hinweis.

Die Regel „Erweiterter Schutz vor Ransomware“, die Prävalenz- und Vertrauenswürdigkeitsregel und die Regel gegen verschleierte Skripte setzen den Cloud-Schutz technisch voraus. Ohne ihn laufen sie ins Leere.

Blockierstufen wirken nur, wenn die Geräte die Defender-Clouddienste auch erreichen. In Umgebungen mit strikten Proxykonfigurationen ist das eine eigene Prüfung wert.

Network Protection: erst zusehen, dann eingreifen

Network Protection zieht den Schutz vor gefährlichen Zieladressen von der Browserebene auf die Betriebssystemebene. Damit gilt er auch für Nicht-Microsoft-Browser und für Prozesse, die gar kein Browser sind — PowerShell zum Beispiel, das gerade eine Nutzlast nachladen möchte. Unter Windows überwacht Network Protection Microsoft Edge übrigens nicht; dort greift SmartScreen. Für alles andere ist Network Protection zuständig, und für benutzerdefinierte Indikatoren und Webinhaltsfilterung außerhalb von Edge muss sie im Blockmodus laufen.

Der Weg dorthin führt über den Auditmodus. Zwei bis drei Wochen mitschreiben, dann auswerten: In Advanced Hunting findest du die Ereignisse in DeviceEvents mit den Aktionstypen ExploitGuardNetworkProtectionAudited und ExploitGuardNetworkProtectionBlocked, lokal im Ereignisprotokoll unter den IDs 1125 für Audit und 1126 für Block. Aus dieser Liste ergeben sich die Zulassungsindikatoren, die du brauchst, bevor du auf Block schaltest. Erlaubende Indikatoren haben Vorrang vor Blockierungen; bis eine Änderung greift, können bis zu zwei Stunden vergehen.

WARNUNG — Die drei Punkte, an denen Network Protection Ärger macht

Blockiert werden Verbindungen auf allen Ports, nicht nur auf 80 und 443. Wer nur die Webnutzung im Blick hat, übersieht Anwendungen mit eigenen Ports.

Für Nicht-Microsoft-Browser müssen QUIC und Encrypted Client Hello deaktiviert sein, sonst kann Network Protection den Zielnamen im TLS-Handshake nicht lesen. In Chrome und Firefox sind das je zwei Richtlinien; alternativ blockierst du ausgehenden UDP-Verkehr auf Port 443 in der Windows-Firewall — mit allen Nebenwirkungen, die das für Office und andere Anwendungen hat.

Auf Windows Server und in Multisession-Umgebungen reicht die Richtlinie nicht: Dort sind zusätzliche Schalter über Set-MpPreference nötig. Die Datagrammverarbeitung auf Servern kann je nach Verkehrsaufkommen Netzwerkleistung kosten. Erst messen, dann flächig ausrollen.

EDR im Blockmodus — und wann er nicht hilft

Der EDR-Blockmodus ist eine Plan-2-Funktion und für einen sehr konkreten Fall gedacht: Auf dem Gerät läuft ein Drittanbieter-Virenschutz, Microsoft Defender Antivirus steht deshalb im passiven Modus, und die verhaltensbasierten EDR-Erkennungen sollen trotzdem behoben werden. Genau das leistet der Blockmodus — er lässt Defender Antivirus nachträglich auf Funde reagieren, die das primäre Produkt durchgelassen hat. Im Aktionscenter tauchen die Ergebnisse als „Blockiert“ oder „Verhindert“ auf.

Wichtig ist, was er nicht leistet. Steht Defender Antivirus im passiven Modus, fallen Echtzeitschutz, ASR-Regeln, Network Protection und die Indikatoren weg. Das sind genau die Funktionen, über die dieses Kapitel bis hierhin gesprochen hat. Der Blockmodus ist ein Sicherheitsnetz, kein Ersatz für die vorherigen drei Stufen. Wer beide Welten will, muss entscheiden, welches Produkt aktiv sein soll — und diese Entscheidung ehrlich zu Ende denken.

