

Microsoft Sentinel anbinden: wann es sich lohnt

Es gibt in Microsoft-365-Projekten einen Moment, der sich mit erstaunlicher Zuverlässigkeit wiederholt. Jemand aus der Geschäftsführung war auf einer Veranstaltung, hat dort das Wort SIEM gehört, und fragt am Montag, ob „wir das auch haben“. Die IT antwortet, man habe ja Defender. Die Antwort darauf lautet regelmäßig: „Reicht das denn?“ Und genau da fängt das Problem an — nicht weil die Frage falsch wäre, sondern weil sie ohne Zahlen nicht zu beantworten ist.

Microsoft Sentinel ist das SIEM- und SOAR-Produkt von Microsoft. Es ist gut, es ist tief in Microsoft 365 integriert, und es kostet Geld nach Datenvolumen. Genau diese Kombination sorgt dafür, dass es in manchen Organisationen die beste Investition des Jahres ist und in anderen ein sehr elegant gestaltetes Archiv, in das nie jemand hineinschaut. Dieser Beitrag sortiert, wann welcher Fall vorliegt.

Wir schauen uns an, was Defender XDR allein schon leistet, wo genau die Grenzen liegen, was die Anbindung kostet, was nichts kostet — und wir ziehen am Ende eine unbequeme Linie. Denn die ehrlichste Beratung zu Sentinel lautet in einer beachtlichen Zahl von Fällen: noch nicht. Der Beitrag gehört zur Serie [Microsoft 365 Security](#), in der wir das Thema Schritt für Schritt durchgehen.

FAKTEN · Die harten Eckdaten in einem Absatz

Aufbewahrung: Advanced Hunting in Defender XDR hält Rohdaten standardmäßig 30 Tage vor. Ein Sentinel-Workspace bringt die ersten 90 Tage Aufbewahrung ohne Zusatzkosten mit und lässt sich darüber hinaus verlängern.

Kostenlos: Azure Activity Logs, Office-365-Audit-Logs (SharePoint, Exchange, Teams) sowie sämtliche Security Alerts und Incidents aus Defender XDR, Defender for Endpoint, Identity, Office 365, Cloud Apps und Defender for Cloud fließen ohne Ingestion-Kosten in Sentinel.

Kostenpflichtig: die Roh Tabellen des Advanced Hunting, die Entra-ID-Sign-in- und Audit-Logs sowie alles, was nicht von Microsoft kommt.

Testphase: beim Aktivieren auf einem Log-Analytics-Workspace sind 31 Tage lang die ersten 10 GB pro Tag im Analytics-Tier frei.

Terminalsache: nach dem 31. März 2027 wird Sentinel im Azure-Portal nicht mehr unterstützt und ausschließlich im Microsoft Defender Portal betrieben.

Was Defender XDR allein leistet — und wo die Luft dünn wird

Bevor wir über Sentinel reden, muss klar sein, was du ohne Sentinel bereits hast. Wer diesen Schritt überspringt, kauft ein SIEM, um Probleme zu lösen, die er schon gelöst hat, und bezahlt dafür pro Gigabyte.

Der Funktionsumfang ohne Zusatzprodukt

Defender XDR ist kein Sammelbecken für Alarme, sondern eine Korrelationsmaschine. Sie zieht Signale aus [Defender for Endpoint: Onboarding ohne Drama](#), [Defender for Identity: das Active Directory im Blick](#), [Defender for Office 365: Safe Links und Safe Attachments](#) und [Defender for](#)

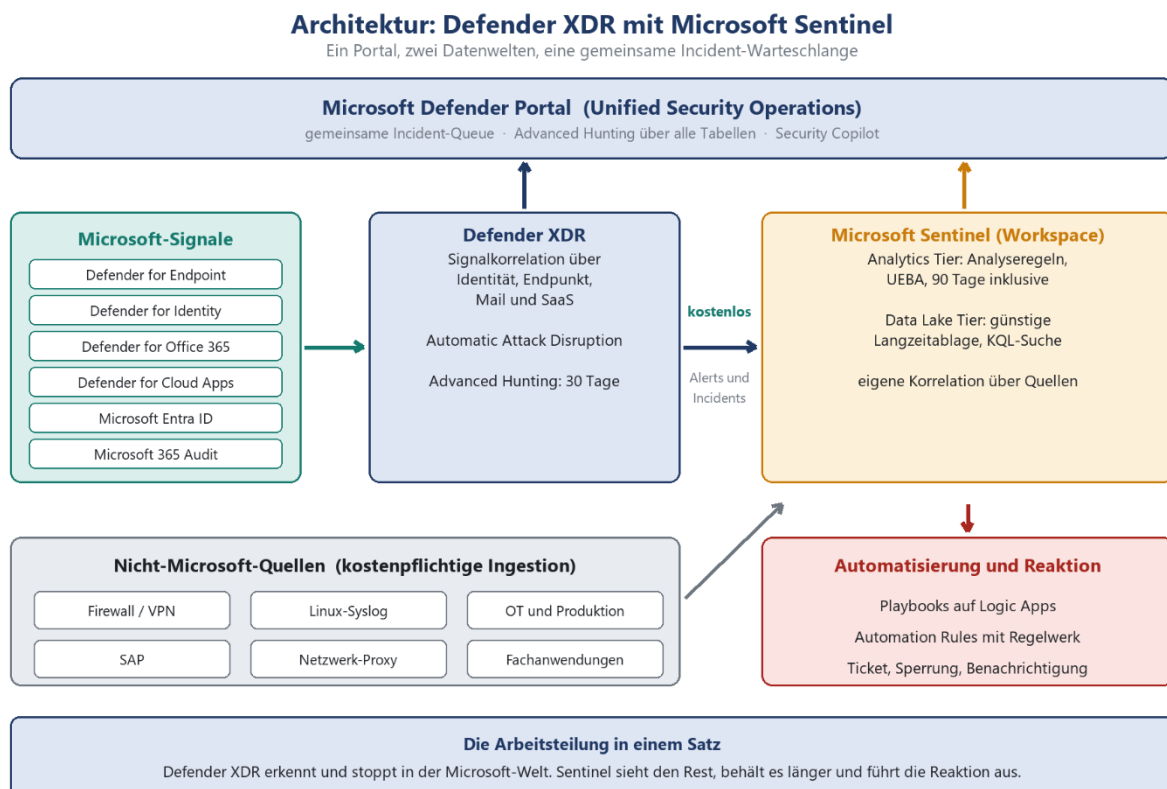
Cloud Apps im Mittelstand zusammen, verknüpft sie zu einem einzigen Incident und ordnet Entitäten wie Konten, Geräte, Postfächer und Dateien einander zu. Wenn ein Phishing-Klick auf einem Laptop zu einem Token-Diebstahl und anschließend zu einer verdächtigen Postfachregel führt, siehst du das als einen Vorfall — nicht als drei unabhängige Meldungen in drei Konsolen.

