



# Microsoft Defender for Cloud Apps

Der Praxisleitfaden zur Einrichtung und Konfiguration

- Snapshot Reports erstellen
- Apps und Dienste überwachen und blockieren
- Richtlinien und Templates aufsetzen



## Über den Autor


### Aaron Siller


Als ich 2014 als IT-Dienstleister startete, stand ich vor denselben Herausforderungen, mit denen heute viele meiner Kunden zu mir kommen: Komplexe Microsoft-Systeme, ständig neue Security-Anforderungen und nie genug Zeit, um alles richtig zu konfigurieren.

Was als klassische IT-Beratung begann, entwickelte sich schnell zu einer klaren Mission: **Microsoft 365 Umgebungen sicherer machen, ohne dass Admins dafür Wochenenden opfern müssen.**



Heute werde ich von führenden Instituten wie der Heise Academy und Golem Karrierewelt als Trainer für Microsoft 365 Security eingesetzt. Meine Expertise bestätigt sich in der Zusammenarbeit mit Unternehmen vom handwerklichen Mittelstand bis hin zu internationalen Konzernen. Schau Dir gerne meine Referenzen auf meiner Website an.

 E-MAIL [aaron@siller.consulting](mailto:aaron@siller.consulting)

 WEBSITE [siller.consulting](https://siller.consulting)

 LINKEDIN [Aaron-Siller](https://www.linkedin.com/in/Aaron-Siller)

 YOUTUBE [Aaron-Siller-YT](https://www.youtube.com/Aaron-Siller-YT)

## Inhaltsverzeichnis

Microsoft Defender für Cloud-Apps.....	5
Warum ein Cloud Access Security Broker verwenden? .....	5
Einführung von Microsoft Defender für Cloud-Apps .....	7
High-Level-Architektur .....	8
Erste Schritte .....	9
Deine Rolle als MDCA-Administrator .....	18
Erkennen von (Cloud-)Anwendungen .....	19
Integration mit Microsoft Defender für Endpunkt (MDE) .....	19
Erfassen von Netzwerkverkehrsprotokollen .....	20
Erstellen eines Momentaufnahmeberichts .....	21
Automatisches Hochladen von Protokolldateien.....	23
Erstellen eines fortlaufenden Berichts.....	25
Fehlerbehebung beim Protokollsammler .....	25
Interpretieren von Ermittlungsberichten.....	27
Überwachen und Sichern von Aktivitäten .....	30
Verbinden einer Anwendung über App-Connectors .....	31
Verwenden von Richtlinien zur Überwachung und Kontrolle von Cloud-Anwendungen.....	32
Untersuchung von Ereignissen.....	38
Governance-Protokoll .....	46
IP-Adressbereiche und Tags .....	46
Arbeiten mit Benutzergruppen .....	48
Verwalten von OAuth-Anwendungen .....	49
In Echtzeit mit Conditional Access App Controls arbeiten.....	53
Wie die Sitzungskontrolle (Proxy) funktioniert .....	54
Erstellen einer Conditional Access App Control-Richtlinie .....	54
Anzeigen von für Conditional Access App Control verfügbaren Anwendungen.....	54
Erstellen einer Sitzungsrichtlinie.....	56
Malware-Erkennung.....	57

Auf Malware-Erkennungen reagieren.....	57
Arbeiten mit Vertraulichkeitsbezeichnungen in MDCA .....	58
Voraussetzungen.....	58
Suche nach vorhandenen Dokumenten mit Labels .....	59
Anwenden von Labels auf Dateien .....	61
Integrationen von Drittanbietern und Automatisierung.....	64
Integration mit einem SIEM von Drittanbietern .....	64
Erstellen von API-Integrationen .....	66
Reale Szenarien .....	66
Überwachung der Nutzung sensibler oder hoch privilegierter Konten.....	67
Verhindern, dass Gastbenutzer Word-Dateien aus SharePoint Online herunterladen .....	70
Downloads von nicht verwalteten Geräten in Exchange Online blockieren.....	74
MFA beim Herunterladen sensibler Dateien von nicht verwalteten Geräten anfordern .....	76
Microsoft 365 Defender .....	78

# Microsoft Defender für Cloud-Apps

## Warum ein Cloud Access Security Broker verwenden?

Lange vorbei sind die Zeiten, in denen IT-Abteilungen ausschließlich bestimmten – oder zumindest weitgehend beeinflussten –, welche Anwendungen verwendet werden oder wie und wo diese Anwendungen gehostet werden. Der kometenhafte Aufstieg von Cloud-Anwendungen in Unternehmen brachte neue Herausforderungen mit sich, nicht zuletzt wenn es darum geht, Unternehmensinformationen und die potenziell sensible Natur solcher Informationen zu schützen.

- **Der fehlende Überblick** darüber, welche (Cloud-)Anwendungen innerhalb der Organisation verwendet werden, hat vielen Organisationen Kopfzerbrechen bereitet - um 1) zu verstehen, wo Daten gespeichert sind, und 2) welche Daten an besagten Orten gespeichert sind. Mit einem verstärkten Fokus auf den Schutz der Privatsphäre ist es von großer Bedeutung zu wissen, wo Daten gespeichert und verarbeitet werden!
- Ebenso macht **das Fehlen von Standards** bei Cloud-Anwendungen es für Organisationen schwierig, die Kontrolle darüber zu behalten, wie Daten innerhalb dieser Cloud-Anwendungen verwendet werden können - oder zumindest zu kontrollieren, welche Daten dort gespeichert werden können. Eine Anwendung bietet möglicherweise eine API, um Einblicke zu gewähren oder ein Stück Software auf dem Gerät zu installieren, eine andere vielleicht nicht. Bei so viel Vielfalt gibt es keinen Einheitsansatz, der auf eine Vielzahl von Plattformen angewendet werden kann. Somit steigt die Komplexität, die Kontrolle über diese Anwendungen zu behalten - ebenso wie die Kosten dafür.
- Der **Aufstieg von BYOD** hat die oben genannten Herausforderungen nicht einfacher gemacht. Es ist viel einfacher zu kontrollieren, welche Anwendungen auf einem Gerät verwendet werden können, das vollständig von der Organisation verwaltet wird. Vollständig verwaltete Geräte werden von Benutzern jedoch nicht immer mit offenen Armen empfangen - sie empfinden es häufig als audringlich und umständlich. Das gilt insbesondere dann, wenn die Sicherheitsrichtlinien sehr restriktiv sind und Benutzer möglicherweise daran hindern, auf bestimmte Anwendungen oder Funktionen des Geräts zuzugreifen.

Das Erstellen eines schriftlichen Verhaltenskodex, in dem Benutzer aufgefordert werden, nur genehmigte Apps zu verwenden, könnte eine Möglichkeit sein, die Kontrolle zurückzugewinnen. Dies würde jedoch erfordern, dass du dich ausschließlich auf den guten Glauben verlässt und darauf hoffst, dass sich die Leute an die Regeln halten. Obwohl wir immer das Beste in anderen suchen sollten, kann die Realität etwas ganz anderes sein. Während Benutzer normalerweise bereit sind, bestimmte Regeln einzuhalten, bietet das keinen Schutz für den Fall, dass ein Gerät

kompromittiert wird oder wenn ein Benutzer unwissentlich eine nicht autorisierte Aktion aufgrund mangelnder Kenntnisse durchführt. Es bietet auch keinen Einblick, ob Benutzer die Aufforderung einhalten.

Es liegt in der menschlichen Natur, nach Lösungen zu suchen (lies: die Richtlinien und Kontrollen zu umgehen), wenn eine (einfache) Aufgabe nicht auf eine einfache und effektive Weise ausgeführt werden kann. Lass mich dir ein Beispiel geben: Die Beliebtheit von Dateifreigabeplattformen wie beispielsweise WeTransfer ist größtenteils das Ergebnis davon, dass viele E-Mail-Systeme das Senden oder Empfangen größerer Anhänge nicht zulassen. Die Entscheidung, Anhänge nur bis zu einer bestimmten Größe zuzulassen, wird normalerweise in gutem Glauben getroffen – oft zum Schutz der E-Mail oder zur Einsparung von Speicherplatz auf diesen Systemen. Die Grenzen entwickelten sich jedoch nie so schnell, wie der Bedarf an größeren Dateien durch das Unternehmen wuchs. Natürlich würden Benutzer nach Alternativen suchen, die sie dann in Lösungen wie WeTransfer, Dropbox und anderen fanden.

Wie gewinnt man also die Kontrolle über ein solches Szenario – oder darüber, welche Anwendungen in der Umgebung verwendet werden? Hier kommen Cloud Access Security Broker (CASB) ins Spiel. Obwohl es viele verschiedene Definitionen dafür gibt, was ein CASB ist, läuft es für mich darauf hinaus: Ein CASB ist ein Dienst (oder eine Lösung), der vor Ort oder in der Cloud gehostet wird und zwischen dem Benutzer und den Cloud-Anwendungen sitzt – um die Nutzung und Aktivitäten innerhalb dieser Cloud-Anwendungen zu überwachen und optional Richtlinien durchzusetzen, um die Einhaltung unternehmensinterner und externer Vorschriften sicherzustellen.

Beim Lesen des Obigen denkst du vielleicht: “Macht das nicht schon seit Jahren irgendwie ein Reverse-Proxy?” Kurz gesagt: Ja. Proxy-Funktionen sind jedoch nur ein Teil dessen, was ein CASB tut. Moderne CASB-Lösungen erweitern Proxy-Funktionen, indem sie zusätzliche Einblicke, Kontrollen und Bedrohungsschutz bieten.

Heutzutage ist die IT-Abteilung nicht immer involviert, wenn neue (Cloud-)Anwendungen in Auftrag gegeben werden, wodurch sie unwissentlich ihre beschworene Pflicht aufgibt, Daten sicher zu halten. Wie könnten sie es auch, wenn sie nicht wissen, dass eine neue Anwendung verwendet wird? Vielleicht ist dieser poetische Ausbruch ein wenig übertrieben, aber er veranschaulicht einige Herausforderungen bei der Verwendung von Cloud-Anwendungen im professionellen Kontext.

Die Aufgabe der Sicherheitsabteilung in der IT besteht nicht darin, die Verwendung bestimmter Anwendungen zu verhindern, sondern vielmehr dem Unternehmen zu ermöglichen, jede benötigte Anwendung auf sichere Weise zu nutzen. So großartig dieses Paradigma auch klingen mag – die Realität ist viel härter, als man hoffen möchte: Das Fehlen von Standards bei verschiedenen Lösungen, Plattformen und Anbietern kann die Erfassung von Protokolldateien, die Zugriffskontrolle und den Schutz von Daten innerhalb dieser Plattformen viel schwieriger machen, als es auf den ersten Blick scheint.



Eine CASB-Lösung existiert, um diese Herausforderungen zu lindern und zu lösen. Was in den nächsten Abschnitten folgt, ist ein Überblick über Microsofts CASB-Lösung und wie ihre Funktionen dir helfen können, die Kontrolle über Shadow-IT zu übernehmen und Daten in verschiedenen (Cloud-)Anwendungen sicher zu halten.

## Einführung von Microsoft Defender für Cloud-Apps

Obwohl es viele Varianten gibt, existieren im Wesentlichen zwei Haupttypen von CASBs: Nur-API- und Multi-Mode-Lösungen. Ein reiner API-CASB verlässt sich vollständig auf APIs, die vom Cloud-Anwendungsanbieter zur Verfügung gestellt werden. Das bedeutet, dass die Funktionalität dieser CASBs durch die Funktionalität (und Informationen) eingeschränkt ist, die von diesen APIs bereitgestellt werden. Multi-Mode-CASBs verlassen sich nicht nur auf APIs und bieten oft zusätzliche Funktionen wie Schutz vor schädlichem Code (Malware), Anwendungs- und Compliance-Einblicke sowie funktionale Kontrolle darüber, welche Aktionen in den überwachten Anwendungen durchgeführt werden können. Letzteres ist oft durch die Verwendung von Inline- (Reverse-Proxy-)Funktionen möglich.

Microsoft Defender für Cloud-Apps, früher bekannt als Microsoft Cloud App Security (MCAS), ist eine Multi-Mode-CASB-Lösung: Sie bietet umfangreiche Einblicke in die Anwendungen, bewertet die Compliance der Anwendungen und ermöglicht eine granulare Steuerung von Aktivitäten und Daten – sowohl mit als auch ohne Verwendung von Proxy-Funktionen.

Die Hauptfunktionen von MDCA sind nachfolgend aufgeführt:

- **Cloud Discovery (Shadow IT):** Entdecke, welche (Cloud-)Anwendungen in deiner Umgebung verwendet werden. Zusätzlich verfügt MDCA über eine Datenbank mit mehr als 16.000 Anwendungen, die verwendet wird, um diesen eine "Sicherheits- und Compliance"-Bewertung zuzuweisen. Weitere Informationen zu dieser Bewertung findest du später in diesem Kapitel.
- **Datenschutz:** Durch Integration mit Lösungen wie Azure Information Protection, Office 365, Microsoft Defender für Endpunkt und bedingten Zugriff kann MDCA einzigartige Einblicke gewinnen, wie und wo Dateien gespeichert werden. Gleichzeitig kann es diese Dateien mit Vertraulichkeitskennzeichnung in Echtzeit durch eine Vielzahl vordefinierter Richtlinien und Kontrollen schützen.
- **Bedrohungsschutz:** Durch User and Entity Behaviour Analytics (UEBA) kann MDCA ungewöhnliches Verhalten über Cloud-Anwendungen hinweg erkennen und dir helfen, Bedrohungen wie kompromittierte Benutzerkonten, Ransomware-Angriffe oder nicht autorisierte Datenübertragungen (Datenlecks) zu erkennen.

- **Compliance-Bewertung (CSPM).** Für jede der MCDA bekannten Anwendungen wird eine Compliance-Bewertung gepflegt, mit der du die Sicherheitslage dieser Anwendung kontinuierlich bewerten und kontrollieren kannst – und festlegen kannst, ob diese Anwendung in deiner Organisation verwendet werden kann oder sollte, indem du sie als genehmigt oder nicht genehmigt markierst.
- **Verwaltung von OAuth-Anwendungen:** Azure AD ermöglicht es Drittanbieter-Anwendungen, eine Verbindung zu Ressourcen herzustellen oder die zentrale Authentifizierung von Azure AD zu nutzen. OAuth, ein offener Standard für die Zugriffsdelegation, ermöglicht es Benutzern, *zuzustimmen*, dass Anwendungen auf ihre Ressourcen zugreifen dürfen – ohne ihre Anmeldeinformationen weitergeben zu müssen. Das Ergebnis ist eine viel sicherere Art der Authentifizierung. Leider bringt OAuth aufgrund seiner Funktionsweise auch Herausforderungen mit sich. Ein Beispiel: App-Entwickler fordern oft deutlich mehr Berechtigungen an, als notwendig wäre. Auch Angreifer haben OAuth für sich entdeckt und nutzen es, um sich Zugriff zu verschaffen und zu behalten – insbesondere dann, wenn Benutzer Zugriffsanfragen selbst autorisieren können. Die App-Governance-Funktion, insbesondere die OAuth-Apps-Galerie in Defender für Cloud-Apps, bietet dir einen einfachen Überblick über alle mit dem Mandaten verbundenen Anwendungen, deren Berechtigungsgrad und weitere Sicherheitsaspekte. So erhältst du eine fundierte Entscheidungsgrundlage darüber, ob eine App in deiner Umgebung erlaubt sein sollte.

In diesem Kapitel konzentrieren wir uns auf die Vollversion von Microsoft Defender für Cloud-Apps, da sie den gesamten Funktionsumfang der Plattform umfasst. Je nachdem, welche Lizenzen dir zur Verfügung stehen, hast du möglicherweise keinen Zugriff auf alle Funktionen. Weitere Informationen zu den Unterschieden zwischen den verschiedenen Versionen von MDCA findest du auf der [folgenden](#) Website.

## High-Level-Architektur

Man kann die High-Level-Architektur in mehrere Hauptkomponenten unterteilen: Discovery, Proxy und Richtlinien. Die Discovery-Komponenten sind für die Aufnahme und Verarbeitung von Daten zuständig, die über unterschiedliche Kanäle empfangen werden. Dazu gehören API-Verbindungen mit Cloud-Anwendungen, Microsoft Defender für Endpunkt oder Verkehrsprotokolle von Netzwerkgeräten, die über einen Protokollsammler eingespeist werden. Zusätzlich können die Discovery-Komponenten Informationen vom MDCA-Proxy empfangen, wenn eine Sitzung über diesen hergestellt wird.

Der MDCA-Proxy ist im Grunde ein Reverse-Proxy, über den Verbindungen zu einer Cloud-Anwendung getunnelt werden. Sobald eine Sitzung über den MDCA-Proxy läuft, stehen dir zusätzliche Steuerungsmöglichkeiten zur Verfügung, etwa das Einschränken bestimmter Aktionen in Echtzeit. Wird hingegen eine direkte Verbindung zu einer Cloud-Anwendung aufgebaut, nutzt MDCA die API-Verbindung, um Aktivitäten zu erkennen und zu steuern, die ein



Benutzer durchführt. Damit das funktioniert, muss MDCA die jeweilige API-Verbindung natürlich unterstützen.

Darüber hinaus kannst du mit verschiedenen Richtlinien die Aktivitäten innerhalb von Cloud-Anwendungen überwachen und darauf reagieren. Abhängig davon, ob die Verbindung API-basiert ist oder über Sitzungssteuerung läuft, können Richtlinien entweder in Echtzeit greifen oder kurz nach Ausführung einer Aktivität wirksam werden.

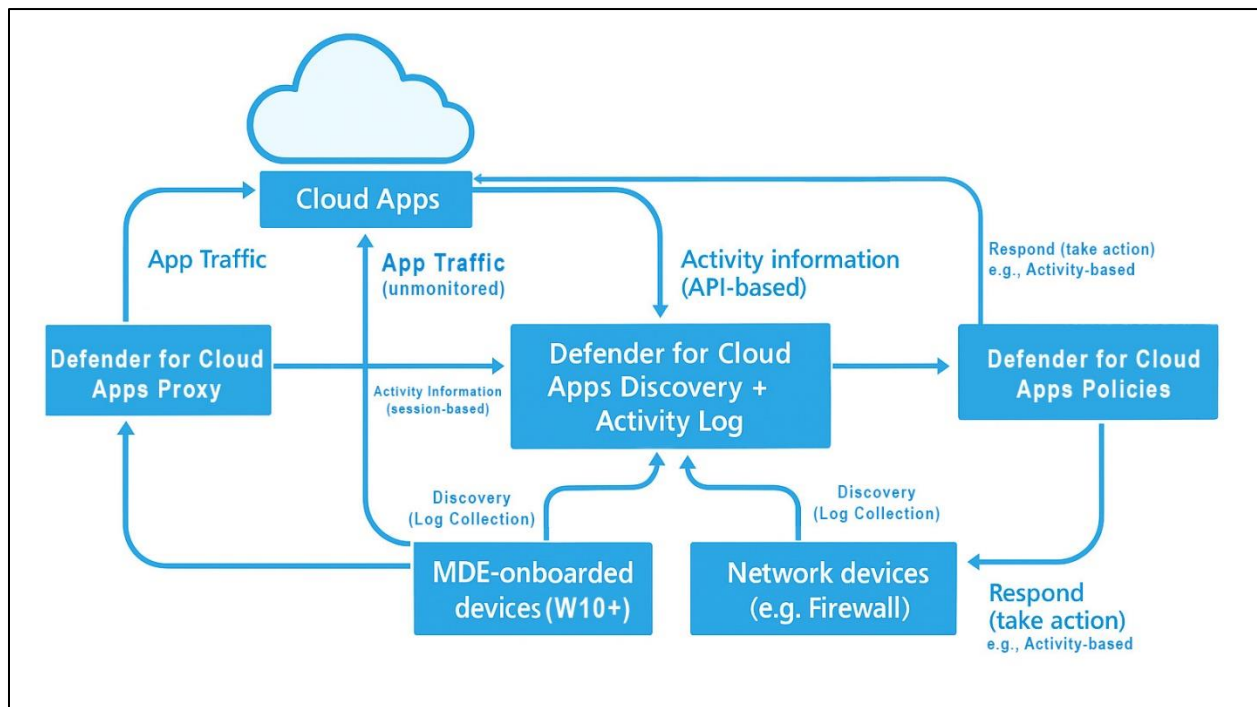


Abbildung 11-1: Hochrangige Architektur von MDCA.