Schalter	Wo eingestellt	Empfehlung	Erwartbare Nebenwirkung
Tamper Protection	Intune oder Defender-Portal, tenantweit oder je Gruppe	an, ohne Testphase	GPO-Änderungen an geschützten Einstellungen wirken nicht mehr
Cloud-Schutz	Intune, Antivirus-Richtlinie	an lassen	keine; ohne Cloud-Schutz funktionieren mehrere ASR-Regeln nicht
Cloud Block Level	Intune, Antivirus-Richtlinie	Hoch	etwas mehr Fehlalarme, dafür vollständige Regelwirkung
Network Protection	Intune, ASR-Richtlinie	Audit, nach Auswertung Block	Blockaden auf allen Ports; QUIC muss in Fremdbrowsern aus
EDR im Blockmodus	Defender-Portal oder Intune-CSP	an, wenn Plan 2 vorhanden	nur relevant bei passivem Defender Antivirus
Automatisierungsgrad	Defender-Portal, Gerätegruppen	vollständig automatisch	automatische Behebung will vorher abgestimmt sein

Tabelle 2: Die sechs Grundeinstellungen nach dem Onboarding.

ASR-Regeln: Audit, dann Block, dann Ruhe

Regeln zur Angriffsflächenreduzierung sind der wirkungsvollste Einzelbaustein in diesem Beitrag — und der einzige, mit dem du dir zuverlässig den Betrieb lahmlegen kannst. Sie verbieten nicht bestimmte Programme, sondern bestimmte Verhaltensweisen: Office startet einen Kindprozess, ein Skript lädt eine ausführbare Datei nach, ein Prozess greift auf den Speicher des LSASS zu. Das Problem daran ist gleichzeitig ihr Charme: Legitime Branchenwendungen benehmen sich manchmal genauso.

Voraussetzungen, die nicht verhandelbar sind

ASR-Regeln sind eine Funktion von Microsoft Defender Antivirus und laufen nur, wenn dieser im aktiven Modus arbeitet — nicht passiv, nicht mit eingeschränkter regelmäßiger Überprüfung, nicht aus. Echtzeitschutz muss an sein, Cloud-Schutz ebenfalls. Die Plattform- und Modulversionen sollten höchstens zwei Versionen hinter dem aktuellen Stand liegen; veraltete Clients erzeugen mehr Fehlalarme. Und auf macOS oder Linux gibt es keine ASR-Regeln, auch wenn die Geräte sauber onboardet sind.

Die Modi und warum „Nicht konfiguriert“ wichtig ist

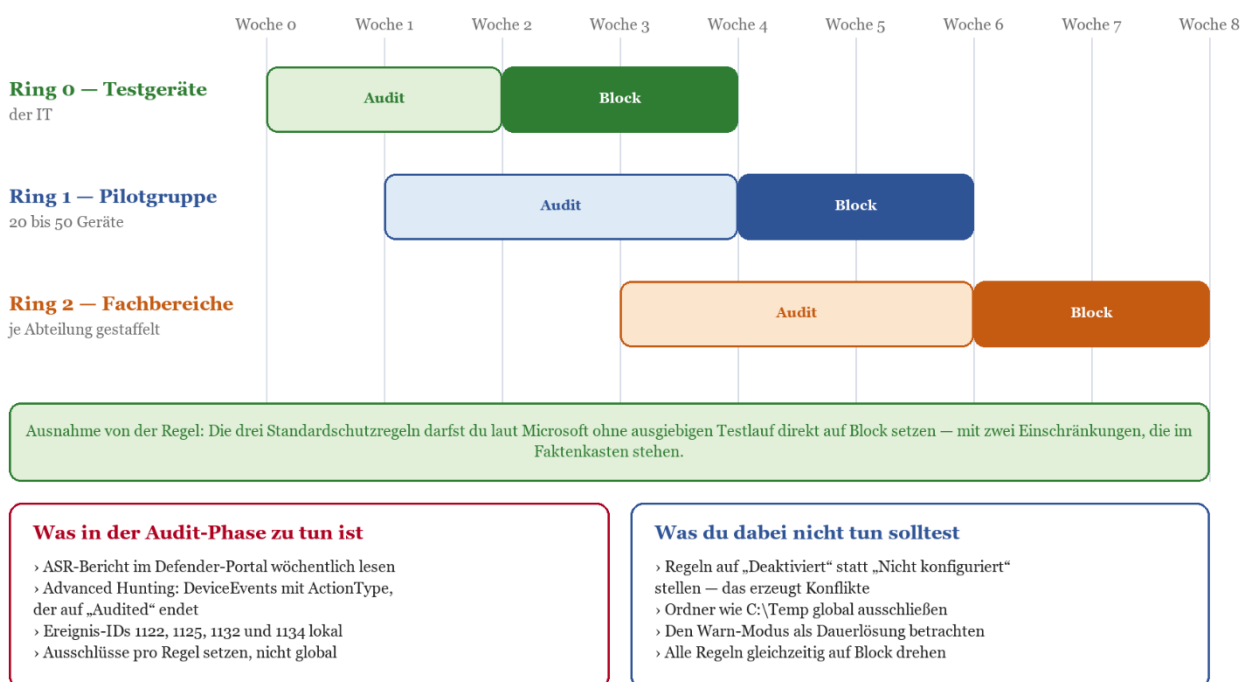
Eine Regel kennt fünf Zustände. Der Unterschied zwischen „Deaktiviert“ und „Nicht konfiguriert“ ist keine Kosmetik: „Deaktiviert“ ist eine aktive Aussage und kann mit einer zweiten Richtlinie kollidieren, die dieselbe Regel scharf stellt. „Nicht konfiguriert“ wirkt genauso, erzeugt aber keinen Konflikt. Wenn Gruppenrichtlinien und MDM dieselbe Regel unterschiedlich setzen, gewinnt standardmäßig die Gruppenrichtlinie.