Dazu kommt Automatic Attack Disruption: Microsoft greift bei bestimmten, mit hoher Konfidenz erkannten Angriffsmustern selbst ein, isoliert Geräte oder sperrt Konten, bevor ein Mensch überhaupt die Meldung gelesen hat. Und das Advanced Hunting erlaubt dir, mit KQL durch die Rohdaten aller angebundenen Defender-Dienste zu suchen. Das ist, ehrlich gesagt, für viele Organisationen bereits mehr Sicherheitsfunktion, als sie personell auswerten können.

Die vier Wände, an die du irgendwann stößt

Defender XDR endet dort, wo Microsoft aufhört. Das ist keine Kritik, das ist Produktdesign. Konkret sind es vier Grenzen, und du solltest wissen, welche davon dich tatsächlich betrifft:

- **Aufbewahrung.** Advanced-Hunting-Daten stehen 30 Tage zur Verfügung. Ein Angriff, der im März begann und im Juni auffällt, ist forensisch nur noch teilweise rekonstruierbar.
- **Fremdquellen.** Die Firewall, das VPN-Gateway, der Linux-Server im Rechenzentrum, die Maschinensteuerung in der Fertigung, das SAP-System — alles unsichtbar für Defender XDR.
- **Eigene Korrelation.** Du kannst in Defender XDR eigene Erkennungsregeln bauen, aber nur über Daten, die Defender selbst hält. Eine Regel, die einen Entra-Sign-in mit einem Firewall-Log verknüpft, ist dort schlicht nicht formulierbar.
- **Automatisierung.** Die eingebauten Reaktionen sind gut, aber vorgegeben. Ein Ticket in deinem Servicedesk anlegen, eine Nachricht in einen Teams-Kanal schreiben, eine Anreicherung aus einer externen Datenbank ziehen — dafür fehlt die Werkbank.



Skizze 1: Defender XDR liefert Korrelation und Reaktion für die Microsoft-Welt. Sentinel ergänzt Fremdquellen, Aufbewahrung und frei gestaltbare Automatisierung — sichtbar bleibt beides im selben Portal.

Das Unified Portal nimmt der Frage die Schärfe

Ein Argument, das früher gegen Sentinel sprach, ist inzwischen weggefallen: der Portalbruch. Im Microsoft Defender Portal laufen Defender XDR und Sentinel in einer gemeinsamen Oberfläche zusammen — eine Incident-Warteschlange, ein Hunting-Fenster über beide Datenbestände, eine Entitätsseite. Wer heute anbindet, zwingt sein Team nicht mehr zum Konsolen-Pingpong.

Das hat allerdings auch eine Kehrseite, die selten jemand ausspricht: Die Bedienoberfläche fühlt sich danach so an, als hätte man ein SOC. Hat man aber nicht. Ein Portal ist kein Prozess, und eine Incident-Queue, die niemand öffnet, ist ein besonders teures Stillleben.

Fähigkeit	Defender XDR allein	Mit Sentinel angebunden
Korrelation Microsoft-Signale	vollständig, automatisch	unverändert, zusätzlich eigene Regeln
Nicht-Microsoft-Quellen	nicht möglich	über 350 Konnektoren, Syslog, CEF, API
Aufbewahrung Rohdaten	30 Tage	90 Tage inklusive, darüber hinaus verlängerbar
Langzeitablege	nicht vorgesehen	Data-Lake-Tier, Jahre statt Wochen
Eigene Erkennungsregeln	nur auf Defender-Tabellen	über alle angebundenen Quellen hinweg
Verhaltensanalyse (UEBA)	produktintern	quellenübergreifend, eigene Baselines
Automatisierung	vorgegebene Aktionen	Playbooks mit Logic Apps, frei baubar
Threat Intelligence	Microsoft-Feeds	zusätzlich eigene und externe Feeds
Auswertung und Reporting	feste Berichte	Workbooks, frei gestaltbar
Kosten	in der Lizenz enthalten	nach Datenvolumen, planbar aber real

TIPP • Erst zählen, dann kaufen

Bevor du über eine Anbindung entscheidest, beantworte drei Fragen schriftlich: Wer schaut werktäglich in die Incident-Queue? Wie viele Alarme kamen in den letzten drei Monaten, und was ist mit ihnen passiert? Welche Datenquelle außerhalb von Microsoft hättest du beim letzten Vorfall gebraucht?

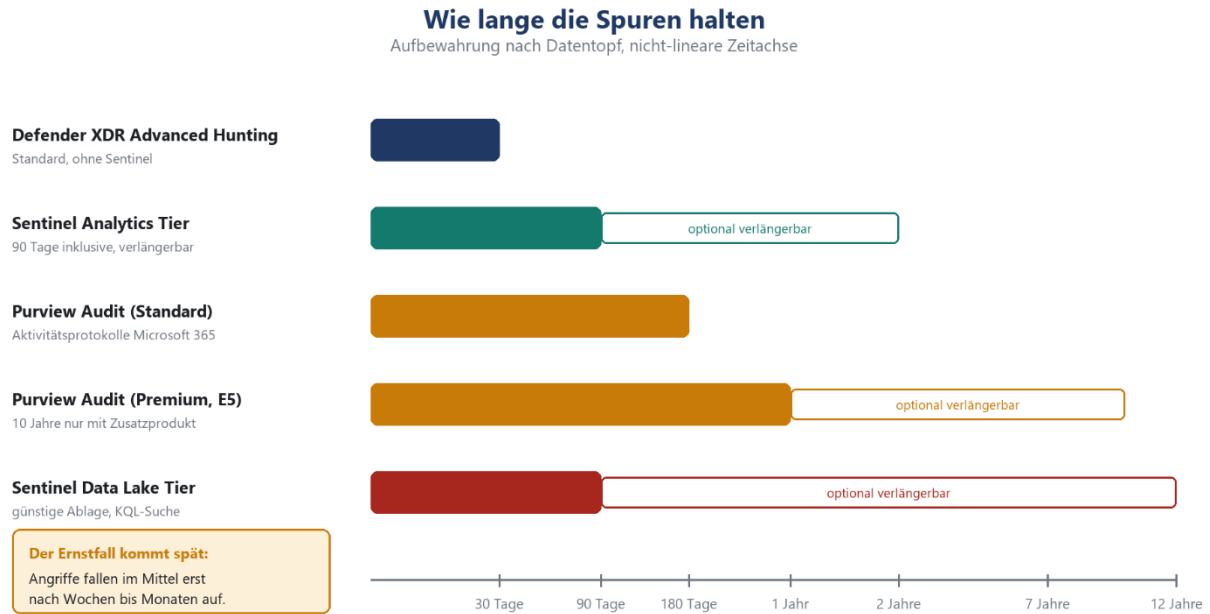
Wenn du die erste Frage nicht mit einem Namen beantworten kannst, ist Sentinel nicht dein nächster Schritt. Dann sind es [Alert Policies und Benachrichtigungen richtig aufsetzen](#) und eine klare Zuständigkeit.