## Erste Schritte

Einer der großen Vorteile von MDCA liegt in der einfachen Bereitstellung: Du kannst innerhalb weniger Minuten loslegen. Das liegt vor allem an den umfangreichen Integrationen mit anderen Microsoft-365-Workloads und daran, dass es sich um eine cloudbasierte Lösung handelt, die kaum zusätzliche Konfiguration benötigt, um einsatzbereit zu sein.

Microsoft Defender für Cloud-Apps ist vollständig in das [Microsoft Defender Security Portal](#) integriert. Bevor du MDCA nutzen kannst, musst du über die entsprechenden [Lizenzen](#) verfügen und dir müssen die nötigen Berechtigungen zugewiesen worden sein. Beim erstmaligen Zugriff auf den MDCA-Bereich ist das entweder die Rolle des globalen Administrators oder des Sicherheitsadministrators. Danach kannst du die Zugriffsrechte feingranular über verschiedene Rollen an Benutzer delegieren. Wie du den administrativen Zugriff genau verwalten kannst, wird später in diesem Kapitel unter „Verwalten des administrativen Zugriffs“ erläutert.

**Altes Portal noch vorhanden:** Derzeit erreichst du das frühere Defender für Cloud Apps-Portal noch unter <https://portal.cloudappsecurity.com>. Es gibt jedoch keinen echten Grund mehr, dieses zu verwenden, und es ist gut möglich, dass es in naher Zukunft abgeschaltet wird.

Die Informationen, die früher im Dashboard des alten Portals angezeigt wurden, sind nun im Startbildschirm des Microsoft 365 Defender Security-Portals enthalten. Wenn du dir die Karten im Portal ansiehst, wirst du dort Elemente finden, die (zum Teil) aus MDCA stammen, wie zum Beispiel **privilegierte OAuth-Apps** oder **gefährdete Benutzer**.

Den Bereich Microsoft Defender für Cloud-Apps findest du im Hauptmenü unter „**Cloud-Apps**“. Dort stehen dir folgende Funktionen zur Verfügung, die später in diesem Kapitel einzeln erläutert werden:

- Cloud Discovery
- Cloud-App-Katalog
- App Governance (enthält Elemente, die zuvor unter *OAuth-Apps* verfügbar waren)
- Dateien
- Aktivitätsprotokoll
- Governance-Protokoll
- Richtlinien

## Grundlegende MDCA-Konfiguration

Bevor du dich mit diesen Funktionen im Detail beschäftigst, solltest du einen Blick auf die Konfigurationsmöglichkeiten werfen, mit denen du MDCA an deine Anforderungen anpassen kannst. Öffne dazu das [Microsoft 365 Defender Security-Portal](#), klicke auf „Einstellungen“ und anschließend auf „Cloud-Apps“. Dort findest du eine Vielzahl an Optionen, die in unterschiedliche Abschnitte untergliedert sind.

### System

In diesem Bereich kannst du globale Einstellungen für Microsoft Defender für Cloud-Apps konfigurieren.

- **Organisationsdetails:** Hier kannst du das Logo deiner Organisation hochladen oder den Namen deiner Organisation ändern. Diese Informationen werden an verschiedenen Stellen in MDCA angezeigt, beispielsweise auf Informationsseiten für Benutzer oder in Warnmeldungen.
- Die **Posteinstellungen** ermöglichen es dir, die Absenderadresse für ausgehende E-Mail-Benachrichtigungen anzupassen. Standardmäßig werden Nachrichten von einer durch Microsoft verwalteten Adresse gesendet ([no-reply@cloudappsecurity.com](mailto:no-reply@cloudappsecurity.com)). Du kannst jedoch eine eigene benutzerdefinierte Adresse eingeben, z. B. eine, die zu deiner primären Domäne gehört.

Beachte dabei: Wenn du eine eigene Adresse verwendest, erfolgt der Versand über einen Drittanbieter (Mailchimp). Damit die Nachrichten korrekt zugestellt werden, musst du sicherstellen, dass die entsprechenden SPF-DNS-Einträge für Mailchimp hinterlegt sind. Zusätzlich hast du die Möglichkeit, eine eigene E-Mail-Vorlage hochzuladen, um das Erscheinungsbild von MDCA-Benachrichtigungen individuell anzupassen. Auch wenn die Standardvorlage functional ist, kann es sinnvoll sein, ein vertrautes Design zu verwenden, das besser zu deiner Organisation passt.

- **Eingeschränkter Einsatz und Datenschutz:** Diese Themen werden später in diesem Kapitel erläutert.
- **IP-Adressbereiche:** Hier kannst du IP-Adressen oder Adressbereiche definieren, die später in Richtlinien verwendet oder zur Kontextanreicherung genutzt werden können.
- **Benutzergruppen:** An dieser Stelle verwaltest du Gruppen, die in Richtlinien oder anderen Funktionen eingesetzt werden können.
- **API-Token:** Über diese Seite erstellst du Token, mit denen Drittanwendungen eine Verbindung zu MDCA herstellen können.
- **SIEM-Agents:** Hier konfigurierst du die Integration mit verschiedenen SIEM-Plattformen. Detaillierte Informationen dazu findest du im Abschnitt mit Microsoft Sentinel.
- **Playbooks:** In diesem Bereich kannst du automatisierte Abläufe erstellen, die später bei der Richtlinienerstellung verwendet werden können.
- **Info:** Zeigt dir Informationen über deine aktuellen MDCA-Instanz an.

## Mein Konto

In diesem Abschnitt legst du fest, ob und wohin Benachrichtigungen versendet werden sollen.

### My email notifications

Set email notifications for your account.

☐
 Receive email notifications for Defender for Cloud Apps alerts whose severity is at least
 

Choose severity
 

Medium

☐
 Receive email notifications for Defender for Cloud Apps system alerts

Save

 We secure your data as described in our [privacy statement](#) and [online service terms](#).

Abbildung 11-2: Konfigurieren der E-Mail-Benachrichtigungen.

## Cloud Discovery

Im Abschnitt Cloud Discovery passt du die Einstellungen für alles an, was mit der Cloud-App-Entdeckung zu tun hat.

- **Bewertungsmetriken:** Hier kannst du anpassen, wie die Bewertung einer entdeckten Anwendung berechnet wird. Wenn deine Organisation beispielsweise im Gesundheitswesen tätig ist und HIPAA unterliegt, solltest du in Erwägung ziehen, die Bedeutung der HIPAA-Compliance zu erhöhen. Dasselbe gilt für eine Vielzahl anderer Vorschriften und/oder gesetzlicher Anforderungen in Bezug auf solche Vorschriften.
- **Momentaufnahmeberichte:** Wie in *Entdecken von (Cloud-)Anwendungen* erläutert, gibt es mehrere Möglichkeiten, Anwendungen zu entdecken. Eine davon ist das Analysieren von (Netzwerk-)Protokolldateien. Wie der Name schon sagt, ermöglicht ein Momentaufnahmebericht das einmalige Hochladen von Protokolldateien zur Untersuchung.
- **Fortlaufende Berichte:** Wie die vorherige Option, aber wiederkehrend. Bevor du einen fortlaufenden (wiederkehrenden) Bericht erstellst, musst du den automatischen Protokoll-Upload für die gewünschte Datenquelle konfiguriert haben. Weitere Informationen zu den verschiedenen Berichten findest du im Abschnitt "Entdecken von (Cloud-)Anwendungen".
- **Automatischer Protokoll-Upload:** Hier kannst du neue Datenquellen konfigurieren und festlegen, wie Protokolle für diese Quellen gesammelt werden. Defender für Cloud Apps verfügt über eine integrierte Protokollerfassung für alles, was über MDCA proxiert wird, oder wenn du es mit Microsoft Defender für Endpunkt integrierst.
- **App-Tags:** Tags können verwendet werden, um Anwendungen zu gruppieren und bestimmte Aktionen auf sie anzuwenden. MDCA wird standardmäßig mit mehreren Tags geliefert: **genehmigt**, **nicht genehmigt** und **überwacht**. Diese Tags geben an, ob eine Anwendung zulässig ist oder nicht. Wenn MDCA mit Microsoft Defender für Endpunkt integriert ist, verwendest du diese Tags, um eine nicht genehmigte App automatisch am Zugriff von Geräten zu hindern, die in MDE integriert sind. Du kannst auch benutzerdefinierte Tags verwenden und sie auf Anwendungen anwenden, damit du a) sie leichter filtern oder b) Anwendungen basierend auf Tags auswählen kannst, wenn du eine neue Richtlinie erstellst. Die Integration mit MDE wird später ausführlicher besprochen.
- **Entitäten ausschließen:** Hier kannst du steuern, welche Benutzer, IP-Adressen und Geräte (Computer) während der Entdeckung von Informationen ignoriert werden. Ausschlüsse werden oft hinzugefügt, wenn es rechtliche oder regulatorische Bedenken hinsichtlich der Daten gibt, die möglicherweise in Defender für Cloud Apps offengelegt werden, oder wenn die Informationen bereits bekannt oder irrelevant für das Ziel der Entdeckung sind. Ausschlüsse können pro Benutzer vorgenommen werden, für importierte Gruppen aus Azure AD, IP-Adressen oder bestimmte Geräte. Für ausgeschlossene Entitäten werden keine Ermittlungsinformationen angezeigt.
- **Microsoft Defender für Endpunkt:** Hier kannst du auswählen, ob Anwendungen von Microsoft Defender für Endpunkt blockiert werden sollen, wenn sie als nicht genehmigt

gekennzeichnet sind. Wenn eine Anwendung nicht genehmigt ist, übermittelt Defender für Cloud Apps automatisch relevante Informationen (wie IP-Adressen, Dateierweiterungen oder URLs) an Defender für Endpunkt, damit die Netzwerkschutzkomponente die Verbindungen zur nicht genehmigten Cloud-Anwendung blockieren kann. Damit dies funktioniert, musst du den Netzwerkschutz in MDE aktiviert haben und das integrierte Gerät muss dies ebenfalls unterstützen. Du kannst auch die Benachrichtigungs-URL konfigurieren – das ist die Seite, zu der Benutzer weitergeleitet werden, wenn eine App überwacht wird. Normalerweise ist die Seite, zu der du deine Benutzer weiterleiten würdest, dazu gedacht, sie aufzuklären, und enthält weitere Informationen darüber, warum die Anwendung möglicherweise blockiert wurde und an wen sie sich bei Problemen wenden sollten.

- **Benutzeranreicherung:** Wenn MDCA während der Ermittlung von Daten einen identifizierten Benutzer einem bekannten Benutzer in Azure AD zuordnen kann, ersetzt es den Bezeichner in den Protokollen durch die tatsächlichen Details des Benutzers wie Benutzername usw.
- **Anonymisierung:** MDCA ermöglicht es dir, Benutzerinformationen (Name) aus den Protokolldateien zu anonymisieren (verschleiern), sodass ein Administrator das Subjekt in den Protokollen nicht sofort identifizieren kann. Auch wenn das eher selten erforderlich ist, kann es in Szenarien nützlich sein, in denen du eine Entität nicht ausschließen möchtest, aber ohne zusätzliche Maßnahmen keine sensiblen Informationen offenlegen möchtest. Wenn Daten anonymisiert werden, wird der Benutzername durch eine GUID ersetzt. Administratoren können diese Seite verwenden, um eine GUID wieder in einen Benutzernamen umzuwandeln. Dies führt jedoch zu einem expliziten Eintrag in den Aktivitätsprotokollen und kann auch Warnungen auslösen.
- **Daten löschen:** Sollte die Zeit kommen, dass du dich von Defender für Cloud Apps abmelden möchtest, kannst du hier die Löschung deiner gesammelten Daten aus dem Dienst beantragen.

## Verbundene Apps

- **App-Connectors** ermöglichen es dir, anzuzeigen und zu steuern, welche Anwendungen (über API) mit Microsoft Defender für Cloud Apps verbunden sind.
- **Conditional Access App Control** Apps bietet eine Übersicht über alle Apps, die für Conditional Access App Control aktiviert wurden. Weitere Informationen über Conditional Access App Control werden später bereitgestellt.

## Informationsschutz

Unter Informationsschutz steuerst du verschiedene Optionen in Bezug auf die Integration mit der Microsoft Information Protection-Plattform und -Funktionen. Weitere Informationen zur Integration mit Azure Information Protection werden später bereitgestellt.

- Die **Admin-Quarantäne** definiert den Speicherort der Admin-Quarantäne und welche Meldungen Benutzern angezeigt werden, wenn eine Datei (vorübergehend) verschoben wurde. Um Dateien in die Admin-Quarantäne zu verschieben, musst du eine Dateirichtlinie mit der Aktion "In Admin-Quarantäne verschieben" erstellen. Dadurch wird die Originaldatei durch einen Platzhalter (Stub ) ersetzt, der die von dir konfigurierte Nachricht enthält. Die Originaldatei wird in den Zielordner der Admin-Quarantäne verschoben. Von dort aus kann ein Administrator die Datei überprüfen und gegebenenfalls die Datei wieder zurückverschieben. Beachte, dass die Admin-Quarantäne nicht für bösartige Dateien wie Malware verwendet wird. In einer brandneuen Umgebung hast du möglicherweise standardmäßig keine gültigen Speicherorte für die Admin-Quarantäne verfügbar. Die Admin-Quarantäne kann ein persönliches OneDrive oder eine bestimmte SharePoint-Seite sein. Wenn die Liste der gültigen Speicherorte leer ist, stelle sicher, dass du zuerst einen gültigen Speicherort erstellst.
- **Microsoft Information Protection** ist der Ort, an dem du die Integration mit Azure Information Protection konfigurierst und wie MDCA mit geschützten Inhalten umgeht. Bevor MDCA Dokumente überprüfen kann, die bereits geschützt sind, müssen die erforderlichen Berechtigungen erteilt werden. Das kannst du von hier aus tun. Betrachte diese Berechtigungen wie die "Super User" RMS-Berechtigungen, die MDCA die Möglichkeit geben, alle geschützten Dokumente zu "lesen" - unabhängig davon, welche Vorlage oder Bezeichnung auf das Dokument angewendet wurde.
- Unter **Dateien** kannst du steuern, ob MDCA geschützte Dateien für Ermittlungszwecke überwachen kann. Dies steuert nicht die Dateiüberwachung in Bezug auf Benutzeraktivitäten wie Änderungen, Downloads, Freigaben usw. Diese Einstellungen werden separat über die Office 365-Überwachungsrichtlinie gesteuert. Weitere Informationen zum Prozess findest du [hier](#).
- **Externe DLP** ist der Ort, an dem du externe DLP-Lösungen konfigurierst, die du möglicherweise in deiner Umgebung verwendest. Die Integration ermöglicht es MDCA, eine Verbindung zu anderen DLP-Systemen herzustellen, um Informationen auszutauschen und darauf zuzugreifen - mit dem Ziel, beispielsweise eine gemeinsame Inhaltsklassifizierung über die verschiedenen Systeme hinweg zu ermöglichen. Die Integration verwendet ein Branchenstandard-Protokoll (ICAP), um sicherzustellen, dass Informationen auf sichere Weise ausgetauscht werden. Aktuell werden nur wenige externe DLP-Lösungen unterstützt. Die Integration erfordert, dass du einen Server einrichtest, um die Verbindung zwischen Microsoft und diesen externen Lösungen zu erleichtern. Weitere Informationen findest du [hier](#).

## Conditional Access App Control

Unter **Conditional Access App Control** sind die folgenden Einstellungen verfügbar:

- **Standardverhalten:** Wähle aus, ob Anwendungen, die dem Conditional Access App Control unterliegen, zugänglich sein sollen, wenn die Conditional Access App Control-



Plattform nicht verfügbar ist oder nicht wie erwartet funktioniert. Dies unterscheidet sich von der Aktion, die in einer Richtlinie konfiguriert ist.

- **Benutzerüberwachung:** Ermöglicht es dir festzulegen, ob Benutzer informiert werden, wenn sie auf eine Anwendung zugreifen, die von Defender für Cloud Apps überwacht wird. Standardmäßig wird den Benutzern vor dem Öffnen der Anwendung eine Informationsseite angezeigt, die ihnen erklärt, dass ihre Sitzung überwacht wird. Obwohl Benutzer die Option deaktivieren können, die Warnung jedes Mal anzuzeigen, wenn sie sich bei einer Anwendung anmelden, kann dies lästig sein, wenn die meisten deiner Anwendungen MDCA-Sitzungsrichtlinien unterliegen. In einem solchen Fall möchtest du die explizite Warnung möglicherweise ausschalten.
- **Geräteidentifikation:** Defender für Cloud Apps verfügt über verschiedene Möglichkeiten, ein Gerät zu identifizieren: Es kann Azure AD oder Intune verwenden, um zu sehen, ob die Geräteinformationen aus den Aktivitätsprotokollen zugeordnet werden können. Für Geräte, die nicht in Azure AD eingebunden oder über Intune verwaltet werden, kann MDCA jedoch auch Gerätezertifikate verwenden. Dazu musst du deine vertrauenswürdigen Stamm-/Zwischenzertifikate bereitstellen, damit MDCA die Geräte ordnungsgemäß authentifizieren kann.
- **App-Onboarding/Wartung:** Hier kannst du festlegen, welche Benutzer (oder Administratoren) Anwendungen für Conditional Access App Control integrieren dürfen. Dies ist besonders nützlich, wenn die Personen, die MDCA verwalten, nicht unbedingt diejenigen sind, die Regeln für bedingten Zugriff erstellen oder neue Anwendungen im Azure AD der Organisation registrieren - oder umgekehrt. Benutzer, die dieser Liste hinzugefügt werden, erhalten (begrenzten) Zugriff auf das MDCA-Portal, über das sie Anwendungen für Conditional Access App Control aktivieren können.

**Realität:** Es ist für den Benutzer möglicherweise nicht immer ganz klar, dass er nur eingeschränkte Berechtigungen hat. Während bestimmte Bereiche (wie das Erstellen von Richtlinien) alle Funktionen ausgrauen, kann der Benutzer in einigen Bereichen (z. B. bei der Verwaltung des Administratorzugriffs) bis zum Ende eines Assistenten durchklicken, nur um am Ende mit einer Fehlermeldung begrüßt zu werden, dass er nicht über ausreichende Berechtigungen verfügt.

## Verwalten des Administratorzugriffs

Als globaler Administrator oder Sicherheitsadministrator hast du vollen Zugriff auf alle Funktionen in MDCA. Es ist jedoch eine gute Praxis, diese Berechtigungen nicht an jeden zu vergeben, der lediglich Zugriff auf MDCA benötigt.

Um spezifischen Zugriff zu gewähren, öffne das [Microsoft 365 Defender Security-Portal](#) und navigiere zu „**Berechtigungen**“. Klicke auf der Berechtigungsseite unter „**Cloud-Apps**“ auf „**Rollen**“. Klicke anschließend auf „**Benutzer hinzufügen**“ und gib die E-Mail-Adresse des Benutzers ein, dem du Zugriff gewähren möchtest. Fahre fort, indem du eine der integrierten Rollen auswählst:

- Globaler Administrator
- Sicherheitsleser
- Compliance-Administrator
- App-/Instanz-Administrator
- Benutzergruppen-Administrator
- Cloud Discovery Global Administrator
- Cloud Discovery-Berichtsadministrator
- Sicherheitsoperator

Wie du feststellen wirst, könnte die Erfahrung beim Hinzufügen eines neuen Administrators verbessert werden. Erstens ist das Delegierungsmodell in MDCA nicht in Azure AD integriert, **obwohl einige Rollen exakt gleich benannt sind wie ähnliche Rollen in Azure AD**. Das bedeutet auch, dass du keine vordefinierten Gruppen einrichten kannst, denen (automatisch) Berechtigungen in MDCA zugewiesen werden. Bis Microsoft dies “behebt”, musst du dich mit Zuweisungen pro Benutzer zufriedengeben. Zweitens erlaubt der Assistent weder die Suche nach einem Benutzer noch die Auswahl aus dem Verzeichnis. Das heißt, du musst den UPN oder die E-Mail-Adresse kennen, bevor du den Benutzer als Administrator hinzufügst. Wenn du die E-Mail-Adresse falsch eingibst, erhältst du erst eine Warnung, wenn du versuchst, die Berechtigungen hinzuzufügen. Schließlich musst du, wenn ein Benutzer bereits eine Art von Administratorzugriff hat, diesen zunächst widerrufen, bevor du ihn ändern kannst.