Modus	Code	Was passiert	Wofür gedacht
Nicht konfiguriert	5	Regel wirkt nicht, erzeugt keinen Konflikt	der saubere Ausgangszustand
Audit	2	Regel bewertet wie im Blockmodus, greift aber nicht ein	Testphase, Ausschlüsse finden
Warn	6	Blockiert mit Umgehungsmöglichkeit für 24 Stunden	Übergangsphase mit Rückmeldung
Block	1	Regel greift durch	Zielzustand
Deaktiviert	0	Regel aus, mit Konfliktpotenzial	möglichst vermeiden

Tabelle 3: Die Regelmodi. Der Weg führt von 5 über 2 nach 1, gern mit einem Zwischenstopp bei 6.

Zum Warn-Modus gibt es eine frische Änderung, die du kennen solltest: Seit Plattformversion 4.18.26060 braucht die Schaltfläche „Entsperren“ eine Administratorfreigabe. Damit ist der Warn-Modus endgültig das, was er immer sein sollte — eine befristete Übergangslösung, kein Selbstbedienungsladen. Zwei Regeln unterstützen ihn ohnehin nicht: die LSASS-Regel und die Regel gegen Code-Injektion aus Office-Anwendungen.

ASR-Regeln ausrollen: erst Audit, dann Block, ringweise



Skizze 4: Ringweiser Ausrollplan über acht Wochen. Die Ringe überlappen bewusst.

Der Ausrollplan, der funktioniert

Beginne mit einem Ring 0 aus IT-eigenen Geräten, weil dort Fehlalarme am schnellsten erklärt sind. Ring 1 ist die eigentliche Pilotgruppe: 20 bis 50 Geräte, quer über die Abteilungen verteilt, mit ausdrücklicher Beteiligung der Bereiche, die exotische Software einsetzen. Wenn in deinem

Pilot weder Buchhaltung noch Konstruktion noch Produktion vorkommen, testest du nicht die Realität, sondern deine eigene Arbeitsumgebung. Ring 2 ist dann die Fläche, abteilungsweise gestaffelt.

In der Audit-Phase liest du den ASR-Bericht im Defender-Portal wöchentlich, ergänzt durch Advanced Hunting auf DeviceEvents mit Aktionstypen, die auf „Audited“ enden. Lokal stehen die Ereignisse unter den IDs 1122, 1125, 1132 und 1134. Aus jedem Treffer wird entweder ein Ausschluss oder die Erkenntnis, dass die Anwendung tatsächlich Unsinn treibt und der Hersteller eine Frage beantworten muss.