Aufbewahrung: die Frage, die dich im Ernstfall einholt

Die Aufbewahrungsdauer ist das Argument, das in Beratungsgesprächen am häufigsten unterschätzt und im Vorfall am schmerzhaftesten nachgereicht wird. Der Grund ist einfache Statistik: Angriffe werden selten am Tag des Erstzugriffs entdeckt. Zwischen dem ersten kompromittierten Konto und dem Moment, in dem jemand stutzig wird, liegen in der Praxis Wochen bis Monate.

Und dann kommt die Frage, die jede forensische Untersuchung eröffnet: Seit wann läuft das? Wenn die Antwort lautet „unsere Daten reichen 30 Tage zurück“, dann ist die ehrliche Übersetzung: Wir wissen es nicht, und wir werden es nie erfahren. Das ist kein technisches Detail,

das ist die Differenz zwischen einem abgeschlossenen Vorfall und einer dauerhaften Unsicherheit darüber, ob der Angreifer noch irgendwo sitzt.



Skizze 2: Verschiedene Datentöpfe, verschiedene Uhren. Wer nur auf Defender XDR schaut, sieht 30 Tage — die Audit-Protokolle laufen deutlich länger, die Telemetrie nicht.

Was wo wie lange liegt

Wichtig ist die Unterscheidung zwischen Aktivitätsprotokollen und Sicherheitstelemetrie. Die Audit-Protokolle aus Microsoft 365 liegen bei Purview Audit im Standard 180 Tage, mit E5-Lizenzierung ein Jahr, und mit einem Zusatzprodukt bis zu zehn Jahre. Die eigentliche Sicherheitstelemetrie — welcher Prozess wurde auf welchem Endpunkt gestartet, welche Netzwerkverbindung wurde aufgebaut — hält deutlich kürzer. Genau die brauchst du aber, um einen Angriff nachzuvollziehen.

Datentopf	Standarddauer	Verlängerbar auf	Wofür du ihn brauchst
Defender XDR Advanced Hunting	30 Tage	90 Tage im Analytics-Tier	Rekonstruktion des Angriffsverlaufs
Purview Audit (Standard)	180 Tage	—	Wer hat wann welche Datei geöffnet
Purview Audit (Premium, E5)	1 Jahr	10 Jahre mit Add-on	Nachweise gegenüber Aufsicht und Gericht
Entra-ID-Anmeldeprotokolle	30 Tage im Portal	beliebig über Sentinel	Kontoübernahmen, Anmeldemuster
Sentinel Analytics-Tier	90 Tage inklusive	kostenpflichtig darüber	aktive Erkennung und Untersuchung
Sentinel Data-Lake-Tier	nach Konfiguration	Jahre	Nachweispflichten, späte Hunts

WARNUNG · Der teuerste Satz nach einem Vorfall

„Die Logs sind weg.“ Diesen Satz wirst du gegenüber einem Versicherer, einer Aufsichtsbehörde oder einem Kunden nur ungern sagen wollen. Bei einer Meldepflicht nach [NIS2 aus Security-Sicht](#):

technische Maßnahmen in M365 oder bei einem Datenschutzvorfall musst du Umfang und Zeitraum der Betroffenheit benennen können. Ohne Daten benennst du gar nichts — und im Zweifel wird zu deinen Lasten angenommen, dass alles betroffen war.

Wie ein realer Fall aussieht, wenn Aufbewahrung und Reaktionsfähigkeit auseinanderfallen, zeigt das Dossier TerminalFix und der Berlin-Hack.

Aufbewahrung ist nicht gleich Auswertbarkeit

Ein Denkfehler, der Budget verbrennt: Daten aufzubewahren und Daten auswerten zu können, sind zwei verschiedene Produkte. Im Analytics-Tier laufen Regeln, die Suche ist interaktiv, die Daten sind Teil deines Hunting-Alltags. Im Data-Lake-Tier liegen sie günstig, sind per KQL durchsuchbar — aber es feuert dort keine Regel. Wer alles in den Lake schiebt, hat ein sehr preiswertes Archiv und keine Erkennung. Wer alles im Analytics-Tier hält, hat eine hervorragende Erkennung und eine Rechnung, die im Controlling für Rückfragen sorgt.

Was Sentinel kostet — und was tatsächlich nichts kostet

Sentinel wird nach der Menge an Daten abgerechnet, die du hineinkippst, und nach der Ebene, auf der sie landen. Das ist die eine Hälfte der Wahrheit. Die andere: Ein erheblicher Teil dessen, was du aus Microsoft 365 anbinden willst, kostet keinen Cent an Ingestion. Genau dieser Umstand macht den Einstieg in vielen Umgebungen erstaunlich günstig — und die Ausbaustufe erstaunlich teuer.

Die kostenlosen Konnektoren

Microsoft stellt eine ganze Reihe von Datenquellen kostenfrei bereit. Die Liste ist überschaubar, aber inhaltlich stark: Azure Activity Logs, die Office-365-Audit-Logs mit SharePoint-, Exchange- und Teams-Aktivität, die Sentinel-eigene Health-Telemetrie sowie sämtliche Security Alerts und SecurityIncident-Einträge aus dem Defender-Umfeld. Damit hast du die Zusammenführung der Alarme, die vollständige Historie, wer welche Datei angefasst hat, und die Basis für Reporting — ohne Ingestion-Kosten.