## Bereitstellungen begrenzen

Auch wenn du möglichst viele Aktivitäten in deinem Mandanten überwachen möchtest, um maximale Einblicke in deine Umgebung zu erhalten, können Datenschutzvorgaben oder Lizenzbeschränkungen erfordern, dass du den Kreis der überwachten Personen einschränkst. Wie beim Ausschließen von Entitäten in einer Richtlinie kannst du in MDCA global bestimmte Benutzer von der Aktivitätsüberwachung ein- oder ausschließen. Ausschlüsse haben Vorrang vor Einschlüssen – dadurch kannst du sehr granular vorgehen. Du könntest z. B. die Aktivitäten eines Benutzers in einer Anwendung überwachen, jedoch nicht in einer anderen.

Bevor du eine Einschränkungsgel erstellen kannst, musst du zuerst Benutzergruppen in MDCA importieren. Wie das geht, wird im Abschnitt „**Verwalten von MDCA-Benutzergruppen**“ erklärt.

Um eine Richtlinie zu erstellen, navigiere zu „**Einstellungen > Cloud-Apps**“ und klicke auf „**Eingeschränkter Einsatz und Datenschutz**“. Wähle anschließend aus, ob du bestimmte Benutzer(gruppen) für die Überwachung ein- oder ausschließen möchtest. In diesem Beispiel klickst du auf „**Ausschließen**“. Klicke in der Registerkarte auf das blaue Pluszeichen, um eine neue Ausschlussregel zu erstellen. Eine Regel besteht aus folgenden Informationen:

- Ein Regelname,

- Für welche Benutzergruppe(n) die Regel erstellt werden soll,
- Für welche Anwendung (oder Anwendungsinstanzen) die Regel gilt

**Einschlüsse führen auch zu Ausschlüssen:** Sei vorsichtig beim Erstellen einer Einschlussregel. Wenn du eine bestimmte Gruppe auswählst, wird nur diese Gruppe überwacht. Jeder Benutzer, der nicht Mitglied dieser Gruppe ist, wird automatisch von der Überwachung ausgeschlossen.

## Datenschutz wahren

Auf Basis der Daten, die MDCA verarbeitet, könnte ein Administrator Zugriff auf potenziell sensible Informationen wie den Standort eines Benutzers, Zeitpunkte von Aktivitäten, Dateinamen usw. haben. Der **Aktivitätsdatenschutz** ermöglicht es dir, eine Gruppe von Personen zu definieren, deren Aktivitäten standardmäßig als privat markiert und ausgeblendet werden. Wenn einem Administrator kein expliziter Zugriff gewährt wurde, diese privaten Aktivitäten anzuzeigen, wird ihm eine Meldung wie in Abbildung 11-3 angezeigt:

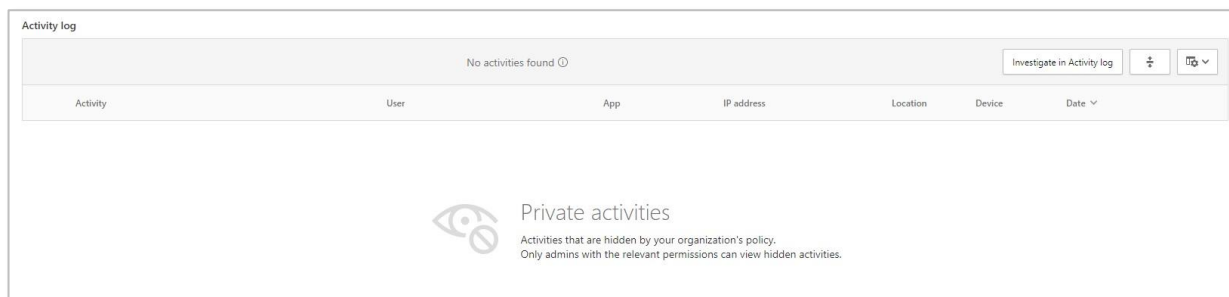


Abbildung 11-3: Ausblenden potenziell sensibler Aktivitäten in MDCA

Um Aktivitäten für eine bestimmte Gruppe auszublenden, öffne das Optionsmenü (Zahnrad) und klicke auf „**Eingeschränkter Einsatz**“. Klicke auf der Seite „**Eingeschränkter Einsatz und Datenschutz**“ auf die Registerkarte „**Aktivitätsdatenschutz**“. Klicke dann auf das Pluszeichen und wähle die Gruppe aus, für die du Aktivitäten standardmäßig ausblenden möchtest. Du kannst eine vorhandene Gruppe verwenden oder eine neue Gruppe in Defender für Cloud Apps erstellen – wie später in diesem Kapitel unter „**Arbeiten mit Benutzergruppen**“ beschrieben.

Die Zuweisung von Berechtigungen zum Anzeigen ausgeblendeter Aktivitäten erfolgt über:

**Berechtigungen > Cloud-Apps > Aktivität Datenschutz-Berechtigungen.** Klicke auf „**Benutzer hinzufügen**“ und wähle die E-Mail-Adresse (UPN) des Administrators aus, dem du die Berechtigungen zum Anzeigen ausgeblendeter Aktivitäten gewähren möchtest.

Sobald ein Administrator diese Berechtigungen erhalten hat, kann er ausgeblendete Aktivitäten automatisch wieder sehen – etwa beim Untersuchen einer Warnung oder beim Durchsuchen der Aktivitätsprotokolle.

## Anwendungen verbinden

Allein durch das Durchlaufen der vorherigen Einstellungen wird MDCA nicht besonders nützlich – du musst deine Cloud-Anwendungen verbinden und Protokolldateien erfassen, um herauszufinden, was in deiner Umgebung passiert. Beide Elemente werden später in diesem Kapitel in „Anwendungen verbinden“ und „Entdecken von (Cloud-)Anwendungen“ ausführlicher erläutert.

## Deine Rolle als MDCA-Administrator

Ich bekomme oft die Frage, was die Rolle eines MDCA-Administrators ist oder wofür das MDCA-Portal verwendet werden sollte. Schließlich können Warnungen an eine proprietäre Lösung wie ein SIEM gesendet werden, wodurch es nicht mehr notwendig ist, das MDCA-Portal dauerhaft geöffnet zu lassen, um neue Warnungen im Auge zu behalten.

Wie bei vielen Dingen hängt die Antwort davon ab, was du erreichen möchtest. Wenn du der Administrator bist, der für die Wartung der Plattform verantwortlich ist, wirst du das Portal wahrscheinlich regelmäßig verwenden. Wenn du jedoch Teil des First-Level-Service bist, wirst du dich wahrscheinlich nie am Portal anmelden müssen. Einige haben möglicherweise eine Vielzahl von Verantwortlichkeiten und müssen beides tun.

Aus der Perspektive des Security Operations (SecOps) kann das MDCA-Portal nützlich sein, um bestimmte Aktivitäten zu untersuchen, die zu einer bestimmten Warnung oder einem Vorfall geführt haben. Andererseits ist es umso wahrscheinlicher, dass deine SecOps-Organisation eine Lösung wie Microsoft Sentinel verwendet, um ihre Untersuchungen durchzuführen und an die benötigten Informationen zu gelangen, je ausgereifter sie ist. Es hängt alles davon ab, welche Tools deine Organisation verwendet – aber noch wichtiger – wo die „Rohdaten“ gespeichert werden. Wenn du keine Aktivitäten von MDCA in dein eigenes SIEM überträgst, kannst du Aktivitäten nicht als Teil der Korrelation verwenden. Das bedeutet auch, dass du dich an das MDCA-Portal wenden musst, wenn du bestimmte Aktivitäten untersuchen möchtest.

Unabhängig von deinem Ansatz ist das Portal so aufgebaut, dass du schnell durch die Informationen navigieren kannst. Wenn du keine sehr ausgereifte Cybersicherheitsorganisation hast, ist es sehr wahrscheinlich, dass das MDCA-Portal dein Hauptwerkzeug sein wird, um die Plattform zu verwalten, mit den von ihr bereitgestellten Daten zu interagieren, Untersuchungen durchzuführen usw.

# Erkennen von (Cloud-)Anwendungen

An diesem Punkt sollte die Bedeutung eines Überblicks darüber, was in deinem Netzwerk passiert, klar sein. Eine der wichtigsten Herausforderungen, die ein Cloud Access Security Broker zu lösen versucht, besteht darin, diese Erkenntnisse bereitzustellen – zum Beispiel, welche (Cloud-)Anwendungen von deinem Netzwerk aus verwendet werden. Es sollte daher nicht überraschen, dass die Fähigkeit, zu entdecken, was in deinem Netzwerk vor sich geht, eine wichtige Funktionalität einer CASB-Lösung ist.

Bevor du mit der Untersuchung beginnen kannst, musst du MDCA mit Daten versorgen. Diese Daten können aus verschiedenen Quellen stammen, z. B. Microsoft Defender für Endpunkt oder verschiedenen Netzwerkgeräten. Um ein vollständiges Bild deiner Umgebung zu erhalten, sollte ein Cloud App Security Broker in der Lage sein, Daten aus verschiedenen Quellen auszuwerten bzw. zu korrelieren. Je mehr Datenquellen du bereitstellst, desto genauer ist deine Sicht auf die Welt.

## Integration mit Microsoft Defender für Endpunkt (MDE)

Eine der Schlüsselfunktionen und meiner Meinung nach eines der wichtigsten Verkaufsargumente von MDCA ist die native Integration mit Microsoft Defender für Endpunkt, die neue Funktionen wie die Möglichkeit bietet, nicht genehmigte Cloud-Anwendungen automatisch zu blockieren und Telemetriedaten von Defender für Endpunkt zu verwenden, um herauszufinden, was in deiner Organisation vor sich geht. Aber das ist noch nicht alles. Wenn du die Integration mit MDE aktivierst, werden Daten, die von Endpunkten gesammelt werden, die in MDE integriert sind, automatisch mit MDCA zur Analyse geteilt.

Um Signale von MDE an MDCA zu senden, musst du die Funktionen vom Windows Defender Security Center aus aktivieren: Navigiere zuerst zum Microsoft 365 Defender-Portal. Klicke im Portal auf **Einstellungen** und navigiere zu **Endpunkt > Erweiterte Funktionen**. Finde **Microsoft Defender für Cloud Apps** in der Liste der Optionen und schalte den Umschalter um, damit die Funktion aktiviert ist. Klicke schließlich auf **Einstellungen speichern**.

**Realität:** Erwarte nicht, dass Daten von MDE sofort in MDCA fließen. Es gibt eine leichte Verzögerung zwischen dem Auftreten einer Aktion auf dem Gerät, der Aufzeichnung in MDE und dem Weg zu MDCA. Dies geschieht jedoch normalerweise innerhalb weniger Minuten.

Sobald du die Funktion aktiviert hast, wird automatisch ein integrierter, fortlaufender Bericht mit dem Namen „Win10 Endpoint Users“ erstellt. Der Bericht kann nicht über MDCA geändert oder verwaltet werden.

Im Gegensatz zu einigen der Einschränkungen, die beim Erfassen von Netzwerkverkehrsprotokollen bestehen, sind die von MDE stammenden Informationen extrem detailliert. Das liegt natürlich daran, dass MDE in das Kernbetriebssystem eingebettet ist und daher aus erster Hand Informationen darüber hat, was auf einem Computer passiert. Wenn du MDE verwendest und Zugriff auf MDCA hast, ist die Aktivierung dieser Integration praktisch ein Kinderspiel. Die Einfachheit der Bereitstellung und die Qualität der Informationen sind nahezu unübertroffen und bieten weit mehr Informationen als viele herkömmliche Netzwerkverkehrsprotokolle, über die wir als Nächstes sprechen werden.

**Hinweis:** Trotz der umfangreichen Informationen von MDE gibt es einige Einschränkungen hinsichtlich dessen, was angezeigt wird. Zum Beispiel kannst du mit der Integration erkennen, wenn jemand Daten in eine nicht genehmigte Anwendung hochlädt, und sie sagt dir sogar, wie viele Daten hochgeladen wurden. Du kannst jedoch nicht feststellen, welche Dateien usw.

## Erfassen von Netzwerkverkehrsprotokollen

Ein Vorteil von Netzwerkverkehrsprotokollen, z. B. von einem Proxy-Server oder einer Firewall, gegenüber den Informationen von MDE ist die Möglichkeit, Daten von Geräten einzubeziehen, die nicht in MDE integriert wurden oder nicht integriert werden können.

Die Herausforderung bei Netzwerkprotokollen besteht darin, dass sie oft nur Daten für Geräte enthalten, die irgendwie direkt oder über ein VPN mit dem Unternehmensnetzwerk verbunden sind. Das ist großartig für stationäre Computer, IoT-Geräte und Server, aber weniger für mobile Geräte, die sich möglicherweise nie mit WLAN verbinden, oder Laptops, die über Netzwerke roamen. Es sei denn, der gesamte ausgehende Datenverkehr zum Internet wird an einem Punkt zentralisiert, z. B. über ein VPN, fehlen dir unter Umständen dennoch wichtige Teile der benötigten Daten, um ein vollständiges Bild zu erhalten. Es sei denn, du verwendest einen Dienst wie einen Cloud-Proxy (z. B. ZScaler), bei dem alle Daten von Geräten den Online-Proxy durchlaufen, bevor sie im Internet landen. Auf diese Weise können Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, dennoch Verkehrsprotokolle generieren, die zur Ermittlung verwendet werden können.

Da nicht jede Umgebung homogen ist, sollte die Bedeutung von Netzwerkverkehrsprotokollen bei der Identifizierung verwendeter (Cloud-)Anwendungen nicht unterschätzt werden. Wenn andere Mittel wie ein Agent auf dem Gerät fehlen, können Netzwerkprotokolle viele nützliche Informationen darüber liefern, was im Netzwerk passiert. Dies beschränkt sich nicht auf typische Office-IoT-Geräte, sondern gilt auch für Industriesteuerungssysteme usw.

**Realität:** Du fragst dich vielleicht, warum IoT-Geräte ein interessantes Thema in Ermittlungsprotokollen sein können. Leider sind IoT-Geräte oft weniger gesichert als beispielsweise ein Desktop-Computer oder Laptop, die gut gewartet werden. Häufig werden IoT-Geräte nach dem Prinzip "Einrichten und Vergessen" behandelt, was bedeutet, dass sie möglicherweise schlecht gewartet und überhaupt nicht aktualisiert werden. Es sollte kaum



überraschen, dass Angreifer ein zunehmendes Interesse an ihnen haben. Zu wissen, welche (Cloud-)Apps von diesen IoT-Geräten verwendet werden, kann nützlich sein, da du Warnmeldungen für Aktivitäten einrichten kannst, sobald unerwarteter Datenverkehr zu einer von einem dieser Geräte auftritt.

Eine der Herausforderungen beim Erfassen von Informationen von Netzwerkgeräten ist das Format, in dem sie gespeichert werden, oder die Art der gespeicherten Informationen. Das kann von einem Anbieter zum anderen und sogar zwischen Gerätetypen desselben Anbieters variieren. Standardmäßig unterstützt MDCA die Erfassung von Protokollen zahlreicher Anbieter, darunter Blue Coat, Barracuda, Check Point, Cisco, Fortinet usw. Das bedeutet, dass MDCA bereits weiß, wie die Informationen zu analysieren sind, wenn du einen Protokollsammler für einen dieser Dienste oder Geräte einrichtest. Für alle anderen Geräte, die standardmäßig nicht enthalten sind, kannst du ein benutzerdefiniertes Protokollformat definieren und festlegen, wie und welche Daten erfasst werden sollen. Beachte, dass es einige Einschränkungen bei der Erfassung von Netzwerkprotokollen gibt. Weitere Informationen darüber, welche Daten von bestimmten Anbietern unterstützt werden, findest du auf [dieser](#) Website.

**Realität:** Müll rein bedeutet Müll raus. Beim Erstellen eines benutzerdefinierten Protokollformats ist es entscheidend, dass du so viele Informationen aus den Protokollen wie möglich definierst und abgleichst. Wenn verfügbar, solltest du angeben, welcher Eintrag im Protokoll mit Quell-/Ziel-IP-Adressen, Benutzernamen, Verkehrsgrößen und den Aktionen des Geräts ausgeführt (z. B. das Zulassen oder Verweigern bestimmter Verbindungen) übereinstimmt.

## Erstellen eines Momentaufnahmeberichts

Momentaufnahmeberichte sind eine hervorragende Möglichkeit, schnell einen Überblick darüber zu bekommen, was in einem Netzwerk passiert. Da sie sich einfach erstellen lassen, eignen sie sich ideal, um schnell Ergebnisse zu präsentieren. Ich verwende sie häufig in Proof-of-Concepts, um 1) den Mehrwert von MDCA zu demonstrieren und 2) zu zeigen, dass Shadow IT in nahezu jeder Umgebung ein Thema ist. Mit den Ergebnissen eines Momentaufnahmeberichts kannst du leicht bestimmte Bereiche und Anwendungen identifizieren, die du anschließend genauer untersuchen möchtest.

Um einen neuen Momentaufnahmebericht zu erstellen, navigiere zum **Einstellungsmenü** oder wähle **Cloud Discovery** im Hauptmenü aus und klicke auf **Aktionen > Cloud Discovery-Momentaufnahmebericht erstellen**, wie in der folgenden Abbildung gezeigt.

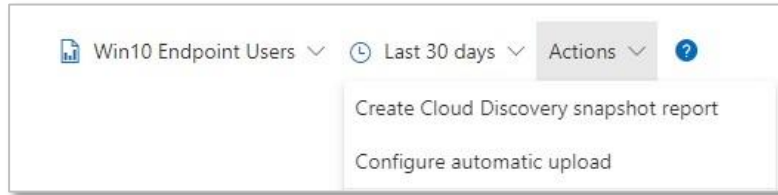


Abbildung 11-4: Hinzufügen eines Momentaufnahmeberichts in MDCA

Im folgenden Beispiel laden wir Protokolldateien von einer (lokalen) FortiGate-Firewall in MDCA hoch. Während des Assistenten wirst du nach verschiedenen Informationen gefragt. Achte darauf, Metadaten wie den Namen und eine Beschreibung des Berichts anzugeben. Verwende eine aussagekräftige Bezeichnung, damit du später nachvollziehen kannst, welche Daten analysiert wurden. Das ist besonders hilfreich, wenn du planst, mehrere Berichte zu erstellen. Wähle anschließend „**Fortinet FortiGate**“ als Datenquelle aus – natürlich solltest du hier das Gerät wählen, das zu deiner Umgebung passt. Falls dein Gerätetyp nicht in der Liste enthalten ist, kannst du ein benutzerdefiniertes Protokollformat auswählen und konfigurieren.

Wähle nun die Protokolldateien aus, die du analysieren möchtest. Du kannst bis zu 20 verschiedene Dateien mit einer Gesamtgröße von maximal 1 GB hochladen. Klicke abschließend auf „**Protokolle hochladen**“.

Sobald die Dateien hochgeladen wurden, beginnt MDCA automatisch mit der Verarbeitung. Je größer die Dateien, desto länger dauert der Vorgang. Den Fortschritt kannst du auf der Seite „**Momentaufnahmeberichte**“ verfolgen. Sobald MDCA die Analyse abgeschlossen hat, ändert sich der Status des Berichts von „**Verarbeitung**“ auf „**Bereit**“ oder „**Fehlgeschlagen**“. Administratoren werden zusätzlich per E-Mail informiert.

Falls beim Analysieren der Dateien ein Problem aufgetreten ist, wechselt der Status auf „**Fehlgeschlagen**“. Wenn du darauf klickst, erhältst du weitere Details zur Ursache. Im Beispiel konnte MDCA keinen Datenverkehr aus den Protokollen bekannten Anwendungen zuordnen.