FAKTEN — Die sieben ASR-Regeln mit der größten Wirkung

1. Diebstahl von Anmeldeinformationen aus dem LSASS blockieren (9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2) — Standardschutzregel. Erzeugt viel Rauschen im Auditmodus, das im Blockmodus fast vollständig harmlos ist. Microsoft empfiehlt, den Auditlauf hier zu überspringen und mit wenigen Geräten direkt zu blocken. Wer LSA-Schutz und Credential Guard aktiv hat, braucht die Regel nicht.
2. Persistenz über WMI-Ereignisabonnements blockieren (e6db77e5-3df2-4cf1-b95a-636979351e5b) — Standardschutzregel gegen dateilose Persistenz. Achtung, wenn Configuration Manager im Einsatz ist: Dessen Client hängt stark an WMI, hier gehört ausführlich getestet.
3. Missbrauch anfälliger signierter Treiber blockieren (56a863a9-875e-4185-98a7-b882c64b5ce5) — Standardschutzregel gegen Bring-your-own-vulnerable-driver. Verhindert das Ablegen solcher Treiber, nicht das Laden bereits vorhandener.
4. Ausführbare Inhalte aus E-Mail-Client und Webmail blockieren (be9ba2d9-53ea-4cdc-84e5-9b1e4ee46550) — trifft den mit Abstand häufigsten Einstiegsweg: die Datei im Anhang.
5. Kindprozesse aus allen Office-Anwendungen blockieren (d4f940ab-401b-4efc-aadc-ad5f3c50688a) — die klassische Makrokette. Greift nur, wenn Office in den Programmverzeichnissen installiert ist.
6. Prozesserzeugung über PsExec und WMI-Befehle blockieren (d1e49aac-8f56-4280-b9ba-993a6d77406c) — schneidet Seitwärtsbewegung ab. Nicht in Kombination mit Configuration Manager über andere Wege aktivieren.
7. Erweiterten Schutz vor Ransomware verwenden (c1db55ab-c21a-4637-bb3f-a12568109d35) — blockiert auch Dateien ohne positiven Ruf. Blockaden an unbekannten, harmlosen Dateien lösen sich in der Regel von selbst auf, wenn der Ruf steigt.

Die Regeln 1 bis 3 sind die sogenannten Standardschutzregeln. Für sie gilt die Ausnahme: Sie dürfen laut Microsoft ohne ausgiebigen Testlauf direkt auf Block — mit den beiden oben genannten Einschränkungen. Alle anderen gehören zuerst in den Auditmodus. Als Nachrücker lohnen sich außerdem die Regel gegen Win32-API-Aufrufe aus Office-Makros, die Regel gegen Kindprozesse aus Outlook und die Regel gegen den Neustart im abgesicherten Modus, die Ransomware gern nutzt, um Schutzprodukte auszuhebeln.

WARNUNG — Ausschlüsse sind kein Werkzeug für Eilige

Ein ausgeschlossener Pfad wird nicht bewertet, nicht protokolliert und nicht gemeldet. Wer C:\Temp global ausschließt, hat die Regel faktisch abgeschaltet und merkt es nie.

Zwei Regeln beachten die Datei- und Ordnerausschlüsse von Defender Antivirus überhaupt nicht: die LSASS-Regel und die WMI-Persistenzregel. Dort helfen nur globale ASR-Ausschlüsse oder Ausschlüsse pro Regel. Prozessausschlüsse beachten dagegen alle Regeln.

Ausschlüsse pro Regel gibt es nur über Intune, die Endpunktsicherheitsrichtlinien im Defender-Portal und Gruppenrichtlinien. Nutze sie — ein globaler Ausschluss löst ein Problem und öffnet siebzehn.

Ausschlüsse greifen erst, wenn der betroffene Prozess neu startet. Ein laufender Dienst löst weiter Erkennungen aus, bis er durchgestartet wurde. Das erklärt die meisten Meldungen mit dem Betreff „Ausschluss funktioniert nicht“.

Wenn es doch passiert: Untersuchung und Isolation

Bis hierhin ging es um Prävention. Der Rest dieses Beitrags geht davon aus, dass sie an einem Dienstagvormittag nicht gereicht hat. Zwei Funktionen entscheiden dann darüber, ob aus einem Vorfall ein Zwischenfall wird oder ein Wochenende: die automatisierte Untersuchung und die Geräteisolation. Beide sind technisch schnell eingerichtet und organisatorisch anspruchsvoll.