Die Falle liegt eine Ebene tiefer. Frei sind die **Alarme**, nicht die Rohdaten. Die Advanced-Hunting-Tabellen von Defender for Endpoint, Identity, Office 365 und Cloud Apps sind kostenpflichtig, ebenso die Entra-ID-Anmeldeprotokolle und die Shadow-IT-Erkennung aus Defender for Cloud Apps. Und ausgerechnet die Anmeldeprotokolle sind die Quelle, die man in fast jedem Fall haben will.

Datenquelle	Ingestion	Praktischer Nutzen
Azure Activity Logs	kostenlos	Änderungen an Azure-Ressourcen nachvollziehen
Office-365-Audit (SharePoint, Exchange, Teams)	kostenlos	Datenzugriffe, Postfachregeln, Freigaben
Security Alerts aus Defender XDR	kostenlos	gebündelte Alarmlage, Incident-Historie
SecurityIncident aus Defender XDR	kostenlos	Auswertung über Zeit, Reporting
Alerts aus Defender for Cloud / Cloud Apps	kostenlos	Cloud-Posture und SaaS-Auffälligkeiten
Health-Telemetrie von Sentinel	kostenlos	erkennen, wenn ein Konnektor stillsteht

Entra-ID Sign-in- und Audit-Logs	kostenpflichtig	Kontoübernahmen, Anmeldeanomalien
Advanced-Hunting-Rohtabellen	kostenpflichtig	tiefe Forensik, eigene Erkennungen
Firewall, Proxy, VPN, Syslog, CEF	kostenpflichtig	der Weg hinein und hinaus
Fachanwendungen und OT	kostenpflichtig	das, was dein Geschäft wirklich ausmacht

Das E5-Datenkontingent — der stille Rabatt

Wer Microsoft 365 E5 oder die entsprechenden A5-, F5- und G5-Varianten lizenziert hat, bekommt zusätzlich ein Datenkontingent für Sentinel: bis zu 5 MB pro Nutzer und Tag für ausgewählte Microsoft-365-Daten. Angerechnet werden genau die Quellen, die sonst weh tun — Entra-ID-Anmelde- und Audit-Logs, die Shadow-IT-Discovery, Informationsschutz-Protokolle und Advanced-Hunting-Daten. Der Abzug erfolgt automatisch auf der Rechnung.

Rechne das einmal durch, es lohnt sich: Bei 500 E5-Nutzern sind das 2,5 GB pro Tag, die für genau die interessanten Microsoft-Quellen zur Verfügung stehen. In vielen mittelständischen Umgebungen deckt das den kompletten Microsoft-365-Anteil ab. Die Rechnung entsteht dann erst durch das, was du zusätzlich anbindest — und das ist eine Entscheidung, die du triffst, keine, die dir passiert.

FAKTEN • Wo das Geld tatsächlich hingeht

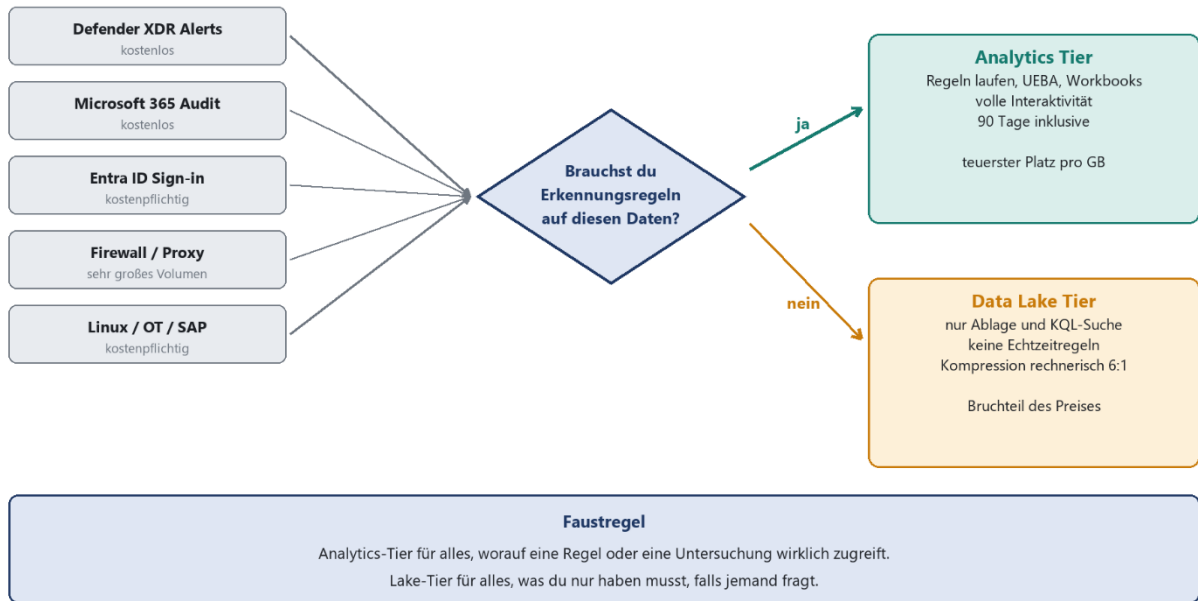
Analytics-Tier: Bezahlung pro Gigabyte, entweder nach Verbrauch oder über Commitment-Stufen, die bei 100 GB pro Tag beginnen und gegenüber der Verbrauchsabrechnung deutlich günstiger sind. Eine Stufe lässt sich jederzeit erhöhen, senken darfst du frühestens nach 31 Tagen.

Data-Lake-Tier: getrennte Zähler für Ingestion, Verarbeitung, Speicherung und Abfrage. Die Speicherung wird mit einer rechnerischen Kompression von 6:1 abgerechnet — aus 600 GB Rohdaten werden 100 GB in der Abrechnung. Abfragen kosten nach gescanntem Volumen, was die Kunst der präzisen KQL-Abfrage plötzlich zu einer betriebswirtschaftlichen Disziplin macht.

Nebenkosten: Playbooks laufen auf Logic Apps und werden dort separat abgerechnet, ebenso Azure Functions, die manche Konnektoren im Hintergrund nutzen. Kleine Beträge, aber sie stehen auf der Rechnung.

Tiering: nicht jedes Log verdient den teuren Platz

Vor der Anbindung entscheiden, was gejagt und was nur aufbewahrt wird



Skizze 3: Die Tiering-Entscheidung fällt pro Tabelle und ist der größte Kostenhebel, den du hast — deutlich größer als jede Verhandlung über den Gigabyte-Preis.