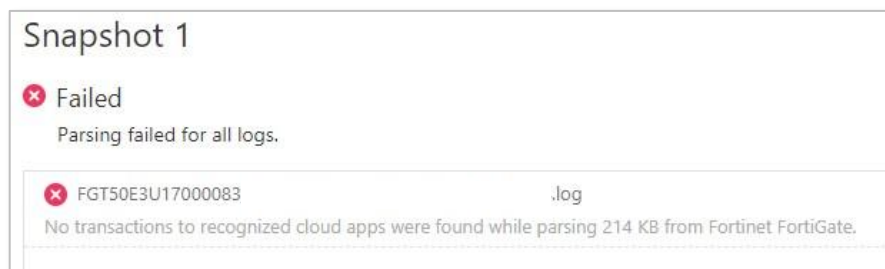


Abbildung 11-5: Details zu Fehlern bei einem Momentaufnahmebericht

**Hinweis:** Du kannst einen fehlgeschlagenen Bericht nicht durch das Hochladen neuer Protokolle korrigieren. Stattdessen musst du ihn löschen und neu beginnen.

# Automatisches Hochladen von Protokolldateien

## Hinzufügen einer Datenquelle und eines Protokollsammlers in MDCA

Bevor du einen fortlaufenden Bericht einrichten kannst, musst du automatische Protokoll-Uploads konfigurieren – das nennt sich auch das Hinzufügen einer Datenquelle. Anstatt eine Datei manuell hochzuladen, nutzt du FTP oder Syslog, um Protokolle direkt vom Gerät an MDCA weiterzuleiten.

Microsoft stellt mehrere Versionen des Protokollsammlers bereit, alle basierend auf einem Docker-Image:

- Windows
- Ubuntu
- Red Hat Enterprise Linux
- CentOS

Viele Organisationen bevorzugen möglicherweise die Windows-Version, da Linux-Kenntnisse fehlen. Obwohl die Windows-Variante offiziell unterstützt wird, hat sie gewisse Nachteile. Zum Beispiel muss ein lokaler Benutzer in Windows angemeldet sein, damit Docker aktiv bleibt und Protokolle sammeln kann.

Meiner Erfahrung nach sind die Linux-Versionen eine deutlich geeignetere Alternative. Besonders in Azure ist die Bereitstellung [unkompliziert und einfach zu befolgen](#). Daher wiederholen wir die Installationsdetails hier nicht. Aus übergeordneter Sicht sind folgende Schritte erforderlich:

1. Füge in MDCA eine neue Datenquelle hinzu. Gehe dazu auf **Einstellungen > Cloud-Apps > Cloud Discovery** und klicke auf **Automatischer Protokoll-Upload**. Danach auf **Datenquelle hinzufügen...** Folge dem Assistenten und kopiere die Konfiguration des Sammlers.
2. Stelle eine virtuelle Maschine - lokal oder in Azure - mit einem der unterstützten Betriebssysteme.
3. Stelle sicher, dass alle notwendigen Firewall-Ports offen sind, eingehend wie ausgehend. Je nach deiner Umgebung entscheidest du, ob UDP oder TCP verwendet wird. Standardmäßig läuft Syslog über UDP-Port 514. Möchtest du mehr Sicherheit, kannst du auf TCP wechseln und TLS zur Absicherung der Verbindung nutzen.
4. Installiere Docker
5. Stelle die kopierte Konfiguration für den Container bereit.

**Standort des Protokollsammlers:** Ob du einen Sammler lokal oder in der Cloud (z. B. Azure) hostest, spielt für MDCA keine wirkliche Rolle. Entscheidend ist, wo deine Anwendungen und

Geräte sich befinden und wie gut die Konnektivität zum Sammler ist. Die Azure-Bereitstellung ist aus meiner Sicht besonders einfach, aber möglicherweise nicht für alle Szenarien optimal.

## Hinzufügen von Datenquellen zu einem vorhandenen Protokollsammler

Ein einzelner Protokollsammler kann mehrere Datenquellen verarbeiten. Um zusätzliche Quellen hinzuzufügen, musst du den Sammler jedoch löschen und neu bereitstellen.

**Hinweis:** Du kannst den selben Protokollsammler nicht sowohl für Microsoft Defender für Cloud Apps als auch für Microsoft Sentinel verwenden. Auch wenn beide auf dem selben System laufen könnten, handelt es sich um zwei getrennte Instanzen mit unterschiedlichen Cloud-Anbindungen.

Füge also zunächst wie zuvor beschrieben eine neue Datenquelle hinzu. Navigiere dann zum Bereich „**Protokollsammler**“, klicke auf die Auslassungspunkte neben dem entsprechenden Connector und dann auf „**Bearbeiten**“. Wähle im Feld „Datenquellen“ die neu hinzugefügten aus und klicke auf „**Aktualisieren**“. Anschließend erhältst du eine aktualisierte Anleitung zur Bereitstellung des Sammlers. Vergiss nicht, den Befehl zu kopieren, den du im nächsten Schritt ausführen musst!

Melde dich auf der VM an, erhöhe deine Berechtigungen mit `sudo -i` und führe dann folgende Befehle aus:

```
Docker stop <LogCollectorName>
Docker rm <LogCollectorName>
```

Falls er läuft, stoppt der erste Befehl den Container. Der zweite Befehl entfernt das Image vom System. Führe nach Abschluss dieser Schritte den Befehl aus, den du zuvor beim Hinzufügen deiner Datenquellen zum vorhandenen Protokollsammler kopiert hast. Dieser Befehl wird dem vorherigen sehr ähnlich sein.

## Hochverfügbarkeit und Lastverteilung

In größeren Produktionsumgebungen möchtest du Protokolldateien wahrscheinlich auf zuverlässige Weise erfassen. In diesem Fall ist es immer eine gute Idee, eine hochverfügbare Protokollsammler-Infrastruktur einzurichten. Insgesamt ist dies kein besonders schwieriger Prozess und lässt sich in folgende Schritte unterteilen:

1. Richte eine zweite virtuelle Maschine ein, die als weiterer Protokollsammler fungieren kann.

2. Erstelle in Microsoft Defender for Cloud Apps (MDCA) einen zweiten Protokollsammler, denselben Datenquellen enthält wie der erste.
3. Konfiguriere den Protokollsammler in der zweiten VM mit den Informationen aus dem neu erstellten Protokollmeld
4. Verteile den eingehenden Syslog-Verkehr auf beide virtuellen Maschinen. Das bedeutet, dass Syslog-Nachrichten von deinen Geräten an einen der beiden Protokollsammler gesendet werden könnten. Von dort aus gelangen sie in MDCA.

Diese Einrichtung stellt sicher, dass der Datenfluss deiner Protokolldateien auch dann gewährleistet ist, wenn eine der beiden VMs nicht verfügbar ist.

Ein zusätzlicher Vorteil dieses Ansatzes ist die Lastverteilung: Durch das Hinzufügen eines oder mehrerer Protokollsammler kannst du die Verarbeitungslast besser verteilen. Besonders in größeren Umgebungen wirst du feststellen, dass ein einzelner Sammler schnell an seine Grenzen stößt, wenn er zu viele Datenquellen verarbeiten muss.

## Erstellen eines fortlaufenden Berichts

Nachdem du einen Protokollsammler eingerichtet hast, kannst du auf Basis der in MDCA erfassten Daten fortlaufende Berichte erstellen. Navigiere dazu zu **Fortlaufende Berichte** und klicke auf **Bericht erstellen**. Gib die gewünschten Details wie den Namen und Kommentare ein. Wähle dann entweder **Alle Datenquellen** oder **Bestimmte Datenquellen** aus. Wenn du Letzteres auswählst, kannst du auch gezielt den gerade eingerichteten Protokollsammler angeben.

Das Erstellen eines Berichts pro Protokollsammler ist sinnvoll, wenn du bestimmte Datenquellen isolieren möchtest – zum Beispiel, wenn du Daten von verschiedenen Standorten unabhängig voneinander betrachten willst. Du kannst aber auch mehrere Sammler auswählen, um einen aggregierten Bericht über mehrere Standorte hinweg zu erstellen – etwa, wenn verschiedene Geräte an einem Standort ihre Daten an unterschiedliche Protokollsammler senden.

## Fehlerbehebung beim Protokollsammler

In den meisten Fällen funktioniert der Docker-Container problemlos, wenn du die unten beschriebenen Schritte befolgst. In einigen Szenarien möchtest du jedoch möglicherweise einen genaueren Blick auf die Vorgänge im Protokollsammler werfen. Melde dich dazu zunächst bei der virtuellen Maschine an, auf der der Sammler läuft. Sobald du dich authentifiziert hast, erhöhe deine Berechtigungen, damit du mit dem Docker-Image interagieren kannst:

```
<user>@<host>:~$ Sudo -i
```

Als Erstes kannst du den Ressourcenverbrauch des Containers prüfen. Verwende dazu den folgenden Befehl – er zeigt dir die aktuelle Ressourcenauslastung an. Wenn du fertig bist, drücke **CTRL+C**, um zur Eingabeaufforderung zurückzukehren:

```
docker stats
CONTAINER ID      NAME                CPU %               MEM USAGE / LIMIT
MEM %            NET I/O            BLOCK I/O           PIDS
242a0f2c845f     LogCollector_Lochristi  0.07%              296.5MiB / 7.769GiB
3.73%            1.59MB / 460kB      0B / 27.4MB        32
```

Anschließend kannst du die Protokolle des Containers prüfen, um herauszufinden, ob beim Start des Sammlers Probleme aufgetreten sind.

### Docker logs -details <CollectorName>

Es werden mehrere Zeilen ausgegeben – die letzten vier sind dabei besonders wichtig. Sie sollten sich alle im Status **RUNNING** befinden.

```
2020-03-22 12:07:48,618 INFO spawned: 'rsyslog' with pid 921
2020-03-22 12:07:48,623 INFO spawned: 'ftpd' with pid 922
2020-03-22 12:07:48,626 INFO spawned: 'columbus' with pid 923
2020-03-22 12:07:50,596 INFO success: cron entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
2020-03-22 12:07:50,596 INFO success: rsyslog entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
2020-03-22 12:07:50,596 INFO success: ftpd entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
2020-03-22 12:07:50,596 INFO success: columbus entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
```

Die bisher genannten Befehle führst du direkt auf der virtuellen Maschine aus. Wenn du noch tiefer einsteigen möchtest, musst du eine Bash-Sitzung innerhalb des Containers starten. Achte dabei unbedingt auf die korrekte Groß- und Kleinschreibung im Containernamen!

```
root@vm:# docker exec -it LogCollectorName bash
```

Wenn die Sitzung erfolgreich geöffnet wurde, befindest du dich nun innerhalb des Containers. Dort findest du mehrere relevante Protokolldateien. Die allgemeinen Statusprotokolle liegen unter **/var/adallom/status**. Um anzuzeigen, welche Dateien verfügbar sind, verwende den folgenden Befehl:

```
root@242a0f2c845f:/# cd /var/adallom/status/
root@242a0f2c845f:/var/adallom/status# ls
lastConfigured lastConnected localState runStartTime
```



Wie du siehst, gibt es vier Statusprotokolle. Um den Inhalt anzuzeigen, gib den entsprechenden Befehl ein. Du kannst dies auch für die anderen Dateien wiederholen.

```
root@242a0f2c845f:/var/adallom/status# more localState OK
```

Der Protokollsammler kann eingehende Daten auf verschiedene Weise empfangen – beispielsweise über FTP oder Syslog. Jeder Typ hat dabei seinen eigenen Ordner mit spezifischen Protokolldateien. Die Syslog-Dateien findest du unter **/var/adallom/syslog**. Dort gibt es wiederum Unterordner für die verschiedenen Verbindungsarten: z. B. **514** für UDP oder **601** für TCP. In jedem dieser Ordner befindet sich eine Datei namens **messages**, die die empfangenen Syslog-Nachrichten enthält. Um deren Inhalt anzuzeigen, verwende diesen Befehl:

```
root@1a8f6b9461eb:/var/adallom/syslog/514# more messages
Mar 22 15:06:05 84.199.232.146 U7PG2,802aa8c90297,v4.0.42.10433: logread[27146]:
Logread connected to 104.47.150.179:514
Mar 22 15:06:05 84.199.232.146 U7PG2,18e829697f7f,v4.0.42.10433: logread[8722]:
Logread connected to 104.47.150.179:514
Mar 22 15:06:08 84.199.232.146 U7PG2,18e829697f7f,v4.0.42.10433: hostapd: ath3: STA
18:e8:29:6b:7f:7f DRIVER: Sead AUTH addr=50:de:06:2b:fd:12 status_code=0
...
```

Beachte, dass die Ordnerstruktur leicht variieren kann. So befinden sich beispielsweise die relevanten Protokolle für den FTP-Listener in unterschiedlichen Unterordnern unter **/var/adallom/ftp/discovery/**.

Wenn du nachvollziehen möchtest, was beim Hochladen der Daten zu MDCA passiert, findest du hilfreiche Informationen im Ordner **/var/log/adallom/columbus**:

```
root@1a8f6b9461eb:/var/log/adallom/columbus# ls dbwrites.log
error.log events.log headers.log info.log trace.log
```

Besonders die Datei **trace.log** ist oft sehr nützlich, da sie z. B. Verbindungsversuche zum MDCA-Portal im Detail protokolliert. Bedenke jedoch: Diese Datei ist meist sehr ausführlich – daher lohnt es sich, zunächst nur die letzten Zeilen zu betrachten.

## Interpretieren von Ermittlungsberichten

Wenn die Protokolldateien korrekt verarbeitet wurden und Daten entdeckt wurden, gelangst du durch einen Klick auf den Status zum **Momentaufnahmebericht**, der wie im folgenden Bild dargestellt aussieht.

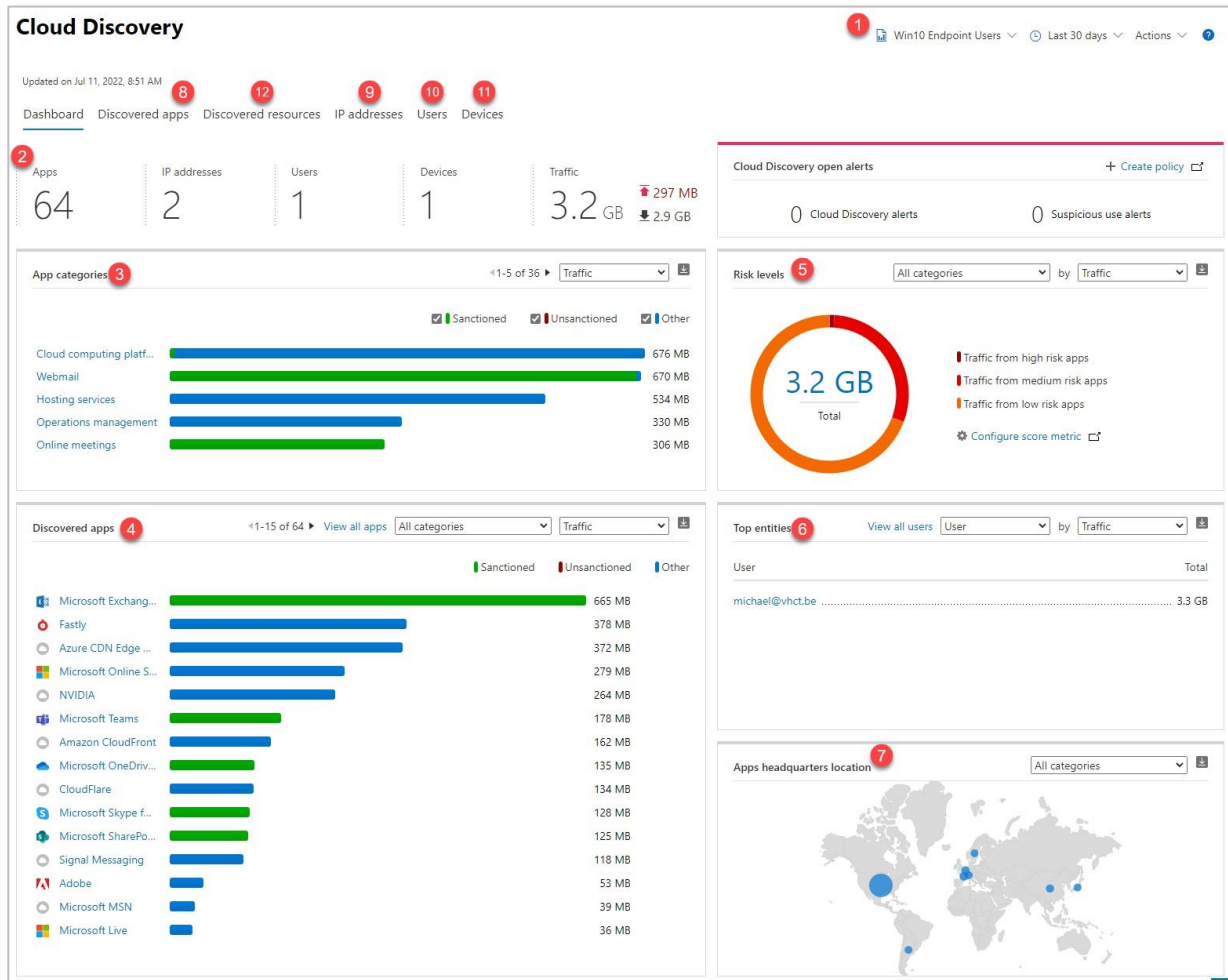


Abbildung 11-2: Ergebnisse einer Cloud Discovery (Snapshot) Bericht

Das Dashboard besteht aus verschiedenen Widgets und Optionen, mit denen du den Bericht effektiv analysieren und gezielt Informationen herausfiltern kannst:

1. Verwende die Berichtsauswahl (1) um zwischen (Snapshot) Berichten zu wechseln.
2. Die High-Level-Übersicht (2) zeigt einige Gesamtmetriken des Berichts an.
3. **App-Kategorien** (3) geben dir mehr Einblicke wie Anwendungen genutzt wurden. In diesem Widget kannst du Daten nach verschiedenen Kriterien filtern – zum Beispiel nach hochgeladene Datenmenge, der Anzahl der Transaktionen oder der Anzahl der Anwendungen pro Kategorie.
4. Das Widget **Entdeckte Apps** (4) bietet dir detaillierte Informationen zu den tatsächlich identifizierten Anwendungen. Auch hier kannst du filtern und gruppieren, um genau die Informationen hervorzuheben, die für dich interessant sind. Ich filtere regelmäßig nach **Cloud-Speicher** und **Upload**, was mir anzeigt, welche Datenmengen in Cloud-Speicheranwendungen hochgeladen wurden.
5. Im Widget **Risikoebenen** (5) findest du die Ergebnisse der berechneten Risikobewertung der entdeckten Anwendungen. MDCA pflegt eine Datenbank mit Anwendungen, für die

es eine Risikobewertung generiert und aktuell gehalten wird. Diese Bewertung basiert auf verschiedenen Kriterien wie der Einhaltung regulatorischen Anforderungen (zum Beispiel DSGVO), den verwendeten Verschlüsselungsprotokolle oder der Verfügbarkeit von Multi-Faktor-Authentifizierung. Wie im Abschnitt "Erste Schritte" erklärt, kannst du die Risikobewertung beeinflussen, indem du die Gewichtung einiger Bewertungskriterien anpasst. Wenn du gezielt Details zu einem bestimmten Risikoniveau suchst – etwa alle **Anwendungen mit hohem Risiko** - genügt ein Klick auf den Linkd im Widget. Du wirst direkt zum Tab **Entdeckte Apps** (8) weitergeleitet, wo die Ergebnisse für diesen Filter vorselektiert sind.