Automatisierte Untersuchung: der Automatisierungsgrad je Gerätegruppe

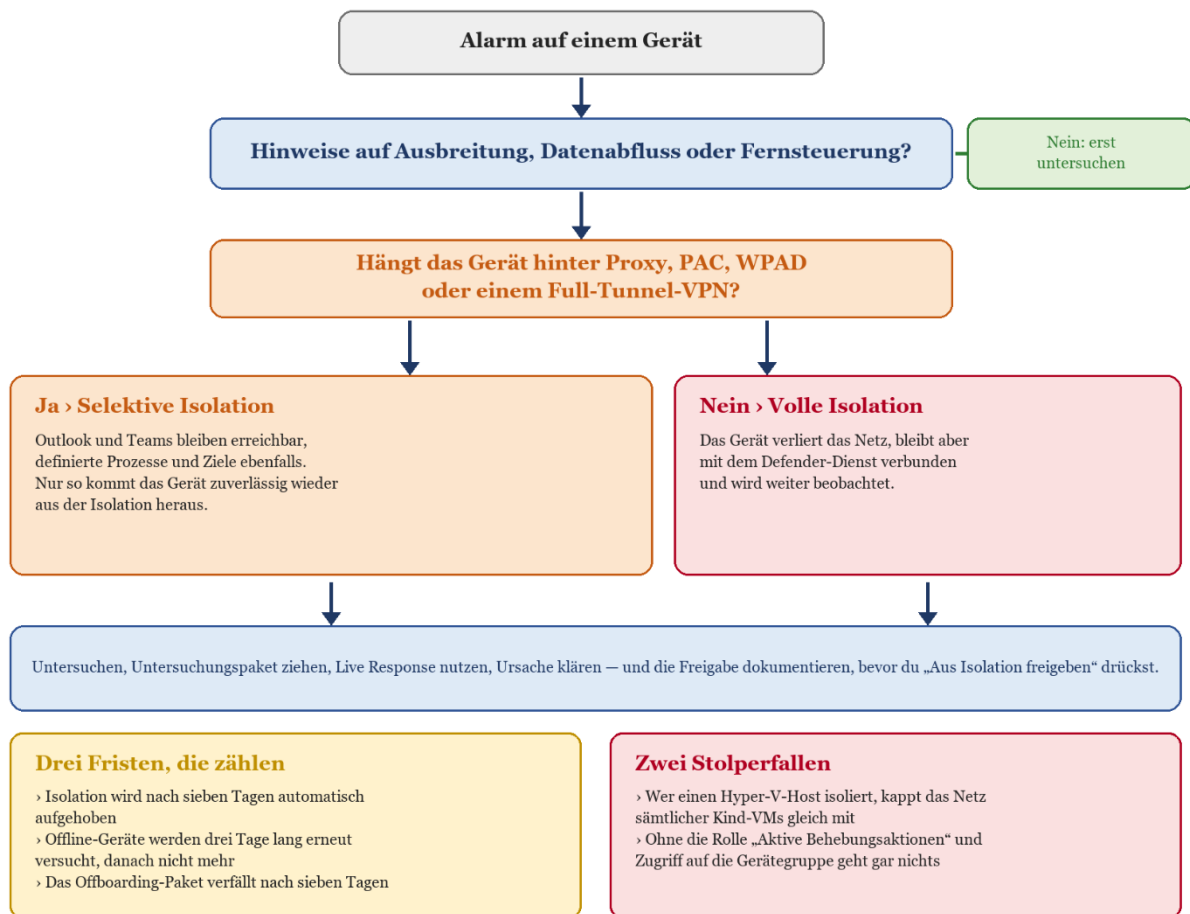
Die automatisierte Untersuchung ahmt nach, was ein Analyst tun würde: Sie sammelt Belege, bewertet Artefakte, schlägt Maßnahmen vor oder führt sie aus. Wie weit sie gehen darf, legst du im Defender-Portal je Gerätegruppe fest. Microsoft empfiehlt „Vollständig — Bedrohungen automatisch beheben“. Das ist eine gute Empfehlung für Standardarbeitsplätze und eine diskussionswürdige für Geräte, an denen ein automatisch entferntes Artefakt eine Produktionsanlage anhält.

Der pragmatische Weg: Gerätegruppen nach Kritikalität schneiden. Büroarbeitsplätze auf vollständige Automatisierung, kritische Systeme auf Genehmigung durch das Team. Für E-Mail und E-Mail-Inhalte trifft die Automatisierung ohnehin nie eigenständig Entscheidungen — dort warten alle Maßnahmen im Aktionscenter auf eine Freigabe. Die Verzahnung mit dem Postfachschutz beschreibt [Defender for Office 365: Safe Links und Safe Attachments](#).