Volumen schätzen, bevor du unterschreibst

Der verlässlichste Weg zur Kostenschätzung ist nicht die Preisliste, sondern die Messung. Aktiviere Sentinel auf einem Workspace, nutze die 31 Tage mit 10 GB täglich im Analytics-Tier, binde zunächst nur die kostenlosen Quellen an und schalte dann eine kostenpflichtige Quelle nach der anderen dazu. Nach vier Wochen hast du echte Zahlen aus deiner Umgebung statt einer Hochrechnung aus dem Datenblatt eines fremden Unternehmens.

TIPP · Die drei Hebel, die wirklich wirken

- 1. Tiering.** Firewall-, Proxy- und Netflow-Daten haben ein enormes Volumen und einen geringen Erkennungswert pro Zeile. Sie gehören in den Lake, nicht in die Analytics-Ebene.
- 2. Transformation beim Eingang.** Felder verwerfen, die du nie abfragst. Ein CEF-Datenstrom schleppt oft mehr mit, als deine Regeln je anfassen.
- 3. Kein Doppel-Sammeln.** Wenn ein Server sowohl über den Defender-Agenten als auch über Syslog meldet, bezahlst du zweimal für dieselbe Information — und verwirrst nebenbei deine Regeln.

Korrelation und Automatisierung: der eigentliche Mehrwert

Wenn Sentinel sich lohnt, dann selten wegen der Aufbewahrung allein. Der Grund, aus dem Organisationen die Anbindung hinterher nicht bereuen, ist ein anderer: Sie können zum ersten Mal Fragen stellen, die über die Grenzen einzelner Produkte hinausgehen.

Fragen, die vorher nicht stellbar waren

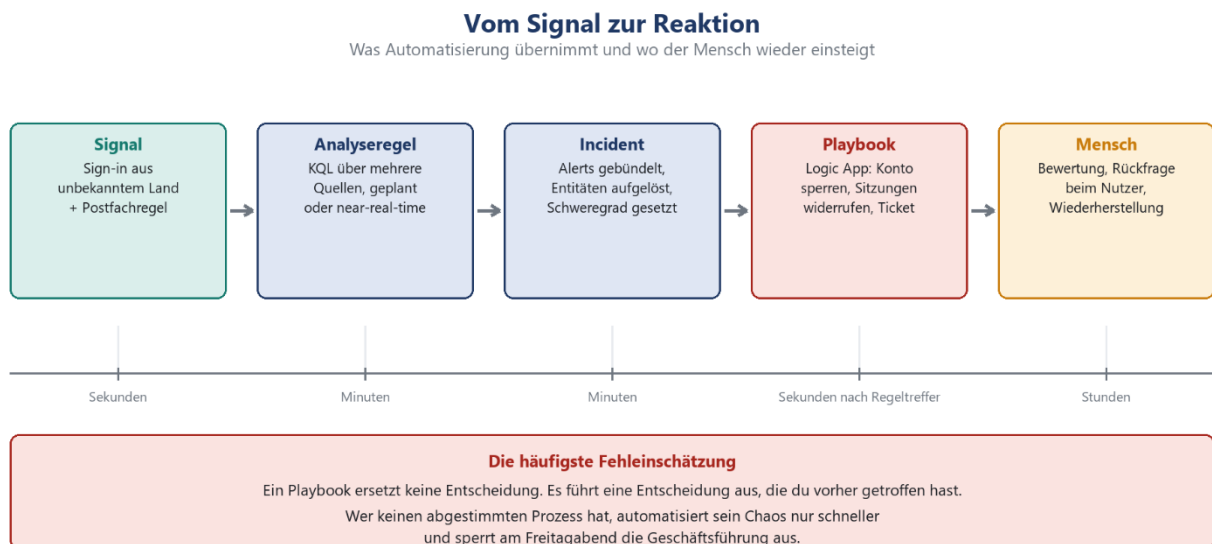
Ein paar Beispiele aus realen Projekten, damit es nicht abstrakt bleibt. Welche Konten haben sich in Entra ID angemeldet, während gleichzeitig ihre VPN-Sitzung aus einem anderen Land aktiv

war? Welcher Endpunkt hat eine Verbindung zu einer Domäne aufgebaut, die eine Stunde vorher in einer Phishing-Mail auftauchte, die Defender for Office 365 gemeldet hat? Welcher Benutzer hat sich in der Fachanwendung ein Recht gegeben, das er in Entra ID gar nicht haben dürfte?

Keine dieser Fragen ist mit Defender XDR allein zu beantworten, weil jeweils mindestens eine Datenquelle außerhalb liegt. Und das ist der Punkt, an dem die Kostenrechnung kippt: Wenn dein Angriffsflächenrisiko wesentlich außerhalb der Microsoft-Welt liegt — Produktion, Fernwartung, ein historisch gewachsenes Rechenzentrum, siehe auch [Kompetenzbereich Kerberos](#) für die Altlasten im Verzeichnisdienst — dann liefert Sentinel Erkenntnis, die du sonst nirgends bekommst.

Playbooks: Automatisierung mit Bremse

Die Automatisierung in Sentinel läuft über Playbooks auf Basis von Logic Apps. Du baust dir damit die Kette, die dein Prozess ohnehin vorsieht: Konto sperren, Sitzungen widerrufen, Ticket im Servicedesk anlegen, Nachricht in den Security-Kanal, Anreicherung aus einer Threat-Intelligence-Quelle. Automation Rules entscheiden davor, welche Incidents überhaupt in welches Playbook laufen und welche automatisch geschlossen werden dürfen.



Skizze 4: Automatisierung verkürzt die Zeit zwischen Signal und Reaktion. Sie verkürzt nicht die Zeit, die du für eine Entscheidung brauchst — die musst du vorher treffen.

WICHTIG · Automatisiere nur, was du entschieden hast

Jedes Playbook mit einer eingreifenden Aktion braucht eine dokumentierte Freigabe: Wer darf ein Konto sperren, unter welchen Bedingungen, und wie kommt der Betroffene wieder hinein? Ohne diese Festlegung baust du dir eine Maschine, die am Freitag um 22 Uhr die falsche Person aussperrt und niemanden findet, der sie wieder hereinlässt. Der passende Rahmen dafür ist ein [Incident-Response-Plan für Microsoft 365](#).

Beginne mit Playbooks, die nur informieren und anreichern. Eingreifende Aktionen kommen erst dazu, wenn der manuelle Ablauf mehrfach funktioniert hat — geübt zum Beispiel in einer [Feuerwehrübung: Security-Notfälle im Team trainieren](#).