6. Unter **Top-Entitäten** (6) kannst du Ergebnisse nach Benutzern oder IP-Adressen filtern. Beachte, dass Benutzerdaten nur angezeigt werden, wenn MDCA den Datenverkehr einem bestimmten Benutzer zuordnen konnte. Bei der Auswahl von IP-Adressen siehst du die Quell-IP-Adressen. Diese Informationen kannst du anschließend verwenden, um sie bestimmten Geräten zuzuordnen und so möglicherweise den Benutzer zu identifizieren.
7. **App-Unternehmenssitz** zeigt dir, wo sich der Hauptsitz der entdeckten Anwendungen befindet. Ich persönlich nutze das nicht sehr oft, aber es kann hilfreich sein, wenn die Nutzung von Anwendungen aus bestimmten Ländern untersagt ist – oder einfach als interessanter Hintergrund.
8. Der Tab **Entdeckte Ressourcen** ermöglicht es dir, Cloud-Ressourcen wie Storage Blobs, benutzerdefinierte Apps, Storage Buckets und weitere Ressourcen anzuzeigen, sofern Netzwerkverkehrsprotokolle mit spezifischen Ziel-URL-Daten vorliegen. Auch wenn du Amazon AWS, Azure oder Google Cloud verbunden hast, werden hier ohne aktivierte Netzwerkverkehrsprotokolle keine Daten angezeigt.

Die meisten Widgets verfügen über einen Download-Button, mit dem du eine CSV-Datei mit den Rohdaten des aktuellen Widgets exportieren kannst. Diese Daten kannst du für eigene Auswertungen oder als Eingabe für von dir entwickelte Skripte nutzen.

**Praxis:** Ein Kunde, mit dem ich in der Vergangenheit gearbeitet habe, nutzte die exportieren Daten, um eine Liste zu erstellen, welche Benutzer versucht hatten, sich mit nicht genehmigten Anwendungen zu verbinden. Das Skript verwendete die von MDCA generierte CSV-Datei und versendete automatische eine E-Mail an die betroffenen Benutzer, um sie an die Unternehmensrichtlinie zu erinnern. Es gäbe auch automatisierte Wege über Power Automate oder Azure Automation, aber der Kunde wollte bewusst eine Manuelle Lösung mit kontrollierter Aktion.

Der Tab „**Entdeckte Apps**“ (8) ist wahrscheinlich der Ort, an dem du bei der Analyse eines Berichts die meiste Zeit verbringen wirst. Im Gegensatz zum Hauptdashboard findest du hier deutlich mehr Details. Du kannst auf Informationen bis zur Anwendungsebene einzoomen. Je tiefer du gehst, desto spezifischer werden die Daten. So kannst du etwa sehen, welche Entitäten (Benutzer oder IP-Adressen) auf eine bestimmte Anwendung zugegriffen haben und wie viele Daten dabei übertragen wurden. Oder du lässt dir die vollständige Risikobewertung

einer Anwendung anzeigen. Beachte, dass diese Informationen auch jederzeit über den **Cloud-App-Katalog** im Hauptmenü zugänglich sind.

Die Benutzeroberfläche ermöglicht dir eine einfache Navigation durch die Daten und eine gezielte Visualisierung. Du kannst beispielsweise auf einen Benutzer klicken und wirst automatisch zur benutzerspezifischen Seite weitergeleitet.

Je nachdem, wer den Bericht auswertet, kann der Fokus variieren. Ein Compliance-Beauftragter interessiert sich möglicherweise besonders für Anwendungen, die ein Risiko in Bezug auf bestimmte Compliance-Frameworks darstellen. Er oder sie würde die Daten entsprechend nach dem **Compliance-Risikofaktor** filtern – etwa nach ISO 27001 oder SOC 3. Denke daran: Die Risikobewertung wird von Microsoft berechnet, lässt sich aber über die Gewichtung der einzelnen Bewertungskriterien anpassen. Falls das nicht ausreicht, kannst du die Bewertung auch manuell überschreiben. Klicke dazu auf die Auslassungspunkte neben einer Anwendung und wähle „**App-Bewertung überschreiben**“.

**Praxis:** Immer wenn du eine neue Abfrage zum Filtern von Daten erstellst, kann es sinnvoll sein, sie zu speichern. So musst sie später nicht erneut manuell erstellen. Gespeicherte Abfragen findest du in der Dropdown-Liste unter **Abfragen**.

Die Tabs „**IP-Adressen**“ (9), „**Benutzer**“ (10) und „**Geräte**“ (11) ermöglichen dir, dieselben Daten wie im Tab „**Entdeckte Apps**“ zu analysieren, jedoch aus einem anderen Blickwinkel. Statt von der Anwendung aus zu starten, beginnst du hier mit einer Entität und kannst dann bis zur Anwendungsebene einzoomen, um zu sehen, wie diese spezifische Entität mit Cloud-Anwendungen interagiert hat. Du könntest zum Beispiel eine IP-Adresse auswählen und analysieren, welche Datenmengen auf Cloud-Speicherplattformen hochgeladen wurden oder welche Anwendungen von dieser IP-Adresse aus genutzt wurden.

## Überwachen und Sichern von Aktivitäten

Eine weitere zentrale Funktion einer CASB besteht darin, die Nutzung von Cloud-Anwendungen oder die darin enthaltenen Daten zu schützen. Doch was bedeutet das konkret? Für manche heißt das, bestimmte Anwendungen vollständig zu blockieren. Andere wollen bestimmte Aktionen – wie Uploads oder Downloads – gezielt überwachen und darauf reagieren.

Eine CASB kann proaktiv, reaktiv oder beides sein. Wenn eine CASB die Nutzung einer Cloud-Anwendung proaktiv schützen soll, muss sie in der Lage sein, in Echtzeit auf Benutzeraktionen zu reagieren. Dafür wird sie als Forward Proxy inline geschaltet. Wenn reaktive Maßnahmen ausreichen, kann sich die CASB auch auf gesammelte Informationen aus der Discovery-Phase, Sitzungsdaten oder – wenn verfügbar – auf API-Integrationen mit der Anwendung verlassen.

Bevor MDCA dir erweiterte Kontrollfunktionen für deine Cloud-Anwendungen bietet, muss es Zugriff auf die Daten dieser Anwendungen erhalten. Wie bereits erwähnt, gibt es zwei Arten der Integration: über eine API (App-Connector) oder als Proxy (Sitzungskontrollen).

Standardmäßig unterstützt MDCA die API-Integration mit mehreren Cloud-Anwendungen. Um die Liste zu sehen, navigiere zu „Einstellungen > **App-Connectors**“ und klicke auf „**App verbinden**“, um alle unterstützten Anwendungen anzuzeigen.

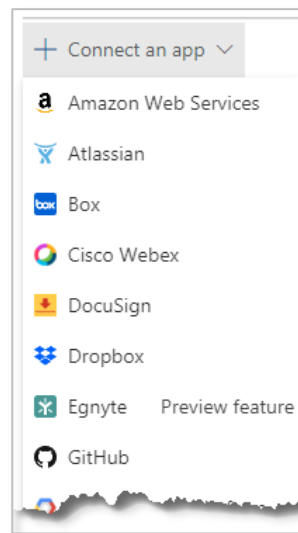


Abbildung 11-7: Überprüfung verfügbarer Cloudanwendungen mit API-Integration.

Auf den ersten Blick wirkt diese Liste möglicherweise eingeschränkt. Aber vergiss nicht: Auch wenn eine Anwendung keine API-Integration bietet, kannst du über Conditional Access App Controls (CAAC) dennoch Sitzungen steuern und Schutzmaßnahmen in vielen weiteren Anwendungen anwenden.

Beachte außerdem, dass nicht alle Funktionen in MDCA von allen Cloud-Anwendungen unterstützt werden. Eine vollständige Übersicht, welche Funktionen bei welcher Anwendung zur Verfügung stehen, findest du [hier](#).

## Verbinden einer Anwendung über App-Connectors

Das Einrichten eines App-Connectors ist unkompliziert. In diesem Beispiel verbindest du Office 365 mit MDCA. Navigiere zu „**Einstellungen > Cloud-Apps**“ und klicke auf „App-Connectors“. Wähle anschließend „**App verbinden**“ und dann Office 365 (oder eine andere gewünschte Anwendung) aus.

Auf der Connector-Seite kannst du die Komponenten auswählen, die du verbinden möchtest, und klickst dann auf „**Verbinden**“.

**Praxis:** Jede Cloud-Anwendung, die du über einen App-Connector verbindest, kann bestimmte Voraussetzungen mitbringen. Damit du zum Beispiel alle MDCA-Funktionen mit Office 365 nutzen kannst, muss die Protokollierung über mehrere Workloads hinweg aktiviert sein. , Um Office 365-Dateien zu erfassen, musst du außerdem die Dateiüberwachung unter Einstellungen > Informationsschutz > **Dateien** aktivieren. Eine vollständige Liste der Anforderungen findest du ebenfalls über den oben genannten Link.

Nachdem du eine Anwendung mit MDCA verbunden hast, wird sie in der Liste der App-Connectors angezeigt. Wenn alles funktioniert und Protokolldateien empfangen werden, ist der Status des App-Connectors **Verbunden**. Wenn weitere Konfigurationsoptionen verfügbar sind, siehst du ganz rechts neben dem App-Connector ein Auslassungspunkte-Symbol. Wenn nicht, wie bei Microsoft Azure, gibt es dieses Symbol nicht.

**Praxis:** Nach Abschluss deiner ersten MDCA-Konfiguration gibt es eigentlich keinen Grund, warum du nicht sofort Office 365 und Azure verbinden solltest. Beide App-Connectors erfordern wenig bis gar keinen Aufwand bei der Einrichtung und liefern eine Fülle von Informationen.

## Verwenden von Richtlinien zur Überwachung und Kontrolle von Cloud-Anwendungen

In MDCA werden Richtlinien verwendet, um das Verhalten innerhalb geschützter Cloud-Anwendungen zu steuern oder um Warnungen zu generieren, wenn bestimmte Bedingungen – wie Richtlinienverstöße – erfüllt sind. Standardmäßig wird MDCA mit einer Vielzahl vordefinierter Richtlinien geliefert. Die meisten davon sind entweder bereits aktiviert oder werden automatisch aktiviert, wenn bestimmte Funktionen verwendet werden. Andere, wie die Malware-Erkennungsrichtlinie, müssen manuell aktiviert werden. Weitere Informationen zum Aktivieren dieser Richtlinie findest du später in diesem Kapitel unter *Malware-Erkennung*.

Es gibt verschiedene Arten von Richtlinien, die jeweils einem bestimmten Anwendungsfall dienen – von der Alarmierung bei anomaler Aktivität bis zur automatischen Ausführung von Aktionen, wenn ein bestimmtes Ereignis eintritt.

Die verschiedenen Arten von Richtlinien sind:

- **Cloud Discovery-Anomalieerkennung:** Diese Richtlinien basieren auf maschinellem Lernen und analysieren die Discovery-Protokolle, um neue Anwendungen oder ungewöhnliches Anwendungsverhalten zu erkennen. Eine Richtlinie kann beispielsweise erstellt werden, um zu erkennen, ob Daten exfiltriert werden. Dazu erstellt das System eine Baseline dessen, was es als normales Verhalten einstuft. Basierend darauf überwachen die Maschine-learning kontinuierlich die Aktivitäten und erkennen, wenn ein Benutzer große Datenmengen in eine Cloud-Speicherplattform hochlädt –



insbesondere, wenn diese Plattform selten oder vom Benutzer noch nie verwendet wurde.

- **App Discovery:** Mit diesen Richtlinien kannst du erkennen und alarmieren, wenn eine neue Cloud-Anwendung in der Umgebung verwendet wird.
- **Aktivität:** Eine Aktivitätsrichtlinie kann verwendet werden, um Aktivitäten in verbundenen Cloud- Anwendungen zu überwachen. Im Gegensatz zu Zugriffs- und Sitzungsrichtlinien funktionieren Aktivitätsrichtlinien nur mit Anwendungen, die eine API-Integration mit MDCA haben.
- **Anomalieerkennung:** Wie die Cloud-Discovery-Anomalieerkennungen kannst du auch hier ungewöhnliche Aktivitäten innerhalb einer Anwendung erkennen lassen. Eigene Anomalieerkennungsrichtlinien kannst du nicht erstellen – du musst auf vordefinierten Richtlinien zurückgreifen. In den meisten Fällen kannst du nur definieren, für welche Benutzer die Richtlinie gilt.
- **Datei:** Diese Richtlinien dienen der Überwachung von Dateien in deinen Cloud-Anwendungen. Du kannst nach bestimmten Inhalten suchen, automatisch Rechtsverwaltungsvorlagen anwenden oder definierte Aktionen ausführen lassen, wenn bestimmte Bedingungen erfüllt sind.
- **OAuth-App:** Auch diese Richtlinie dient der Erkennung. Anhand eines Kriterienkatalogs wirst du gewarnt, wenn bestimmte Schwellenwerte erreicht werden – etwas, wenn eine OAuth-App von einer bestimmten Anzahl an Benutzern autorisiert wurde oder wenn ihre Risikobewertung einen definierten Wert übersteigt. Es gibt auch vordefinierte Richtlinien zur Erkennung verdächtiger OAuth-Apps, etwas wenn diese bekanntermaßen Teil einer Phishing-Kampagne sind oder anderweitig böses Verhalten zeigen.
- **Zugriff:** Zugriffsrichtlinien überwachen in Echtzeit die Anmeldungen bei Anwendungen und ermöglichen dir, spezifische Kontrollen für diese Logis festlegen.
- **Sitzung:** Sitzungsrichtlinien bieten – wie Zugriffsrichtlinien - die Möglichkeit, Aktivitäten in Cloud-Anwendungen zu überwachen und bei Bedarf zu kontrollieren.

## Arbeiten mit Richtlinien

Um zu den Richtlinien zu navigieren, klicke im Menü auf **Richtlinien > Richtlinienverwaltung**. Du siehst dann einen Bildschirm wie in Abbildung 11-8. In der Übersicht werden dir Richtlinien mit allgemeinen Informationen angezeigt, wie der Anzahl aktiver (offener) Warnungen, dem eingestellten Schweregrad der Warnung und den zugewiesenen Aktionen. Ein Glockensymbol bedeutet beispielsweise, dass die Richtlinie lediglich eine Warnung generiert, während ein Blitzsymbol auf weitere definierte Aktionen (wie E-Mail- oder SMS-Versand) hinweist.

Wenn du die Seite öffnest, werden standardmäßig alle Richtlinien angezeigt. Da du vermutlich viele davon nutzen wirst, kannst du mit **Zurück/Weiter** am unteren Bildschirmrand zwischen den Seiten navigieren. Um gezielter zu arbeiten, kannst du auch zwischen den verschiedenen Richtlinienarten über die Registerkarten (1) wechseln oder Filteroptionen (2) nutzen. Einen eigenen Filter erstellst du über **Erweitert** (3) auf der rechten Seite.

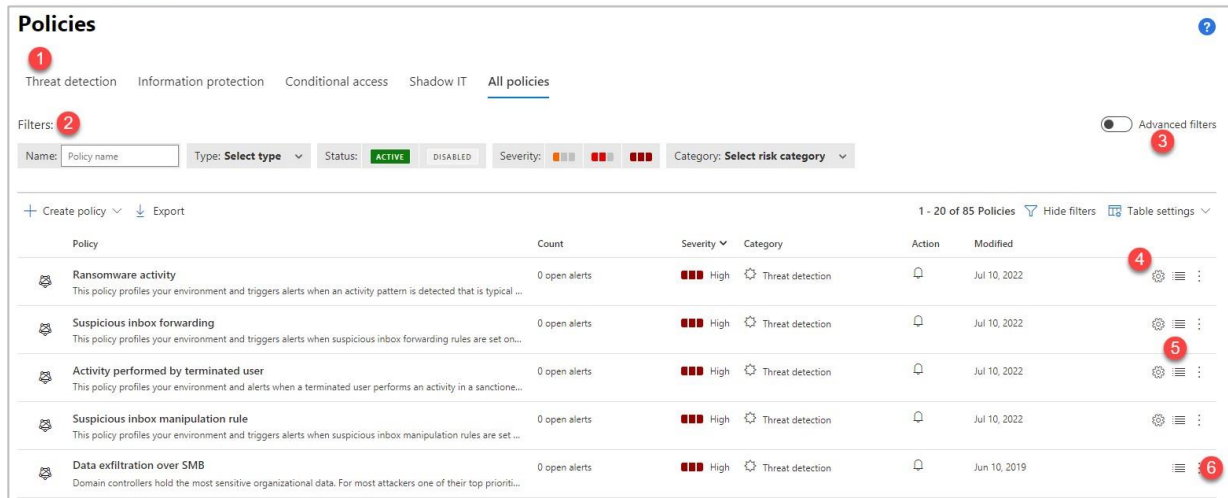


Abbildung 11-8: Arbeiten mit Richtlinien

Je nach Richtlinie stehen dir möglicherweise nicht alle Optionen zur Verfügung. In Abbildung 11-8 siehst du beispielsweise, dass bei der Richtlinie *Riskante Anmeldung* kaum etwas geändert werden kann – außer dem Schweregrad. Du kannst diese Richtlinie aber über die Auslassungspunkte (6) aktivieren oder deaktivieren.

Benutzerdefinierte und einige vordefinierte Richtlinien lassen sich bearbeiten – meist allerdings nur eingeschränkt. Typischerweise kannst du nur festlegen, für welche Benutzer sie gelten. Um das zu tun, klicke entweder auf den Namen der Richtlinie oder auf das Zahnradsymbol (4).

Um Richtlinienübereinstimmungen – also die Ereignisse, die die Richtlinie ausgelöst haben – einzusehen, klickst du auf das Listensymbol (5). Du gelangst damit zum Aktivitätsprotokoll dieser Richtlinie. Wie du das Aktivitätsprotokoll verwendest, erfährst du später im Kapitel *Untersuchung von Ereignissen*. Auch wenn die meisten Administratoren über eine Warnung zum Protokoll gelangen, ist der Zugriff von hier oft hilfreich, da du dort alle Aktivitäten einsehen kannst, die zu einer oder mehreren Warnungen geführt haben.

Die Richtlinienseite ist auch der Ort, an dem du eigene benutzerdefinierte Richtlinien erstellen kannst.

## Erstellen von Richtlinien

Nachdem du auf **Richtlinie erstellen** geklickt hast, wählst du den gewünschten Richtlinientyp aus. Je nach Auswahl erhältst du unterschiedliche Optionen. Das Seitenlayout bleibt jedoch in der Regel gleich.

Falls verfügbar, kannst du eine passende **Richtlinienvorlage** verwenden. Diese Vorlagen wurden von Microsoft bereitgestellt und bilden typische Anwendungsfälle ab. Sie sind besonders hilfreich, wenn du neu bei Defender for Cloud Apps bist. Wählst du eine Vorlage aus, wird die Seite aktualisiert, ein vorgefertigter Filter erstellt und Standardwerte konfiguriert. Du musst diese Werte nicht übernehmen, sondern kannst sie anpassen.

Wenn du keine Vorlage verwendest, definierst du alle Bedingungen selbst. Die benötigten Informationen variieren je nach Richtlinientyp. Bei einer Aktivitätsrichtlinie entscheidest du zum Beispiel, ob auf eine einzelne oder wiederholte Aktivität reagiert werden soll und welche Aktivitäten die Richtlinie auslösen. Eine Dateirichtlinie verlangt zusätzliche Angaben zu Dateityp oder Inhalt.

Der Filtermechanismus in MDCA ist sehr leistungsfähig. Durch Kombination verschiedener Bedingungen, Werte und Operatoren kannst du sehr spezifische Abfragen erstellen. Du könntest z. B. nach einer bestimmten Aktivität suchen, die von nicht konformen Geräten und aus unbekannten Standorten ausgeführt wurde. Diese Präzision hilft, Fehlalarme zu vermeiden und die wirklich relevanten Ereignisse zu erfassen.