Geräteisolation: mächtig, endlich, folgenreich

Die Isolation trennt ein Gerät vom Netz, hält aber die Verbindung zum Defender-Dienst aufrecht, damit du weiter beobachten und untersuchen kannst. Es gibt sie in zwei Ausprägungen. Die volle Isolation kappt alles außer der Dienstverbindung. Die selektive Isolation lässt definierte Prozesse und Ziele durch und kann Outlook und Microsoft Teams erreichbar halten — was den praktischen Vorteil hat, dass die betroffene Person noch erklären kann, was passiert ist.

Isolieren oder nicht: der Entscheidungsweg im Ernstfall



Skizze 5: Der Entscheidungsweg. Die Netzwerkarchitektur entscheidet über die Isolationsart, nicht der Bauchgefühlfaktor.

Vier Randbedingungen bestimmen, ob das im Ernstfall funktioniert. Erstens: In Umgebungen mit Proxykonfigurationen über PAC, WPAD oder statische Einträge kommen Geräte unter Umständen nicht mehr aus der Isolation heraus – dort ist die selektive Isolation die richtige Wahl. Zweitens: Ein Gerät hinter einem Full-Tunnel-VPN erreicht den Defender-Dienst nach der Isolation nicht mehr. Für den Defender-Verkehr gehört ein Split-Tunnel eingerichtet, und zwar bevor du ihn brauchst. Drittens: Wer einen Hyper-V-Host isoliert, nimmt sämtliche Kind-VMs mit vom Netz. Viertens: Ohne die Rolle „Aktive Behebungsaktionen“ und ohne Zugriff auf die betreffende Gerätegruppe kann niemand isolieren – und im Ernstfall ist der falsche Moment, um Rollenzuweisungen zu klären.

Dazu kommen drei Fristen, die man einmal gelesen haben sollte: Eine Isolation wird nach sieben Tagen automatisch aufgehoben. Ist das Gerät zum Zeitpunkt der Anweisung offline, versucht der Dienst die Durchsetzung drei Tage lang; danach musst du die Aktion neu auslösen. Und die automatische Isolation im Rahmen der automatischen Angriffsunterbrechung greift ausschließlich auf Endanwender-Arbeitsplätzen, die onboardet und verwaltet sind – Server bleiben außen vor.

WICHTIG – Isolation ist auch eine Organisationsfrage

Wer darf isolieren? In welchen Fällen ohne Rückfrage, in welchen mit? Wer informiert die betroffene Person, und mit welchem Wortlaut? Diese drei Fragen gehören vor den ersten Einsatz geklärt und in den [Incident-Response-Plan für Microsoft 365](#) geschrieben.

Automatische Behebung und Isolation sind Eingriffe an Arbeitsmitteln und erzeugen

personenbeziehbare Daten. In Betrieben mit Betriebsrat ist das kein Randthema, sondern der Ausgangspunkt einer Vereinbarung — siehe [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Geübt wird vorher, nicht im Ernstfall. Eine Isolation an einem freiwillig gemeldeten Testgerät dauert zehn Minuten und beantwortet mehr Fragen als drei Konzeptrunden. Wie so eine Übung aufgebaut wird, steht in [Feuerwehrrübung: Security-Notfälle im Team trainieren](#).

Was der Endpunkt nicht sieht

Defender for Endpoint ist gut in dem, was auf dem Gerät passiert. Er sieht nicht, was im Verzeichnisdienst passiert. Wenn ein Angreifer nach dem ersten Zugriff Kerberos-Tickets einsammelt, Dienstkonto missbraucht oder Berechtigungen im Active Directory verschiebt, ist das eine andere Perspektive — dafür gibt es [Defender for Identity: das Active Directory im Blick](#). Die Kombination aus beidem ist der Punkt, an dem aus einzelnen Alarmen ein zusammenhängender Vorfall wird. Für Cloud-Anwendungen und nicht genehmigte Dienste ergänzt [Defender for Cloud Apps im Mittelstand](#) das Bild.

Wenn du beides betreibst und die Alarme in ein übergreifendes Betriebsmodell überführen willst, ist die Frage nach einem SIEM nicht mehr weit. Wann sich das rechnet und wann nicht, behandelt [Microsoft Sentinel anbinden: wann es sich lohnt](#). Vorher lohnt es sich allerdings, die Benachrichtigungswege sauber aufzusetzen — dazu [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Häufige Fragen

Wir haben Microsoft 365 Business Premium. Reicht das?