Und die Mitbestimmung sitzt mit am Tisch

Sentinel korreliert Daten über Systemgrenzen hinweg und speichert sie länger. Beides sind Merkmale, die eine Anlage zur Verhaltens- und Leistungskontrolle kennzeichnen können. Wer die Anbindung technisch sauber baut und dabei den Betriebsrat übergeht, hat ein funktionierendes SIEM und ein Beschäftigungsverbot dafür. Was genau mitbestimmungspflichtig ist und wie eine tragfähige Betriebsvereinbarung aussieht, steht in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — das gehört in die Projektplanung, nicht in die Abnahme.

Praktisch heißt das: Zweckbindung schriftlich festhalten, Aufbewahrungsfristen je Datenart begründen, Zugriffsrechte auf den Workspace eng führen und ein Vier-Augen-Prinzip für Auswertungen mit Personenbezug vorsehen. Das ist zusätzlicher Aufwand — aber deutlich weniger als eine nachträgliche Abschaltung. Die Verzahnung mit Klassifizierung und Aufbewahrung im [Kompetenzbereich Microsoft Purview](#) lohnt sich hier besonders.

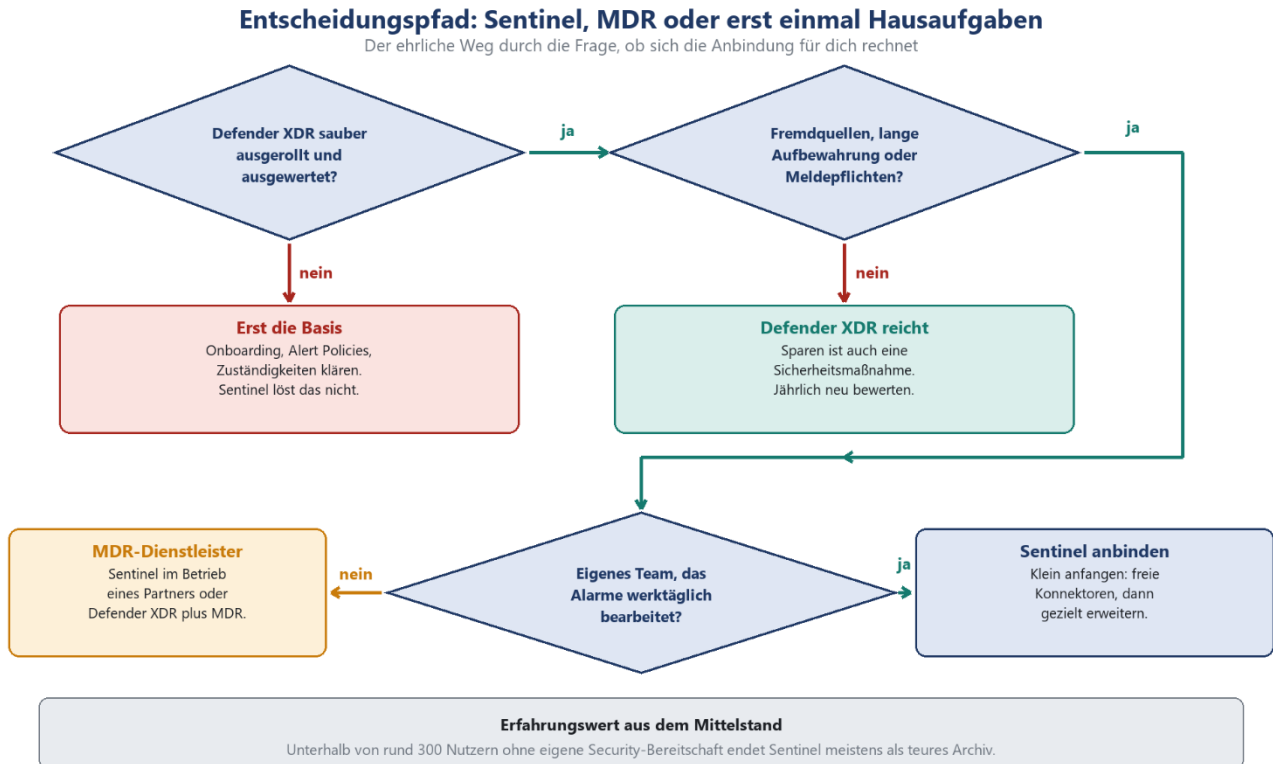
Die ehrliche Grenze: wann Sentinel dein Problem nicht löst

Jetzt der Teil, den Vertriebspräsentationen auslassen. Sentinel ist ein Werkzeug für Menschen, die damit arbeiten. Ohne diese Menschen ist es eine Datenbank mit Abonnement.

Unter etwa 300 Nutzern ohne eigenes SOC: selten sinnvoll

Diese Zahl ist keine Naturkonstante, sondern ein Erfahrungswert, und sie hängt weniger an der Nutzerzahl als an dem, was dahinter steht. Unterhalb von rund 300 Nutzern gibt es in der Regel keine Person, deren Aufgabe die Bearbeitung von Sicherheitsalarmen ist. Es gibt einen IT-Verantwortlichen, der auch für die Telefonanlage, die Warenwirtschaft und den Drucker im dritten Stock zuständig ist. Diese Person wird die Sentinel-Konsole in den ersten drei Wochen täglich öffnen, dann wöchentlich, dann wenn etwas passiert ist.

Und genau darin liegt das eigentliche Risiko: Ein SIEM erzeugt eine Sicherheitsvermutung. Man hat ja etwas gekauft, es steht im Risikobericht, es gibt ein Dashboard. Dass niemand hineinschaut, fällt bis zum Ernstfall nicht auf. Ein ungenutztes SIEM ist schlechter als kein SIEM, weil es Budget bindet und Aufmerksamkeit vortäuscht.



Skizze 5: Der Entscheidungspfad führt in drei mögliche Enden — und zwei davon heißen nicht Sentinel.

Der ehrliche Alternativweg: MDR

Wenn du die Sichtbarkeit brauchst, aber die Besetzung nicht hast, ist ein MDR-Dienstleister — Managed Detection and Response — der sachlich richtige Weg. Dort sitzt jemand rund um die Uhr vor der Konsole, dessen Beruf das ist. Zwei Varianten sind üblich: Der Dienstleister betreibt Sentinel in deinem Tenant und bearbeitet die Alarme, oder er arbeitet direkt auf deinem Defender XDR und du sparst dir das SIEM zunächst ganz.