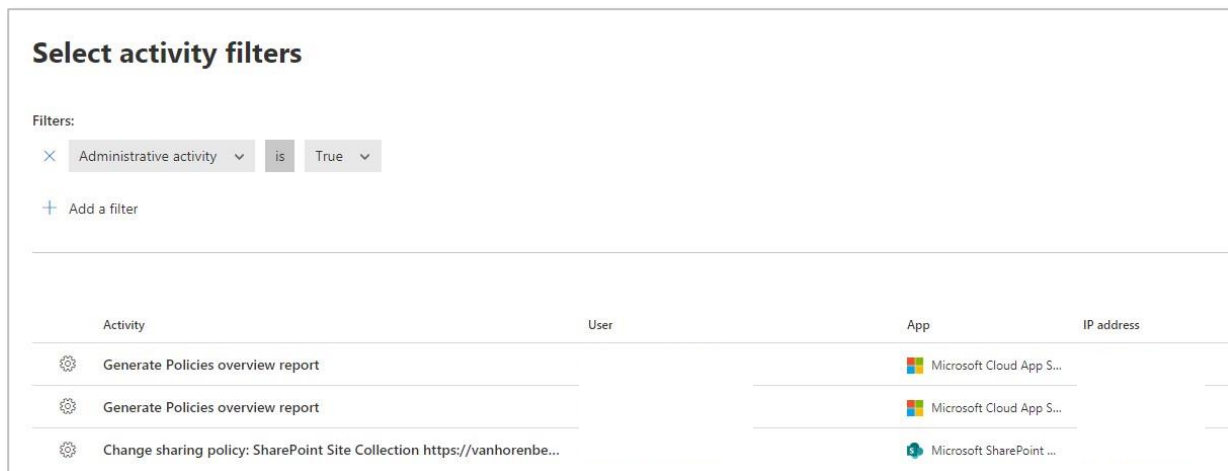


Abbildung 11-9: Arbeiten mit dem Filter in MDCA.

Sobald du die Bedingungen definiert hast, legst du fest, ob und wie du benachrichtigt werden willst – sowie, welche automatisierten Aktionen ausgeführt werden sollen. Wenn eine Warnung generiert wird, erscheint sie automatisch im Microsoft Security Graph. So kannst du sie auch mit anderen Tools wie Microsoft Sentinel weiterverarbeiten. Zusätzlich werden Warnungen in MDCA und im Microsoft 365 Defender angezeigt (siehe Kapitel 7).

Neben der Anzeige kannst du dich auch per E-Mail oder SMS benachrichtigen lassen. Standardmäßig begrenzt MDCA die Anzahl der Nachrichten pro Warnung, Empfänger und Tag. Das SMS-Limit liegt bei 10 Nachrichten pro Tag – mehr würde vermutlich nur stören. Auch E-Mail-Warnungen sind auf 500 Nachrichten pro Warnung und Tag begrenzt.

**Praxis:** Man könnte argumentieren, dass zu viele Warnungen durch eine einzelne Richtlinie deren Nutzen infrage stellen. Auch ich stimme dem grundsätzlich zu. In größeren Umgebungen muss jedoch mit einer entsprechend höheren Anzahl gerechnet werden. Zwar sind E-Mail-Warnungen weiterhin sinnvoll, aber viele Organisationen nutzen zusätzlich Service-Management-Lösungen. Wie du später im Kapitel "Integrationen von Drittanbietern und Automatisierung" sehen wirst, lassen sich solche Lösungen leicht über die Security Graph Api oder direkt über MDCA integrieren.

Schließlich kannst du für jede Richtlinie eine oder mehrere Governance-Aktionen definieren. Governance-Aktionen sind automatisierte Vorgänge, die jedes Mal ausgeführt werden, wenn eine Richtlinienübereinstimmung auftritt. Abhängig davon, welchen Richtlinientyp du ausgewählt hast oder von der jeweiligen Anwendung, stehen dir zahlreiche Optionen zur Verfügung. Eine Dateirichtlinie ermöglicht es dir beispielsweise unter anderem, eine Datei automatisch zu entfernen, Berechtigungen zum Teilen zu aktualisieren, eine Klassifizierungsbezeichnung anzuwenden oder zu entfernen und vieles mehr.

## Exportieren von Richtlinien

Auf der Hauptseite für Richtlinien kannst du außerdem einen Bericht über deine Richtlinien generieren. Ein solcher Bericht enthält eine Übersicht über alle Richtlinien auf der Seite, einschließlich Informationen über die generierten Warnungen (neu, offen und geschlossen) sowie über die in der Richtlinie erfassten Benutzer und Dateien – Letzteres gilt zum Beispiel bei einer Dateirichtlinie. Sobald du einen Bericht angefordert hast, findest du ihn im Abschnitt „Exportierte Berichte“ des Optionsmenüs.

## Automatisieren von Antworten durch Power Automate (Flow)

Trotz der vielen integrierten Aktionen kann es sein, dass du ein ganz bestimmtes Ergebnis erzielen oder sogar einen Workflow auslösen möchtest, der mehrere Aufgaben abdeckt. Mit Ausnahme einiger integrierter Richtlinien kannst du für jede Richtlinie einen Flow in Power Automate auslösen.

Mithilfe integrierter Connectors kannst du Flows erstellen, die viele weitere Aufgaben übernehmen – etwa die Verbindung zu einem anderen System oder die Ausführung eines Skripts. Dank der Flexibilität der Power-Automate-Plattform sind dir dabei praktisch keine Grenzen gesetzt. Lass deiner Fantasie freien Lauf!

Falls du noch keinen Flow für Microsoft Defender for Cloud Apps (MDCA) erstellt hast, kannst du auf „**Playbook in Power Automate erstellen**“ klicken – du wirst dann automatisch zu deiner Umgebung weitergeleitet. Dort kannst du einen neuen Flow erstellen. Microsoft stellt auch mehrere Vorlagen bereit, die du nutzen kannst. Selbst wenn diese deinen Anwendungsfall nicht exakt abbilden, ist es oft einfacher, eine Vorlage anzupassen, als einen Flow komplett neu zu entwickeln.

Es gibt mehrere Möglichkeiten, einen Flow basierend auf einer MDCA-Warnung auszulösen. Wenn du den Trigger „**Bei allen neuen Warnungen**“ oder „**Bei neuen Warnungen mit hohem Schweregrad**“ verwendest, wird dein Flow ausgelöst, sobald die Bedingung zutrifft – unabhängig davon, was in der Richtlinie festgelegt ist. Nur wenn du „**Wenn eine Warnung generiert wird**“ auswählst, wird dein Flow ausschließlich dann ausgelöst, wenn dies explizit in der Richtlinie angegeben wurde, wie in Abbildung 11-10 zu sehen ist:

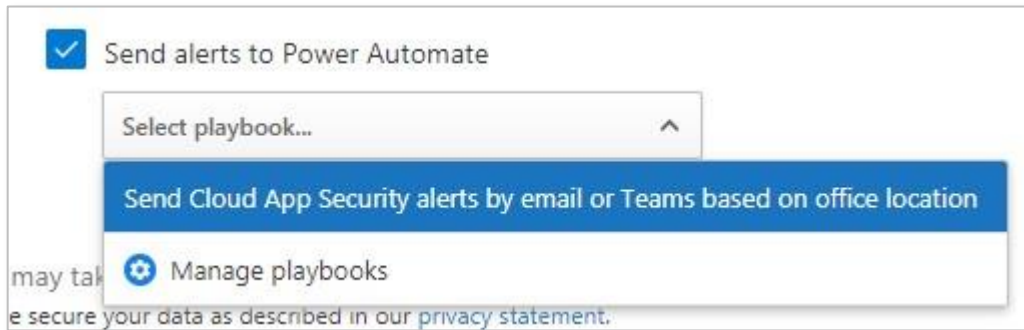


Abbildung 11-10: Festlegen eines Flows als automatisierte Aktion für eine Warnung

Wenn du mit der Erstellung deines Flows beginnst, wirst du zunächst nach Details gefragt, wie du dich mit MDCA verbinden möchtest. Weitere Informationen dazu findest du im Abschnitt „Integrationen und Automatisierung von Drittanbietern“.

Nachdem du deinen Flow erstellt hast, kannst du ins MDCA-Portal zurückkehren und ihn aus der Liste der verfügbaren Flows auswählen. Denk daran, dass du möglicherweise die Seite aktualisieren musst, bevor dein Flow erscheint.

**Realität:** Du kannst pro Richtlinien nur einen einzigen Flow auswählen. Falls du mehrere Workflows auslösen willst, musst du das innerhalb des Flows selbst umsetzen.

## Kontext ist wichtig

Einer der großen Vorteile von Defender for Cloud Apps ist, dass es von Microsoft entwickelt wurde und damit den Kontext sowie die Aktivitäten der integrierten Workloads vollständig versteht. Um dir zu zeigen, wie hilfreich das ist, schauen wir uns Microsoft Teams als Beispiel an.

Wenn du eine Richtlinie erstellen und nach bestimmten Aktivitäten suchen möchtest, wählst du den Filter „**Aktivitätstyp**“ und dann die Aktivität(en) aus, die dich interessieren. Je mehr Anwendungen du mit MDCA verbindest, desto länger wird diese Liste – und desto schwieriger wird es, die richtigen (unterstützten) Aktivitäten zu finden. Um gezielt zu filtern, genügt es, zuerst die App und dann den entsprechenden Aktivitätstyp auszuwählen, wie in der folgenden Abbildung dargestellt.

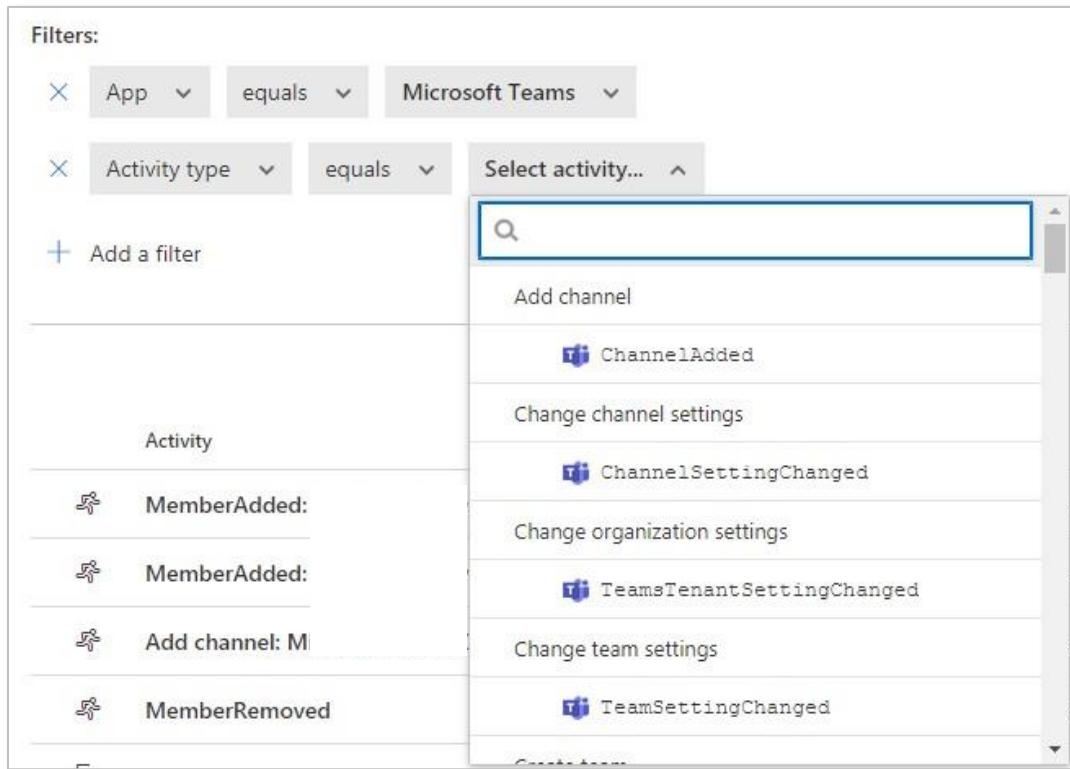


Abbildung 11-11: Liste der Aktivitäten basierend auf der/den ausgewählten App(s)

## Untersuchung von Ereignissen

### Die Rolle von Untersuchungen

Eine der wichtigsten Aufgaben in MDCA ist die Untersuchung von Warnungen, die vom System generiert werden. In vielerlei Hinsicht ähnelt das dem Threat Hunting – also der Verfolgung potenziell bösartiger Aktivitäten oder Malware. Ziel ist es herauszufinden, ob eine Aktion wirklich böswillig war und, wenn ja, welche Folgen sie hatte.

Obwohl MDCA bereits viele intelligente Mechanismen einsetzt, um Fehlalarme zu minimieren, ist der erste Schritt bei jeder Warnung immer derselbe: Du musst prüfen, ob die Warnung gerechtfertigt ist. Wenn ja, kannst du entsprechende Maßnahmen einleiten. In einigen Fällen lässt sich eine Warnung automatisch als „True Positive“ einstufen – dann ist eine automatische Aktion die effizienteste Lösung. Es gibt aber auch viele Szenarien, in denen das weder möglich noch sinnvoll ist. In solchen Fällen ist es besonders wichtig, schnell zwischen verschiedenen Ansichten zu navigieren, um die Untersuchung effizient durchzuführen.



## Überprüfung von Warnungen über MDCA

Warnungen, die von Defender for Cloud Apps ausgelöst werden, findest du auf der Seite „**Warnungen**“, die du direkt über das Hauptmenü auf der linken Seite erreichst. Auf dieser Seite stehen dir mehrere Optionen zur Verfügung, um die Warnungen gezielt zu durchsuchen und zu filtern – besonders hilfreich, wenn du dich auf einen bestimmten Warnungstyp konzentrieren möchtest:

The screenshot shows the 'Alerts' page in MDCA. It features a filter section at the top with various dropdowns and buttons. Below the filters is a table of alerts. Numbered callouts are placed as follows: 1 points to the 'Advanced filters' toggle; 2 points to the 'Hide filters' and 'Table settings' links; 3 points to the 'Bulk selection' and 'Export' buttons; 4 points to the first alert entry in the table; 5 points to the vertical ellipsis menu on the right of the first alert entry.

Alert	Status	Resolution type	Severity	Date
System alert: Deprecation of Label Management in the Azure Portal Microsoft Cloud App Security	OPEN	—	High	2/24/21, 8:00 AM
System alert: Deprecation of Label Management in the Azure Portal Microsoft Cloud App Security	OPEN	—	High	2/17/21, 7:24 AM
Impossible travel activity Impossible travel	OPEN	—	Medium	2/2/21, 9:29 PM
Impossible travel activity Impossible travel Microsoft Exchange Online	OPEN	—	Medium	1/31/21, 9:43 PM
Impossible travel activity Impossible travel	OPEN	—	Medium	1/17/21, 11:29 AM

Abbildung 11-12: Überprüfen von Warnungen in MDCA

Die Seite für Warnungen ist ähnlich aufgebaut wie andere Bereiche in MDCA. Im oberen Abschnitt (1) kannst du nach bestimmten Kriterien filtern. Wenn dir die vordefinierten Filter nicht ausreichen, kannst du den erweiterten Filter nutzen und eine eigene Abfrage formulieren. Der Abfrage-BUILDER funktioniert ähnlich wie beim Erstellen einer neuen Richtlinie.

Oben rechts im Haupt-Dashboard (2) findest du Optionen zum Schließen des Filters, zum Exportieren der Ergebnisse oder um mehr Einträge gleichzeitig anzuzeigen. Auf der linken Seite befindet sich die Auswahl-schaltfläche (3), mit der du Massenaktionen auf Warnungen anwenden kannst – etwa, um mehrere Warnungen gleichzeitig manuell zu schließen.

Die eigentlichen Warnungen (4) werden im unteren Bereich des Dashboards angezeigt. Achte auch auf die Auslassungspunkte rechts neben jeder Warnung (5): Darüber kannst du eine Warnung schnell schließen oder kategorisieren.

Wenn du auf eine Warnung klickst, gelangst du zur Detailseite, die unter anderem folgende Informationen enthält:

- Eine allgemeine Übersicht über die Warnung und die beteiligten Entitäten. Jeder Punkt ist anklickbar und führt dich zur Detailansicht der jeweiligen Entität.
- Eine kurze Beschreibung der Warnung.
- Hervorgehobene Informationen, die dir helfen, schnell zu erkennen, was die Warnung ausgelöst hat.
- Weitere Details zum Ereignis und/oder unter welcher MITRE-Taktik die Warnung klassifiziert wurde.
- Ein Auszug aus dem Aktivitätsprotokoll (weitere Informationen unten).

The screenshot shows the 'Impossible travel activity' alert detail page in Microsoft Defender for Cloud Apps. The page is divided into several sections:

- Alert summary:** Shows the alert title 'Impossible travel activity', priority '5', and the application 'Microsoft Exchange Online'.
- Alert story:** A section for the alert's history.
- What happened:** A text description stating that a user was involved in an impossible travel incident, connecting from two countries within 264 minutes from IP addresses in Belgium and the United States.
- Important information:** A list of key details, including that the user is an administrator in Office 365 and that certain IP addresses were used for the first time in 180 days.
- Related activities:** A table showing 28 items of related activity, including commands like 'Run command: task Ma...' and 'Create item: email RgA...', and logon events for Office 365.
- Alert state:** Shows the classification as 'Not Set' and the assigned state as 'Unassigned'.
- Evidence:** A table with columns 'Entity Name', 'Remediation Status', and 'Verdict', showing multiple instances of 'Unknown'.
- Alert Policy:** A link to 'View policy on Microsoft Defender for Cloud App'.
- Incident details:** Shows the incident name 'Impossible travel activity involving one user' and its severity as 'Medium'.
- Active alerts:** A summary bar showing 1/1 active alerts, 0 devices, 1 user, 0 mailboxes, and 1 app.
- Impacted assets:** A section for users involved in the incident, showing 1 user.

Abbildung 11-13: Überprüfen einer von Microsoft Defender for Cloud Apps generierten Warnung

Wie die meisten anderen Seiten in MDCA ist auch die Detailseite für Warnungen sehr interaktiv. Mit den meisten der auf der Seite angezeigten Objekte kannst du interagieren. Sie führen dich entweder auf eine andere Seite mit zusätzlichen Informationen oder zeigen Inhalte direkt inline an. Wenn du zum Beispiel auf eine der Aktivitäten klickst, wird darunter ein Detailbereich eingeblendet und es werden weitere relevante Informationen angezeigt (weitere Informationen findest du unter „Verwenden des Aktivitätsprotokolls“).

Eine weitere interessante Funktion auf der Seite ist die Möglichkeit, die Richtlinie, die die Warnung ausgelöst hat, sofort zu überprüfen und zu aktualisieren. In diesem Beispiel wurde eine integrierte Warnung („Unmögliche Reise“) ausgelöst. Klicke dazu auf der rechten Seite auf den Namen der Richtlinie. Dadurch wird die Richtlinienenseite geöffnet – genauso, als würdest du über **Richtlinien** > **Richtlinienverwaltung** navigieren. Wenn du über die entsprechenden Berechtigungen verfügst, kannst du die Richtlinie sofort anpassen. Das ist besonders hilfreich, wenn viele Fehlalarme generiert werden.

**Optimierung:** Nicht alle Warnungen lassen sich auf die gleiche Weise optimieren. Integrierte Richtlinien sind in der Regel stärker eingeschränkt als benutzerdefinierte Richtlinien. Vieles hängt auch davon ab, welche Art von Richtlinie du optimieren möchtest. In dem obigen Beispiel betrachten wir eine Aktivität zur unmöglichen Reise, die durch eine Richtlinie zur Anomalieerkennung ausgelöst wird.

Nachdem du nun die Warnungsseite kennengelernt hast, stellt sich die Frage: Wie gehst du bei der Untersuchung von Warnungen vor? Was ist der erste sinnvolle Schritt? Die Antwort ist nicht so eindeutig, wie man vielleicht denkt. Vieles hängt davon ab, um welche Warnung es sich handelt. Eine Warnung über eine unmögliche Reise unterscheidet sich offensichtlich stark von einem Versuch der Datenexfiltration. Die Maßnahmen, die du bei der Untersuchung ergreifst, hängen also stark von der Art der Bedrohung ab. Neben der Warnung selbst spielt auch der Kontext eine entscheidende Rolle.

Schauen wir uns noch einmal die Warnung „Unmögliche Reise“ an. In manchen Organisationen deutet sie fast immer auf eine verdächtige Aktivität hin. In anderen – insbesondere dort, wo Mitarbeitende häufig reisen – kann diese Warnung viele Fehlalarme erzeugen. Solche Fehlalarme entstehen aus unterschiedlichen Gründen. Wenn jemand beispielsweise ins Ausland reist und gleichzeitig sein Laptop (über VPN) und sein Mobilgerät verwendet, kann es sein, dass das Laptop als aus dem Unternehmensnetzwerk stammend erkannt wird, während das Mobilgerät sich über einen ganz anderen Standort verbindet. Das kann eine Warnung über eine unmögliche Reise auslösen. Obwohl es sich dann technisch um einen Fehlalarm handelt, sieht es aus Sicht der Daten wie ein echter Treffer aus – der Kontext fehlt.