Für Organisationen bis 300 Nutzer in aller Regel ja. Defender for Business enthält Next-Generation-Schutz, ASR-Funktionen, EDR und automatisierte Untersuchung. Was fehlt, ist vor allem die Ermittlungstiefe: kein Advanced Hunting mit sechs Monaten Historie, keine Threat Analytics, keine Tiefenanalyse. Solange ihr keine eigene Sicherheitsmannschaft habt, die diese Werkzeuge auch benutzen würde, ist das ein verkraftbarer Verzicht.

Müssen wir für das Onboarding Software verteilen?

Für Windows 10 und 11 nein. Der Client ist Teil des Betriebssystems, das Onboarding erfolgt über die Konfiguration aus der EDR-Richtlinie. Für macOS, Android und iOS musst du die jeweilige Anwendung tatsächlich verteilen und konfigurieren — dort gibt es kein automatisches Onboarding-Paket aus dem Connector. Für Windows und Linux gibt es inzwischen zusätzlich das Defender Deployment Tool, ein selbstaktualisierendes Hilfsprogramm für die Verteilung.

Wie lange dauert es, bis ein Gerät im Portal auftaucht?

Rechne mit 15 bis 30 Minuten nach dem Zuweisen der Richtlinie. Der Verbindungsstatus des Connectors in Intune braucht seinerseits bis zu 15 Minuten. Wenn nach einer Stunde nichts sichtbar ist, liegt das selten am Timing und meistens an der Zuweisung: Benutzergruppe statt Gerätegruppe, Gerät nicht in Intune eingeschrieben, oder eine zweite Richtlinie, die dieselben Einstellungen anders setzt.

Können wir ASR-Regeln nicht einfach alle auf Block stellen?

Technisch ja. Betrieblich ist es die zuverlässigste Methode, das Projekt zu beenden. Die drei Standardschutzregeln sind für den direkten Blockmodus vorgesehen; alle anderen gehören in den Auditmodus, bis du weißt, welche eurer Anwendungen sich verdächtig benehmen. Der Unterschied zwischen beiden Wegen sind ungefähr sechs Wochen Geduld und ungefähr sechs Monate Vertrauensverlust.

Was ist mit unserem vorhandenen Virenschutz von einem anderen Hersteller?

Dann läuft Microsoft Defender Antivirus im passiven Modus. Damit entfallen Echtzeitschutz, ASR-Regeln, Network Protection und Indikatoren. Übrig bleibt mit Plan 2 der EDR-Blockmodus, der nachträglich auf verhaltensbasierte Erkennungen reagiert. Das ist besser als nichts, aber es ist nicht der Funktionsumfang, den Microsoft in seinen Unterlagen beschreibt. Die Entscheidung für ein Parallelbetrieb-Szenario sollte eine bewusste sein, keine historische.

Brauchen wir Intune, oder geht das auch anders?

Intune ist der empfohlene und in der Praxis komfortabelste Weg, aber nicht der einzige. Es gibt Configuration Manager, Gruppenrichtlinien, lokale Skripte und die Sicherheitseinstellungsverwaltung von Defender for Endpoint für Geräte, die nicht in Intune eingeschrieben sind. Für ASR-Regeln mit Ausschlüssen pro Regel und für die zentrale Auswertung willst du allerdings eine der modernen Verwaltungsoberflächen — Gruppenrichtlinien und Manipulationsschutz vertragen sich schlecht.

Wie hängt das mit Conditional Access zusammen?

Über die Compliance-Bewertung. Wenn du die Windows-Auswertung im Connector einschaltest, liefert Defender for Endpoint eine Risikostufe je Gerät. Eine Compliance-Richtlinie mit der Einstellung „Gerät muss auf oder unter der Risikobewertung liegen“ macht daraus einen Konformitätsstatus, und eine Conditional-Access-Richtlinie macht daraus eine Zugriffsentscheidung. Microsoft empfiehlt die Schwelle „Niedrig“ als Ausgangspunkt. Wie eine brauchbare Richtlinienbasis aussieht, steht in [Conditional Access: Baselines, die nicht nerven](#).

Was passiert beim Offboarding?

Das Gerät sendet keine neuen Erkennungs-, Schwachstellen- und Sicherheitsdaten mehr. Vorhandene Daten bleiben bis zum Ablauf der Aufbewahrungsfrist im Portal, das Geräteprofil selbst bleibt bis zu 180 Tage in der Inventur stehen. Wichtig: Das Offboarding-Paket verfällt sieben Tage nach dem Download, und Onboarding- und Offboarding-Richtlinien dürfen nie gleichzeitig auf dasselbe Gerät wirken.