Bei der Auswahl zählen weniger die Werkzeuge als die vertraglichen Zusagen. Frage nach Reaktionszeiten je Schweregrad, nach den Befugnissen des Dienstleisters (darf er ein Konto sperren, oder ruft er dich um drei Uhr nachts an?), nach dem Eskalationsweg und danach, wem die Daten und die Regeln gehören, wenn der Vertrag endet. Wer die Kriterien vorher nicht sauber definiert, kauft eine monatliche Rechnung mit E-Mail-Anhang.

Die Entscheidungskriterien in einer Tabelle

Die folgende Tabelle ist bewusst so gebaut, dass du sie in eine Entscheidungsvorlage kopieren kannst. Gehe sie Zeile für Zeile durch und markiere die zutreffende Spalte. Wenn du in der rechten Spalte mehr als fünf Treffer hast, ist die Anbindung wahrscheinlich richtig. Wenn du in der linken Spalte mehr als fünf Treffer hast, spar das Geld und investiere es in [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Kriterium	Gegen die Anbindung	Für die Anbindung
Größe und Besetzung	unter 300 Nutzer, keine dedizierte Rolle	ab etwa 300 Nutzern oder benanntes Security-Team
Alarmbearbeitung	Alarme werden gelegentlich gesichtet	werktägliche Bearbeitung ist verbindlich geregelt
Quellen außerhalb	praktisch reines Microsoft-365-	Firewall, OT, SAP, Fachanwendungen

Microsoft	Haus	sind sicherheitsrelevant
Aufbewahrungsbedarf	30 Tage genügen fachlich und rechtlich	Nachweispflichten über Monate oder Jahre
Regulatorik	keine sektorspezifischen Vorgaben	NIS2, KRITIS, Aufsicht, Kundenauditierung
Reifegrad Defender XDR	Onboarding unvollständig, Policies unklar	vollständig ausgerollt, Baseline sitzt
Eigene Erkennungslogik	Standardregeln reichen aus	spezifische Angriffsmuster im eigenen Geschäft
Automatisierungsbedarf	keine definierten Reaktionsprozesse	abgestimmte Abläufe, die Werkzeuge suchen
Budget und Planbarkeit	kein Spielraum für variable Kosten	Datenvolumen ist bekannt, Commitment-Stufe kalkulierbar
Vorfallhistorie	keine relevanten Vorfälle bekannt	es gab Vorfälle, deren Umfang unklar blieb
Bereitschaftszeiten	niemand außerhalb der Bürozeiten erreichbar	Rufbereitschaft existiert oder wird eingekauft
Mitbestimmung	Thema noch gar nicht angesprochen	Betriebsvereinbarung liegt vor oder ist in Arbeit

WARNUNG · Vier Anti-Muster, die immer wieder auftauchen

Das Compliance-SIEM. Angeschafft, weil ein Fragebogen danach fragte. Nie geöffnet. Besteht jedes Audit und erkennt nichts.

Der Datenstaubsauger. Alles angebunden, was einen Konnektor hat. Nach vier Monaten kommt die Rechnung ins Controlling, danach kommt die Reduktionsrunde, und am Ende bleibt weniger übrig als vorher geplant war.

Das SIEM statt der Hausaufgaben. Legacy-Protokolle noch aktiv, MFA lückenhaft, Conditional Access unvollständig — aber ein SIEM ist da. Siehe [Legacy Authentication endgültig abschalten](#) und [Conditional Access: Baselines, die nicht nerven](#).

Die Regel-Sammelwut. Alle mitgelieferten Analyseregeln aktiviert. Ergebnis: vierhundert Incidents pro Woche, davon drei relevant, und ein Team, das die Queue nicht mehr öffnet.

Wenn du anbindest: in Etappen, nicht auf einmal

Für den Fall, dass die Entscheidung für Sentinel fällt, hier der Ablauf, der sich in Projekten bewährt hat. Er ist bewusst langsam.

Etappe	Zeitraum	Inhalt	Ergebnis
1 Messen	Woche 1–4	Workspace anlegen, nur kostenlose Konnektoren, Testphase nutzen	belastbare Volumenzahlen aus der eigenen Umgebung
2 Ordnen	Woche 3–6	Tabellen den Tiers zuordnen, Aufbewahrung je Datenart festlegen	Kostenrahmen und Betriebsvereinbarung stehen
3 Erkennen	Woche 5–10	wenige, gut begründete Analyseregeln, Schwellenwerte justieren	eine Alarmlage, die ein Mensch bewältigen kann
4 Erweitern	ab Woche 8	Fremdquellen nach Risikobeitrag anbinden, nicht nach Verfügbarkeit	Sichtbarkeit dort, wo sie fehlt
5	ab Woche 12	erst informierende, dann	kürzere Reaktionszeiten mit

Automatisieren		eingreifende Playbooks	dokumentierter Freigabe
6 Berichten	laufend	Workbooks für Betrieb und Leitung trennen	das SIEM wird sichtbar, auch wenn nichts brennt

Etappe sechs wird regelmäßig unterschätzt und entscheidet trotzdem darüber, ob das Projekt im nächsten Haushalt überlebt. Ein SIEM, das nur meldet, wenn es brennt, sieht in ruhigen Monaten aus wie eine überflüssige Kostenstelle. Wie du die Wirkung so darstellst, dass sie ohne IT-Vorbildung verständlich ist, steht in [Security-Reporting für die Geschäftsführung](#). Und wenn du dir bei der Auslegung des Zuschnitts unsicher bist, ist genau das ein Thema für die [Microsoft 365 Security Beratung](#) — die Entscheidung gegen eine Anbindung ist dabei ein völlig legitimes Projektergebnis.

Häufige Fragen

Brauche ich Sentinel, wenn ich Microsoft 365 E5 habe?

Nicht automatisch. E5 bringt Defender XDR vollständig mit, und das deckt die Microsoft-Welt gut ab. E5 bringt allerdings auch das Datenkontingent von bis zu 5 MB pro Nutzer und Tag für Sentinel mit, das ausgerechnet die sonst teuren Quellen abdeckt. Wenn du E5 hast und Bedarf an längerer Aufbewahrung, ist der Einstieg günstiger, als die meisten annehmen. Die Frage bleibt trotzdem: Wer wertet aus?

Kann ich Sentinel testen, ohne sofort zu bezahlen?