Das zeigt: Es gibt keinen universellen Trick, mit dem du alle Warnungen richtig einschätzt. Wie du mit einer Warnung umgehst, hängt von der Warnung selbst, den betroffenen Aktivitäten, den beteiligten Entitäten und vielen weiteren Faktoren ab. Wenn es aber eine Regel gibt, dann die: Du solltest die verschiedenen Parameter der Warnung genau prüfen und bewerten, ob es

sich um eine echte Bedrohung handelt. Die Detailseiten in MDCA sind Werkzeuge, die dir helfen sollen, den nötigen Kontext zu erfassen, um das besser beurteilen zu können.

Ich persönlich beginne nach dem Überblick über die allgemeinen Details meistens damit, zu prüfen, von wo aus die Aktivitäten durchgeführt wurden und welchen Ruf die dabei verwendeten IP-Adressen haben. Danach schaue ich mir den betroffenen Benutzer oder das betroffene Gerät an und versuche herauszufinden, ob etwas ungewöhnlich erscheint. Besonders aussagekräftig wird eine MDCA-Warnung, wenn sie von einer Endpoint-Warnung aus Microsoft Defender for Endpoint begleitet wird – das ist ein deutlicher Hinweis darauf, dass wirklich etwas nicht stimmt.

## Verwenden des Aktivitätsprotokolls

Im Aktivitätsprotokoll werden sämtliche Benutzeraktivitäten für die verschiedenen Cloud-Anwendungen erfasst, die mit MDCA verbunden sind. Welche Informationen genau im Protokoll landen, hängt vom Grad der Integration ab: Apps, die über eine API eingebunden sind, liefern deutlich mehr Details als Anwendungen, bei denen nur Sitzungsaktivitäten erfasst werden.

Es gibt verschiedene Wege, auf das Aktivitätsprotokoll zuzugreifen. Abhängig davon, von wo aus du das Protokoll öffnest, können unterschiedliche Filter bereits voreingestellt sein. Wenn du es zum Beispiel über eine Richtlinie aufrufst, siehst du nur Aktivitäten, die mit dieser Richtlinie zusammenhängen. Rufst du es hingegen über die Benutzerseite auf, werden dir nur Aktivitäten dieses Nutzers angezeigt.

Um das Aktivitätsprotokoll über das Hauptmenü zu öffnen, klickst du einfach auf „**Aktivitätsprotokoll**“. Es zeigt dir dann die zuletzt erfassten Aktivitäten an – wie in Abbildung 11-14 dargestellt:

**Realität:** In der Realität kann es je nach Datenquelle zu einer leichten Verzögerung kommen, bis Aktivitäten im Protokoll erscheinen – insbesondere bei Aktivitäten, die über APIs erfasst werden. Diese Verzögerung kann mehrere Minuten betragen.

## Activity log

Queries: Select a query 1 Save as 3 Advanced filters

App: Select apps... User name: Select users... Raw IP address: Enter IP address... Activity type: Select activity...

Location: Select countries/regions... 2

+ New policy from search Export 1 - 20 of 5,000+ activities Show details Hide filters Table settings

Activity	User	App	IP address	Location	Device	Date
Access file: file https://v...		Microsoft ...	84.199.232.146 <span>6</span>	Belgium	Windows	Feb 28, 2021, ... <span>4</span>
FileModifiedExtended: f... <span>5</span>		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
Modify file: file https://...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
FileAccessedExtended: f...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
FileAccessedExtended: f...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
FileModifiedExtended: f...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
FileModifiedExtended: f...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...
FileAccessedExtended: f...		Microsoft ...	84.199.232.146	Belgium	Windows	Feb 28, 2021, ...

Abbildung 11-14: Einträge im Aktivitätsprotokoll

Oben auf der Seite kannst du mit Abfragen die Anzeige filtern. Aufgrund der großen Datenmenge im Aktivitätsprotokoll ist das eines deiner wichtigsten Werkzeuge. Die vordefinierten und gespeicherten Abfragen (1) sind besonders nützlich, um Aktivitäten nach Typ zu filtern – zum Beispiel Anmeldungen, Postfachzugriffe, Passwortänderungen oder Datei-Downloads. Mit dem Filter (2) kannst du dir eigene Ansichten zusammenstellen. Und mit den erweiterten Optionen kannst du sogar komplexe Abfragen definieren, die nur einen bestimmten Teil der Informationen anzeigen. Mit der Zeit wirst du sicher deine eigenen Lieblingsabfragen entwickeln!

Im Hauptbereich der Seite werden die Aktivitäten aufgelistet. Beachte, dass fast jede Eigenschaft einer Aktivität anklickbar ist, um weitere Details einzusehen. Wenn du auf die Auslassungspunkte rechts klickst (4), öffnet sich ein Menü mit Optionen – je nach Art der Aktivität etwa zum Anzeigen ähnlicher Warnungen oder aller Aktivitäten eines bestimmten Benutzers.

Ein Klick auf den Aktivitätsnamen (5) öffnet ein neues Detailfenster, wie in Abbildung 11-15 dargestellt. Hinweis: Der Screenshot zeigt aus Gründen der Übersicht nicht alle verfügbaren Informationen.

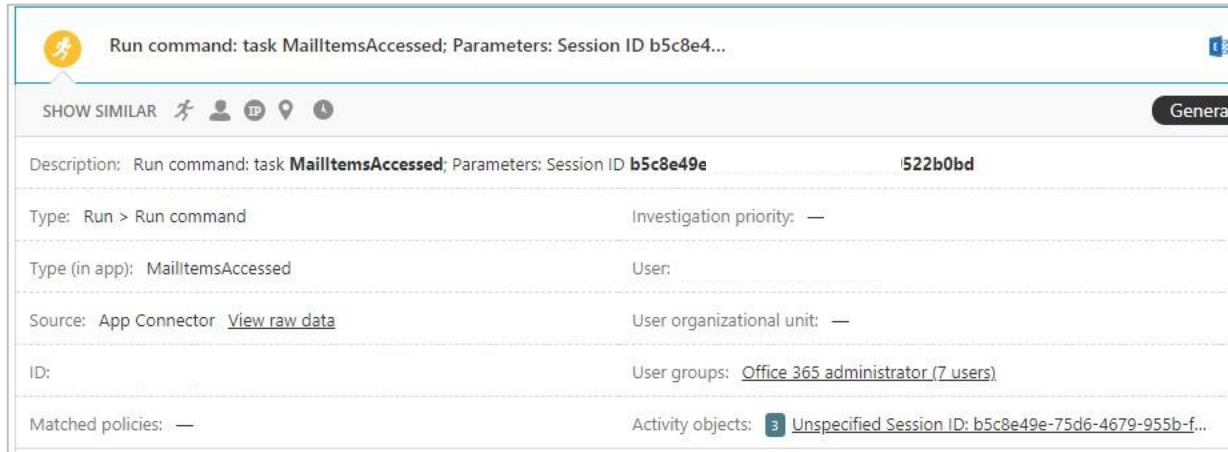


Abbildung 11-15: Aktivitätsdetails-Bereich

Viele Informationen sind in den Details zunächst ausgeblendet. Du kannst aber erkennen, welcher Benutzer beteiligt war, zu welchen Gruppen er gehört, welche Aktivität ausgeführt wurde, gegen welchen Dienst, und von welchem Standort aus. Einige Aktivitäten liefern dir auch Rohdaten der Warnung – darunter Angaben wie Prozessnamen oder den genauen Namen der betroffenen Datei oder Nachricht.

Du kannst außerdem auf den Namen des Benutzers oder die IP-Adresse klicken (6). Dabei werden dir relevante Informationen zum jeweiligen Objekt angezeigt. Klickst du zum Beispiel auf eine IP-Adresse, siehst du, wie oft sie im Protokoll erscheint, wem sie zugeordnet ist und aus welchem Land sie stammt. Von dort aus kannst du direkt alle Aktivitäten anzeigen, die mit dieser IP in Zusammenhang stehen. Genauso funktioniert es beim Benutzernamen – du erhältst eine Übersicht mit Statistiken zu den Aktivitäten, etwa aus welchen Ländern sie stammen, wie viele Aktionen durchgeführt wurden und wie viele Warnungen noch offen sind. Beachte: Bis hierhin hast du die Seite nicht gewechselt oder neu laden müssen – das macht schnelle Untersuchungen extrem effizient. Um zu vermeiden, dass du ständig zwischen Seiten wechseln musst, gibt es die praktische Slideout-Funktion für Benutzer- und IP-Adressinformationen. Diese erlaubt dir einige schnelle Aktionen – zum Beispiel:

- **Zugehörige Aktivitäten anzeigen** – öffnet das Protokoll in einer neuen Registerkarte, vorgefiltert auf den Benutzer.
- **Zugehörige Governance anzeigen** – zeigt spezifische Governance-Aktivitäten zu diesem Nutzer.
- **Zugehörige Warnungen anzeigen** – listet alle ähnlichen Warnungen zum Gleichen Benutzer auf.
- **Im Besitz befindliche Dateien anzeigen** – öffnet die Dateienansicht mit allen Dateien des Nutzer. Beachte, dass du die tatsächlichen Dateinamen der Dateien siehst, die dem Benutzer gehören!
- **Mit diesem Benutzer geteilte Dateien anzeigen** – zeigt alle Dateien, auf die der Nutzer Zugriff hat.
- **Azure AD-Kontoeinstellungen**



**Realität:** Die Datenfülle in MDCA - insbesondere bei API-gestützten Anwendungen – kann auch überwältigend wirken. Daher ist es wichtig klare Vereinbarungen zu treffen, wie du mit diesen Informationen umgehst. Achte darauf, dass Daten aus MDCA nicht außerhalb des vorgesehenen Kontextes verwendet werden. Werden Aktivitätsdetails missbraucht oder falsch interpretiert, kann das schnell zu ernsthaften Datenschutz- oder PR-Problemen führen.

Die oben genannten Aktionen beziehen sich alle auf die Untersuchung der Warnung und zielen darauf ab, so viele Informationen wie möglich zu erhalten. Mit den folgenden Aktionen, die nur für interne Benutzer verfügbar sind, kannst du auch schnell auf die Warnung reagieren!

- **Benutzer als kompromittiert bestätigen.** Dadurch wird bestätigt, dass die Aktivitäten nicht vom Benutzer ausgeführt wurden, und das Benutzerrisiko auf "hoch" gesetzt. Wenn du zuvor eine Benutzerrisiko-Richtlinie in Azure Identity Protection erstellt hast, unterliegt der Benutzer jetzt der Aktion, die einem "hohen" Risiko entspricht. Verwende diese Aktion nur, wenn du sicher bist, dass der Benutzer die Aktivitäten, die du untersuchst, nicht durchgeführt hat. Der Benutzer wird nicht nur aufgefordert, sich erneut anzumelden oder - schlimmer noch - gesperrt, sondern es ist auch ein starkes Signal an Microsoft: Die Details der Aktivität werden verwendet, um andere potenziell riskante Aktivitäten mit ähnlichen Eigenschaften zu identifizieren (zum Beispiel die IP-Adresse, von der aus Aktivitäten ausgeführt wurden usw.).
- **Benutzer auffordern, sich erneut anzumelden.** Wie es der Name sagt.
- **Benutzer sperren.** Dadurch wird das Benutzerkonto über Azure AD gesperrt.
- **Kontoeinstellungen in der App.** Dadurch wird die Profilseite des Benutzers in Azure AD geöffnet. Beachte, dass du die richtigen Berechtigungen benötigst, wenn du diese Details sehen möchtest.

Wenn du auf „**Zur Benutzerseite wechseln**“ klickst, wirst du zur Benutzerseite weitergeleitet. Diese Seite enthält viele der gleichen Informationen wie in der Zusammenfassung der Slideout-Ansicht, aber ein Großteil der Informationen wird auf eine andere Art und Weise dargestellt – standardmäßig erweitert oder mit zusätzlichen Informationen angereichert –, um dir schnell ein Verständnis für das mit dem Benutzer verbundene Risiko zu vermitteln. Zum Beispiel zeigt die Aktivitätsliste an, welche Aktionen des Benutzers in den letzten sieben Tagen zu einer Erhöhung der Risikobewertung beigetragen haben. Das ist hilfreich, da es dir möglicherweise dabei hilft, besser zu verstehen, auf welche Aktivitäten du dich bei diesem Benutzer konzentrieren solltest.

**Hinweis:** Wenn du auf den Link für ein externes Konto wie Gastkonten oder Dienstkonten von Microsoft klickst, gelangst du zu einer leeren Benutzerseite.

Für die IP-Adress-Slideout stehen die folgenden Aktionen zur Verfügung. Weitere Informationen zur Arbeit mit Tags findest du unter „IP-Adressbereiche und Tags“.

- **Als Unternehmens-IP markieren und zur Whitelist hinzufügen.** Dadurch wirst du aufgefordert, die IP-Adresse als Unternehmens-IP-Adresse zu markieren.

- **Als VPN-IP markieren und zur Whitelist hinzufügen.** Markiere die IP-Adresse als VPN-Adresse.
- **Als riskante IP markieren und zur Blacklist hinzufügen.** Markiere die IP-Adresse manuell als riskant.

## Governance-Protokoll

Zusätzlich zum Aktivitätsprotokoll gibt es auch das **Governance-Protokoll**. Im Gegensatz zum ersteren ist es nicht über die Menüoption „**Untersuchen**“ zugänglich, sondern über das allgemeine Menü „**Einstellungen**“ (Zahnrad).

Das Governance-Protokoll enthält Informationen über Aktionen, die im Rahmen einer Richtlinie oder spezifischer Aktionen für Dateien, Ordner und Konten von einem Administrator ausgeführt wurden. Daher ist der Zweck des Governance-Protokolls ein ganz anderer. Es ist besonders nützlich, wenn untersucht werden soll, ob – oder vielleicht sogar warum – eine bestimmte Aktion für einen Benutzer ausgeführt wurde.

## IP-Adressbereiche und Tags

Bei der Arbeit mit MDCA wirst du regelmäßig auf Warnungen, Ereignisse und Aktivitäten stoßen, bei denen es wichtig ist zu verstehen, von wo aus sie ausgeführt wurden. Schließlich ist das Öffnen eines Postfachs von einer bekannten, vertrauenswürdigen IP-Adresse nicht dasselbe wie das Öffnen desselben Postfachs von einem Host, von dem bekannt ist, dass er bösartig ist. Die Überwachung von IP-Adressen, ihren Standorten, ihrem Zweck usw. ist nicht einfach. Natürlich könntest du selbst eine Liste führen und jedes Mal darauf verweisen, wenn du Informationen über eine IP-Adresse nachschlagen musst, aber es ist viel einfacher, dies innerhalb der Anwendungen zu tun.

In MDCA kannst du IP-Adressgruppen erstellen und diesen Gruppen Tags zuweisen, damit es einfacher ist, eine IP-Adresse zu erkennen, wenn sie in den Aktivitätsprotokollen oder Warnungen auftaucht. MDCA wird mit mehreren vordefinierten IP-Adressbereichen ausgeliefert. Diese Bereiche bezeichnen verschiedene gängige Cloud-Anbieter wie Google Cloud, Microsoft Azure, Alibaba, Akamai Technologies, Salesforce usw. Sie werden von Microsoft erstellt und gepflegt, sodass du dich nicht darum kümmern musst. Das bedeutet auch, dass IP-Adressen, die zu einem dieser Cloud-Anbieter gehören, automatisch erkannt werden.

Du kannst auch deine eigenen IP-Adressbereiche erstellen. Es ist zum Beispiel eine gute Idee, eine Liste aller Unternehmens-IP-Adressen zu führen, damit sie richtig identifiziert und markiert werden. Das wird bei der Untersuchung von Aktivitäten hilfreich sein, da du IP-Adressen anhand ihrer Tags erkennen kannst, anstatt sie dir merken oder in einer separaten Datei oder Datenbank nachschlagen zu müssen. Thijs Lecomte hat einen [ausgezeichneten Artikel](#)

geschrieben, in dem beschrieben wird, wie du „Named Locations“ von Microsoft Entra ID mit MDCA synchronisieren kannst.

**Realität:** Benutzerdefinierte IP-Adressbereiche haben Vorrang vor den integrierten. Das bedeutet, dass, wenn du zusätzliche oder andere Informationen für eine bekannte IP-Adresse angibst, die von dir angegebenen Informationen verwendet werden.

Um deine eigenen IP-Adressbereiche zu erstellen, navigiere zum Einstellungsmenü (Zahnrad) und klicke auf „**IP-Adressbereiche**“. Auf der Seite „IP-Adressbereiche“ klickst du auf das Pluszeichen (blaue Schaltfläche). Ein Popup wie in Abbildung 11-16 wird geöffnet und erlaubt dir, einen neuen Bereich zu definieren:

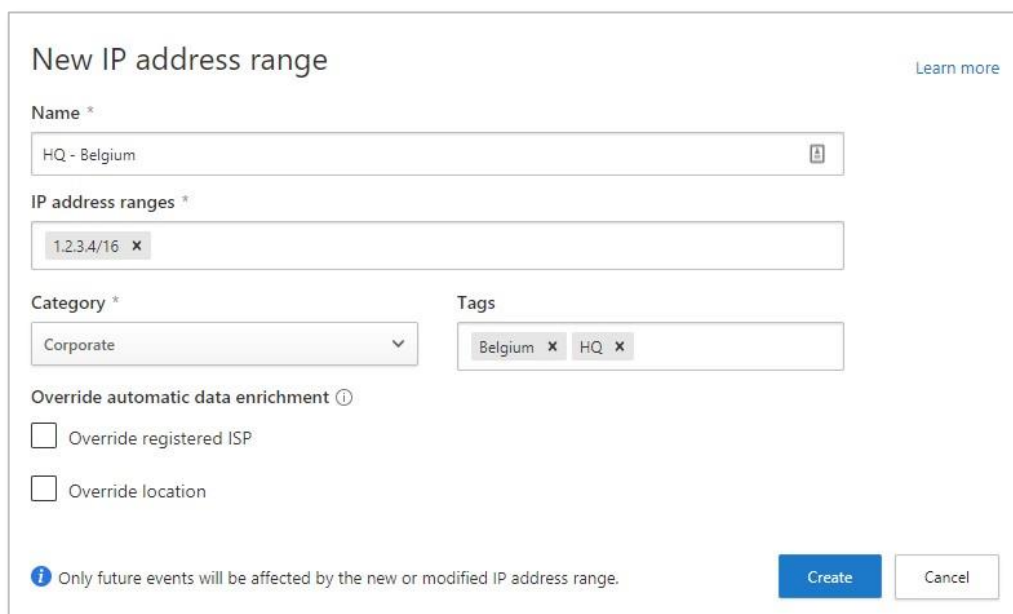


Abbildung 11-16: Definieren eines neuen IP-Adressbereichs

In diesem Beispiel haben wir einen neuen IP-Adressbereich für einen Unternehmensstandort (HQ – Belgien) erstellt. Das Eingabefeld für IP-Adressbereiche ermöglicht es dir, mehrere IP-Adressbereiche mit der CIDR-Notation hinzuzufügen. Um eine einzelne IP-Adresse hinzuzufügen, verwende die Subnetzmaske /32.

Die Dropdown-Liste „**Kategorie**“ ermöglicht die Auswahl einer bestimmten Kategorie. Kategorien sind:

- **Administrativ** - um IP-Adressen zu kennzeichnen, die von Benutzern mit Administratorrechten (Administratoren) verwendet werden
- **Cloud-Anbieter** - um anzugeben, welche IP-Adressen zu einem Cloud-Anbieter gehören, der nicht in den integrierten Listen enthalten ist.
- **Unternehmen** - um dein internes Netzwerk und deine Bürostandorte anzugeben.