Wie messen wir, ob das etwas gebracht hat?

Nicht am Secure Score allein — der ist ein Kompass, kein Zeugnis. Brauchbare Kennzahlen sind die Onboarding-Quote gegen die Anzahl verwalteter Geräte, die Zahl der ASR-Erkennungen je hundert Geräte im Zeitverlauf, die Zeit von Alarm bis erster Reaktion und der Anteil der Geräte mit aktuellem Plattformstand. Wie du daraus etwas machst, das eine Geschäftsführung lesen will, beschreibt [Security-Reporting für die Geschäftsführung](#). Zur Einordnung des Scores selbst siehe [Secure Score: sinnvoll nutzen statt Punktejagd](#).

Fazit

Das Onboarding von Defender for Endpoint über Intune ist ein Nachmittag Arbeit. Der Connector, die EDR-Richtlinie, eine Pilotgruppe, ein Detection Test — fertig. Alles, was danach kommt, ist kein Installationsprojekt mehr, sondern eine Reihe von Entscheidungen: wie scharf der Cloud-Schutz eingestellt wird, wann Network Protection von Audit auf Block wechselt, welche ASR-Regeln in welchem Ring landen, wie weit die Automatisierung gehen darf und wer im Ernstfall den Isolationsknopf drücken darf.

Genau diese Entscheidungen sind der Grund, warum Defender-Projekte scheitern oder gelingen — nicht die Technik. Wer alle Regeln gleichzeitig scharf stellt, produziert innerhalb von zwei Tagen so viel Widerstand, dass die nächste Sicherheitsmaßnahme im Haus grundsätzlich als Zumutung gilt. Wer die Reihenfolge einhält, hat nach acht Wochen einen Schutz, den niemand bemerkt, und Zahlen, mit denen sich argumentieren lässt.

Ein realistischer Zeitplan sieht so aus: Woche 1 das Onboarding samt Manipulationsschutz und Cloud-Schutz. Woche 2 bis 4 Network Protection im Auditmodus und die drei Standardschutzregeln im Blockmodus. Woche 3 bis 8 die übrigen ASR-Regeln ringweise von Audit nach Block. Parallel dazu die organisatorischen Fragen: Automatisierungsgrad, Isolationsbefugnis, Betriebsvereinbarung. Danach ist es Betrieb — und Betrieb heißt, den ASR-Bericht auch dann zu lesen, wenn gerade nichts brennt.

Was dieser Beitrag nicht ersetzt, ist die Vorsorge für den Fall, dass alles davon zu spät kommt. Wiederherstellungsfähigkeit ist eine eigene Disziplin, und die steht in [Ransomware-Vorsorge in Microsoft 365](#). Wie ein konkreter Vorfall abläuft, wenn niemand vorbereitet ist, zeigt das [Dossier TerminalFix und der Berlin-Hack](#). Und wenn dir bei der Auslegung für deine Umgebung jemand zur Seite stehen soll, ist die [Microsoft 365 Security Beratung](#) der passende Einstieg.

WEITER — Passende Beiträge aus dieser Reihe

- › [Microsoft 365 Security](#) — die Übersicht über alle Bausteine
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — die Grundlagen, die vor dem Endpunkt kommen
- › [Defender for Identity: das Active Directory im Blick](#) — die Perspektive, die Defender for Endpoint fehlt
- › [Dossier TerminalFix und der Berlin-Hack](#) — der Klickpfad A1 und A2 im Detail, an einem realen Fall
- › [Ransomware-Vorsorge in Microsoft 365](#) — Vorsorge für den Fall, dass die Prävention nicht reicht
- › [Incident-Response-Plan für Microsoft 365](#) — wer im Ernstfall was entscheidet
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — die mitbestimmungspflichtigen Anteile
- › [Phishing-Vorfall: die ersten 60 Minuten](#) — die ersten 60 Minuten, wenn es doch geklappt hat
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) — wo der Endpunkt im Gesamtbild steht
- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — welche dieser Maßnahmen regulatorisch zählen
- › [Kompromittiertes Konto erkennen und aufräumen](#) — wenn nicht das Gerät, sondern die Identität betroffen ist
- › [Microsoft 365 Security Beratung](#) — Unterstützung bei Auslegung und Rollout
- › [Schulung Microsoft 365 Security](#) — wenn das Team es selbst können soll