Ja. Beim Aktivieren auf einem Log-Analytics-Workspace sind 31 Tage lang die ersten 10 GB pro Tag im Analytics-Tier frei. Nutze diese Zeit nicht, um alles anzubinden, was geht, sondern um Volumen zu messen. Automatisierung über Logic Apps und Data-Lake-Kosten fallen auch während der Testphase an.

Was passiert mit dem Azure-Portal?

Nach dem 31. März 2027 wird Sentinel im Azure-Portal nicht mehr unterstützt und läuft ausschließlich im Microsoft Defender Portal. Wer heute neu anbindet, sollte gar nicht erst Betriebsabläufe auf die Azure-Oberfläche aufbauen. Bestehende Umgebungen planen den Umzug besser jetzt als im letzten Quartal vor dem Stichtag.

Verliere ich Funktionen in Defender XDR, wenn ich Sentinel anbinde?

Nein. Die Anbindung ergänzt, sie ersetzt nichts. Automatic Attack Disruption, die produktinternen Erkennungen und die Defender-Automatisierung laufen unverändert weiter. Was sich ändert, ist die Menge dessen, was du zusätzlich sehen und abfragen kannst — und die Rechnung.

Reicht es, nur die kostenlosen Konnektoren anzubinden?

Für einen ersten Schritt: durchaus. Du bekommst die vollständige Alarmhistorie, die Office-365-Audit-Daten über deutlich längere Zeiträume und eine Grundlage für Auswertungen. Was fehlt, sind die Anmeldeprotokolle aus Entra ID und die Rohtabellen für tiefe Forensik. In vielen Fällen ist das ein sehr vernünftiger Einstieg mit überschaubarem Risiko.

Wie viele Analyseregeln sollte ich zu Beginn aktivieren?

Deutlich weniger, als der Katalog anbietet. Ein tragfähiger Einstieg sind zehn bis fünfzehn Regeln, die zu deinen tatsächlichen Risiken passen, mit sauber justierten Schwellenwerten und definierten Ausnahmen. Jede Regel, die niemand bearbeitet, senkt die Aufmerksamkeit für die Regeln, die zählen. Die Logik dahinter ist dieselbe wie bei [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Ersetzt Sentinel meine Backup- und Wiederherstellungsstrategie?

Nein, und diese Verwechslung kommt häufiger vor, als man denkt. Sentinel protokolliert, was passiert ist. Es stellt nichts wieder her. Bei einem Verschlüsselungsvorfall hilft dir Sentinel bei der Frage, wie der Angreifer hereinkam und was er angefasst hat — zurück bringt deine Daten die [Ransomware-Vorsorge in Microsoft 365](#).

Wir haben einen MDR-Vertrag. Brauchen wir dann trotzdem Sentinel?

Das hängt vom Vertrag ab. Manche Dienstleister arbeiten auf deinem Defender XDR und brauchen kein SIEM. Andere setzen einen Sentinel-Workspace voraus, weil sie eigene Regeln und Playbooks einbringen. Kläre vor Vertragsschluss, wem der Workspace gehört, wer die Kosten für die Datenaufnahme trägt und was beim Vertragsende mit den Regeln und den historischen Daten passiert.

Wie merke ich, dass die Anbindung sich nicht gelohnt hat?

An drei Signalen: Die Incident-Queue wird seltener als wöchentlich geöffnet. Die letzte selbst geschriebene Analyseregeln stammt aus dem Einführungsprojekt. Und bei der letzten Untersuchung hat niemand in Sentinel nachgeschaut, sondern direkt in Defender XDR. Wenn alle drei zutreffen, ist die richtige Konsequenz nicht mehr Budget, sondern ein Gespräch über MDR — oder ein kontrollierter Rückbau auf die kostenlosen Quellen.

WEITERLESEN • Passend zum Thema

- › [Alert Policies und Benachrichtigungen richtig aufsetzen](#) — die Grundlage, die vor jedem SIEM sitzen muss
- › [Security-Reporting für die Geschäftsführung](#) — damit die Investition auch außerhalb der IT ankommt
- › [Incident-Response-Plan für Microsoft 365](#) — der Prozess, den Automatisierung voraussetzt
- › [Defender for Endpoint: Onboarding ohne Drama](#) — die Datenquelle mit dem größten Volumenanteil
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — was vor der Anbindung geklärt sein muss
- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — wenn Regulatorik die Aufbewahrung vorgibt
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) — der Rahmen, in den das Monitoring gehört
- › [Schulung Microsoft 365 Security](#) — KQL und Erkennungslogik im Team verankern

Fazit

Microsoft Sentinel ist kein Statussymbol und keine Pflichtübung, sondern ein Werkzeug mit einer klaren Aufgabe: Es macht sichtbar, was Defender XDR nicht sieht, und es bewahrt auf, was Defender XDR nach dreißig Tagen vergisst. Wenn dein Risiko wesentlich außerhalb der Microsoft-Welt liegt, wenn du Nachweispflichten über Monate hast oder wenn dir bei der letzten Untersuchung die Daten ausgegangen sind, dann ist die Anbindung eine der wenigen Sicherheitsinvestitionen, deren Nutzen sich im Ernstfall sofort zeigt.

Der Einstieg ist dabei günstiger, als der Ruf des Produkts vermuten lässt. Die Alarme und Incidents aus dem gesamten Defender-Umfeld, die Office-365-Audit-Daten und die Azure-Aktivitätsprotokolle kosten keine Ingestion. Mit einem E5-Datenkontingent kommt oft noch der Rest der Microsoft-Quellen dazu. Teuer wird es erst durch das, was du zusätzlich hineinschiebst — und das ist eine Entscheidung, die du pro Tabelle triffst.

Bleibt die unbequeme Hälfte. Unterhalb von rund 300 Nutzern und ohne jemanden, der die Alarmbearbeitung als Aufgabe im Kalender stehen hat, wird Sentinel erfahrungsgemäß zu einem gepflegten Archiv mit monatlicher Rechnung. In diesem Fall ist ein MDR-Dienstleister die bessere Antwort, und die noch bessere ist oft, zuerst Defender XDR vollständig auszurollen, [Secure Score: sinnvoll nutzen statt Punktejagd](#) ernst zu nehmen und die Zuständigkeiten zu klären. Ein sauber betriebenes Defender XDR schlägt ein ungenutztes SIEM in jeder Übung — und ganz sicher in jedem echten Vorfall.

Die Frage lautet also nicht „Sentinel oder nicht“, sondern: Was passiert mit einem Alarm um 23 Uhr an einem Donnerstag? Wer die Antwort darauf kennt, weiß auch, ob sich die Anbindung lohnt.