- **Riskant** - um IP-Adressen anzugeben, die verdächtiges Verhalten zeigen oder wenn du sie aus einem anderen Threat Intelligence Feed (TI) erhalten hast
- **VPN** - um Mitarbeiter im Außendienst zu kennzeichnen, die sich über ein VPN verbinden.

Durch das Hinzufügen von **Tags** kannst du zusätzliche Informationen über die Kategorie hinaus einbeziehen. Es gibt eine Liste von integrierten Tags, aber du kannst auch eigene eingeben, indem du sie manuell hinzufügst.

Der Grund, warum es wichtig ist, eine Kategorie und relevante Tags einzubeziehen, ist, dass diese Informationen verwendet werden können, um Filter in der gesamten Lösung zu erstellen. Auf diese Weise kannst du den Umfang einer Richtlinie oder einer Aktivitätssuche eingrenzen (oder erweitern) und gezielter arbeiten, anstatt eine Vielzahl von Aktivitäten einbeziehen zu müssen, an denen du vielleicht gar nicht interessiert bist und die ansonsten mehr Zeit in Anspruch nehmen würden, um sie manuell zu ignorieren oder zu untersuchen.

**Hinweis:** Standardmäßig versucht MDCA, die von dir angegebenen Daten durch eine WHOIS-Abfrage der angegebenen IP-Adresse(n) anzureichern. Wenn du diese Informationen nicht verwenden möchtest, kannst du die registrierte IP oder den Standort, der mit den IP-Adressen verknüpft ist, überschreiben, indem du die Überschreibungen aktivierst.

## Arbeiten mit Benutzergruppen

Im Laufe deiner Bemühungen wirst du wahrscheinlich mehr als einen einzelnen Benutzer untersuchen müssen. Obwohl die meisten Filter die Angabe mehrerer Werte wie Benutzernamen zulassen, ist es viel einfacher, wenn du mit Gruppen arbeiten kannst: Anstatt einzelne Benutzernamen angeben zu müssen, kannst du eine Gruppe auswählen und loslegen. Die Verwendung von Gruppen ist nicht nur bei Untersuchungen nützlich, sondern auch zur Begrenzung von Richtlinien.

Wenn du Anwendungen wie Office 365 mit MDCA verbindest, werden einige Gruppen für dich erstellt. Zum Beispiel wird die Office 365-Administratorgruppe von MDCA erstellt und gepflegt und enthält automatisch alle Benutzer, die über globale Admin-, Unternehmensadmin-, Benutzeradmin-, Helpdeskadmin-, Dienstadmin- oder Abrechnungsadminberechtigungen verfügen. Die Gruppe der externen Benutzer umfasst alle Benutzerentitäten wie externe Dienstkonten oder Gastbenutzer.

Du kannst Gruppen nicht direkt in MDCA erstellen. Stattdessen musst du sie aus einer Quelle wie Entra ID importieren. Navigiere dazu zu **Einstellungen > Cloud-Apps** und wähle **Benutzergruppen** aus. Klicke dann auf **Benutzergruppe importieren** und wähle **Office 365 (Entra ID)** als Quelle aus. Du kannst nun auswählen, welche Gruppe du aus Entra ID importieren

möchtest. Nach einer kurzen Verzögerung werden importierte Gruppen automatisch gepflegt: Änderungen in Entra ID werden schließlich an MDCA weitergereicht.

## Verwalten von OAuth-Anwendungen

Die Verwendung von OAuth zur Interaktion mit anderen Cloud-Diensten oder den Daten eines Benutzers ist recht häufig: Viele SaaS-Anwendungen basieren entweder auf einer anwendungs- oder benutzerbezogenen Integration, um ihre Funktionalitäten bereitzustellen. Um das besser zu verstehen, lass uns ein gängiges Beispiel verwenden. Viele Benutzer nutzen eine Vielzahl von Drittanbieter-Anwendungen, die mit Daten aus beispielsweise ihrem Postfach interagieren. Eine solche Anwendung ist Boomerang. Im Folgenden wird das Konzept von OAuth und die Verwendung von Zustimmung zur Verbindung mit Benutzerdaten auf sehr hoher Ebene beschrieben. Dies soll keineswegs eine Vertiefung sein, da es noch viele andere Aspekte gibt, die wir an dieser Stelle nicht behandeln.

Um sich mit dem Postfach des Benutzers zu verbinden, benötigt Boomerang das, was gemeinhin als „Zustimmung“ bezeichnet wird. Um diese Zustimmung zu erhalten, fordert die Anwendung den Benutzer auf, bestimmte Berechtigungen zu genehmigen, wenn sie zum ersten Mal verwendet wird. Vorausgesetzt, Entra ID ist so konfiguriert, dass Benutzer einer Anwendung zustimmen können, kann Boomerang mit dem Postfach des Benutzers interagieren, sobald sie auf „Akzeptieren“ klicken. Für den Fall, dass Benutzer einer Anwendung nicht zustimmen können, muss ein Administrator dies entweder für sie tun oder eine Anwendung mandantenweit vorab genehmigen.

Aufgrund der Funktionsweise von OAuth gibt es eine Vielzahl von Berechtigungen, die eine Anwendung haben kann – oft ohne dass der Benutzer (oder die Organisation) erkennt, was dieses Maß an Zugriff tatsächlich bedeutet. Schließlich liest niemand das Kleingedruckte?

Die Verwaltung von OAuth und Anwendungen erfolgt über Entra ID. Du kannst jedoch MDCA nutzen, um die Nutzung solcher Anwendungen zu überwachen oder um zu beobachten, wann eine neue Anwendung in der Umgebung auftaucht. Für jede Anwendung kannst du dann sehen, welche Benutzer die Anwendung nutzen, wie viel Verkehr über die Anwendung läuft oder welche Aktivitäten kürzlich durchgeführt wurden – vorausgesetzt, die letztgenannten Informationen sind verfügbar. Um eine Liste der OAuth-Anwendungen anzuzeigen, die in deinem Mandanten vorhanden sind, klicke auf **App-Governance** im Menü. Beachte, dass Office 365 mit MDCA verbunden sein muss, bevor du sehen kannst, welche OAuth-Anwendungen vorhanden sind.

In der Liste der Anwendungen siehst du sofort, wann eine Anwendung zuletzt in deiner Organisation autorisiert wurde. Dies ist das letzte Mal, dass jemand der Anwendung zugestimmt hat. Du siehst auch, wie viele Benutzer zugestimmt haben oder wie hoch das Berechtigungsniveau der Anwendung ist. Je höher das Berechtigungsniveau, desto höher das Risiko, das mit einer Anwendung verbunden ist.

**Realität:** Die meisten Anwendungen sind harmlos und stellen eine Vielzahl von SaaS-Anwendungen oder intern entwickelten Anwendungen dar. Hin und wieder findest du jedoch eine Anwendung, die verdächtig erscheint und vielleicht wirklich bösartig ist. Die Flexibilität von OAuth ermöglicht es auch einem Angreifer, sie zu nutzen. Indem ein Benutzer dazu verleitet wird, einer gefälschten Anwendung zuzustimmen, könnten sich Angreifer unbefugten Zugriff auf Daten verschaffen. Diese Art von Angriff wird immer häufiger und kann sogar zur Verschlüsselung von Inhalten verwendet werden! Weitere Informationen darüber, wie OAuth missbraucht werden könnte, findest du in [diesem Artikel](#).

Wenn du auf eine Anwendung stößt, die nicht verwendet werden soll, kannst du zu Entra ID wechseln, um sie dort zu blockieren oder zu entfernen. Alternativ kannst du, wenn du die Netzwerkblockierungsfunktionen über MDE aktiviert hast, die Anwendung blockieren („unsanctioned“), woraufhin Benutzer automatisch daran gehindert werden, darauf zuzugreifen – vorausgesetzt, ihre Geräte führen MDE aus. Das Unsanctioning von Anwendungen entfernt auch automatisch die Berechtigungen für die Anwendung in Entra ID.

## App Governance

Anfang 2023 hat Microsoft beschlossen, App Governance als Teil der Microsoft Defender for Cloud Apps-Lizenz und nicht als separate kostenpflichtige Erweiterung aufzunehmen. Diese Funktion soll Administratoren dabei helfen, besser zu kontrollieren, wie OAuth-fähige Apps mit Microsoft 365 interagieren können, indem:

- **Bereitstellung von Einblicken** in die OAuth-Anwendungen und deren Berechtigungsumfang.
- **Kontrolle** darüber, welche Anwendungen sich verbinden dürfen und welche Aktionen bei neuen Verbindungen ausgeführt werden. Beispielsweise könnte eine neue App-Richtlinie erstellt werden, um hochprivilegierte Apps automatisch zu blockieren, sobald sie im Mandanten erkannt werden.
- **Erkennung** von anomalen Aktivitäten oder Richtlinienverstößen.
- **Automatisch Korrektur** von Richtlinienverstößen oder potenziell bösartigen Anwendungen.

Unter der Haube sammelt und kombiniert App Governance Informationen aus Entra ID und Defender for Cloud Apps, um so viele Informationen wie möglich über eine Anwendung zu erhalten. Dazu gehören Informationen über die Aktivität einer App, Anmeldungen bei der Anwendung und die Risikobewertung von Defender for Cloud Apps. Diese Informationen können dann wiederum verwendet werden, um Erkenntnisse in das App-Governance-Portal zu übertragen, sodass du dir schnell ein Bild davon machen kannst, was und wie Apps innerhalb der Umgebung verwendet werden.

App Governance bringt verschiedene Elemente von Microsoft 365 zusammen: Nutzungs- und Anmeldeinformationen aus Entra ID, API-Einblicke aus Defender for Cloud Apps, und kombiniert



diese Informationen, um ein vollständigeres Bild davon zu zeichnen, wie Anwendungen (OAuth) innerhalb der Organisation verwendet werden. Warnungen, die aus App Governance kommen, sind noch etwas unausgereift – aber es ist noch in Arbeit.

## Erste Schritte mit App Governance

Sobald du App Governance aktiviert hast, kannst du darauf über das [Microsoft 365 Defender Security-Portal](#) zugreifen und dann zu **Cloud-Apps > App Governance** navigieren.

## Anwendungseinblicke erhalten

Einer der beiden Hauptzwecke von Application Insights ist – wie du vielleicht schon erraten hast – mehr Transparenz darüber zu erhalten, welche (OAuth-)Anwendungen in der gesamten Umgebung verwendet werden, welche (Ebene von) Berechtigungen sie haben, wie oft sie verwendet werden, wer sie verwendet usw.

Über das App-Governance-Dashboard kannst du verschiedene Einblicke über Anwendungen in der Umgebung erhalten. Die Übersichtsseite enthält mehrere Informationen, von denen die „Top-Apps nach Kategorien“ besonders interessant sind. Auf einen Blick siehst du, welche (Top-)Anwendungen hohe Berechtigungen haben, überprivilegiert sind, keinen verifizierten Herausgeber haben usw.

**Was bedeutet überprivilegiert?** Der Begriff überprivilegiert klingt ernst, aber was bedeutet er wirklich? Microsoft liefert keine Definition dafür, betrachtet jedoch, welche Berechtigungen einer Anwendung erteilt wurden und welche sie tatsächlich nutzt. Wenn es eine Diskrepanz gibt, wird die App als überprivilegiert markiert. Mit anderen Worten: Wenn einer App Berechtigungen zugewiesen wurden, die sie nicht nutzt und die daher widerrufen werden könnten, gilt sie als überprivilegiert.

Das Portal bietet auch eine Liste aller (registrierten) Anwendungen in deinem Mandanten, zusammen mit nützlichen Informationen wie: von wem sie veröffentlicht wurde, wann sie dem Mandanten hinzugefügt wurde, wie hoch das (wahrgenommene) Berechtigungsniveau ist, wie viele Benutzer sie hat usw. Diese Übersicht sieht etwa so aus wie die folgende Abbildung:

**App governance** What's new Learn more

Get in-depth visibility and control over OAuth apps registered on Azure Active Directory.

Overview **Apps** Alerts Policies

Export 30 items Search Customize columns

Filter Save the query Reset Filters

API access: Any Privilege level: Any Permission usage: Any Permission type: Any Publisher verified: Any Services accessed: Any Sensitivity labels accessed: Any

App name ↑	App status	Graph API access	Permission type	Consent type	Publisher	Last modified	Added on	Permission usage	Data usage	Priv
<input type="checkbox"/> Adobe Acrobat	Enabled	No	Delegated	Admin (34)	N/A	Jan 2, 2023 4:06 PM	Dec 12, 2018 4:56 PM	N/A	0 (0%)	
<input type="checkbox"/> AltspaceVR	Enabled	Yes	Delegated	User (1)	N/A	Jan 2, 2023 4:06 PM	Oct 21, 2021 1:27 PM	N/A	0 (0%)	
<input type="checkbox"/> API Explorer	Enabled	Yes	Delegated	User (1)	N/A	Jan 2, 2023 4:06 PM	May 28, 2015 3:45 PM	Some unused	0 (0%)	

Abbildung 11-17: Eine Übersicht der Anwendungen im Mandanten

Wenn du auf eine Anwendung klickst, öffnet sich ein Slide-Out, der weitere (detaillierte) Informationen über die Nutzung der Anwendung anzeigt. Zu den Einblicken, die du sehen wirst, gehören:

- Nutzungsdetails über die Anwendung, wie z.B. wie oft auf sie zugegriffen wurde und wie viele Daten verarbeitet wurden,
- welche Benutzer der Anwendung zugestimmt haben und sie aktiv nutzen,
- welche Berechtigungen der Anwendung zugewiesen wurden und welches Zugriffsniveau diese Berechtigungen auf die Umgebung bieten.

Letztendlich sollen dir diese Informationen ein klares Bild davon vermitteln, welche Auswirkungen Anwendungen auf die Organisation haben können – damit du einfacher kontrollieren kannst, wie und welche Anwendungen verwendet werden, oder um potenziell bösartige oder übermäßig berechtigte Anwendungen zu erkennen. Vor allem Letzteres ist meiner Meinung nach ein echtes Problem: Oft wählen Entwickler von Drittanbietern den bequemsten Ansatz und fordern so viele Berechtigungen wie möglich an, selbst wenn sie diese gar nicht benötigen. Auch wenn das nicht zwangsläufig ein Problem ist, finde ich es persönlich bedenklich, wenn Anwendungen auf alle meine Daten zugreifen können, obwohl sie nur Zugriff auf eine Teilmenge benötigen.

## Anwendungen steuern

Die andere wichtige Rolle von App Governance ist die Möglichkeit, Richtlinien zu definieren, die festlegen, wie Anwendungen verwendet werden dürfen oder welche Berechtigungen sie erhalten können. Dafür stehen zwei Arten von Richtlinien zur Verfügung:

- **App-Nutzungsrichtlinien**, die eingreifen können, wenn eine Anwendung bestimmte Kriterien erfüllt. Wenn eine App z. B. plötzlich mehr Daten als üblich verarbeitet oder wenn mehr Benutzer der Anwendung zustimmen, kannst du sie automatisch deaktivieren und eine Warnung ausgeben lassen, damit ein Administrator prüfen kann, was passiert ist. Auf diese Weise kannst du verhindern, dass eine bösartige

Anwendungen Daten aus deiner Umgebung exfiltriert ( z.B. durch plötzlichen Datenanstieg) oder viele Benutzer gleichzeitig betrifft (Anstieg der z. B. durch plötzlichen Anstieg der Zustimmungen).

- **App-Berechtigungsrichtlinien**, die die Berechtigungen überwachen, die Anwendungen erteilt werden, und eingreifen können, wenn Berechtigungen auf hoher Ebene vergeben wurden.

## In Echtzeit mit Conditional Access App Controls arbeiten

Bisher haben wir beschrieben, wie du eine Anwendung über eine API-Verbindung mit MDCA verbinden kannst. Es gibt jedoch viele weitere Anwendungen, die keine native API-Integration mit MDCA haben, für die du aber trotzdem Transparenz und Kontrolle möchtest. Das ist über Conditional Access App Control (CAAP) möglich.

CAAP kann als Gemeinschaftsprojekt zwischen Conditional Access und MDCA betrachtet werden: Wenn du in einer Conditional-Access-Regel angibst, dass eine Anwendungssitzung über MDCA weitergeleitet werden soll, fungiert MDCA als Proxy. So erhält es die Möglichkeit, Aktivitäten innerhalb der Sitzung zu überwachen und zu steuern. Diese Aktivitäten können protokolliert und überprüft werden (mithilfe einer Sitzungsrichtlinie). Bei Bedarf kann MDCA bestimmte Aktionen blockieren, z. B. das Hoch- oder Herunterladen von Dateien, und zusätzlich Rechteverwaltungsvorlagen anwenden.

Bevor du eine Anwendung mit CAAP nutzen kannst, muss sie mit Entra ID verbunden sein. Mit anderen Worten: Du musst dich mit deinen Entra-ID-Anmeldeinformationen bei der Anwendung anmelden. Sobald die Sitzung über MDCA geleitet wird, wirst du feststellen, dass sich die URL – z. B. von myapplication.com – in myapplication.com.eu.cas.ms oder myapplication.com.cas.ms ändert. Die Daten werden dann über die Rechenzentrumsregion geleitet, in der dein MDCA-Mandant gehostet wird. Wenn du z. B. einen US-Mandanten nutzt, läuft der Datenverkehr über die US-MDCA-Infrastruktur; bei einem EU-Mandanten über die europäische Infrastruktur.

**Drittanbieter-IdP:** Die Integration mit Entra ID ist der einfachste Weg, um Sitzungsrichtlinien zu nutzen. Du kannst sie jedoch auch verwenden, wenn eine Anwendung nicht direkt mit Entra ID verbunden ist. Dafür musst du deinen Identity Provider so konfigurieren, dass er mit MDCA zusammenarbeitet - möglich ist das allerdings nur, wenn die Authentifizierung über SAML2.0 erfolgt. Weitere Informationen zur Erstellung dieser Integration findest du [hier](#).

## Wie die Sitzungskontrolle (Proxy) funktioniert

In Microsofts Terminologie sprechen wir von Sitzungskontrolle, wenn eine Verbindung über MDCA geproxyt wird. Wenn sich ein Benutzer bei einer Anwendung anmeldet, die durch eine Sitzungskontrollrichtlinie geschützt ist (mehr dazu später), wird der gesamte Datenverkehr über die MDCA-Proxy-Infrastruktur geleitet. Diese Infrastruktur wird in Azure-Rechenzentren weltweit betrieben. Abhängig vom Standort des Benutzers und den Verkehrsmustern kann es vorkommen, dass der Datenverkehr über Rechenzentren außerhalb der geografischen Heimatregion geleitet wird. Beispielsweise können EU-basierte Benutzer bei Reisen in die USA feststellen, dass ihre Sitzung über die nordamerikanische Infrastruktur geführt wird – dies dient der bestmöglichen Benutzererfahrung.

**Datenschutz:** Um die Privatsphäre deiner Benutzer zu schützen, werden keine Sitzungsdaten außerhalb ihrer geografischen Heimatregion gespeichert. Außerdem werden nur öffentliche Inhalte zwischengespeichert - wie in RFC 7234 definiert.

## Erstellen einer Conditional Access App Control-Richtlinie

Um Conditional Access App Control zu aktivieren, musst du zunächst eine Conditional-Access-Richtlinie erstellen und sie so konfigurieren, dass Sitzungsrichtlinien verwendet werden. Navigiere dazu im Azure-Portal zu Entra ID → Conditional Access. Klicke auf der Seite „Conditional Access | Richtlinien“ auf **Neue Richtlinie**, um eine neue Richtlinie zu erstellen. Weitere Details zum Erstellen solcher Richtlinien findest du in Kapitel 4 „Sicherung von Identitäten“. Achte in diesem Beispiel darauf, dass du unter **Zugriffssteuerung** die Option **Conditional Access App Control verwenden** auswählst.

## Anzeigen von für Conditional Access App Control verfügbaren Anwendungen

Nachdem du die CA-Richtlinie erstellt hast, musst du dich mindestens einmal bei der Anwendung anmelden. Dadurch wird die Anwendung in MDCA „onboarded“. Wenn du dich nach dem Erstellen der Richtlinie das erste Mal anmeldest, wirst du möglicherweise mit einer Seite wie der in Abbildung 11-18 gezeigten begrüßt:

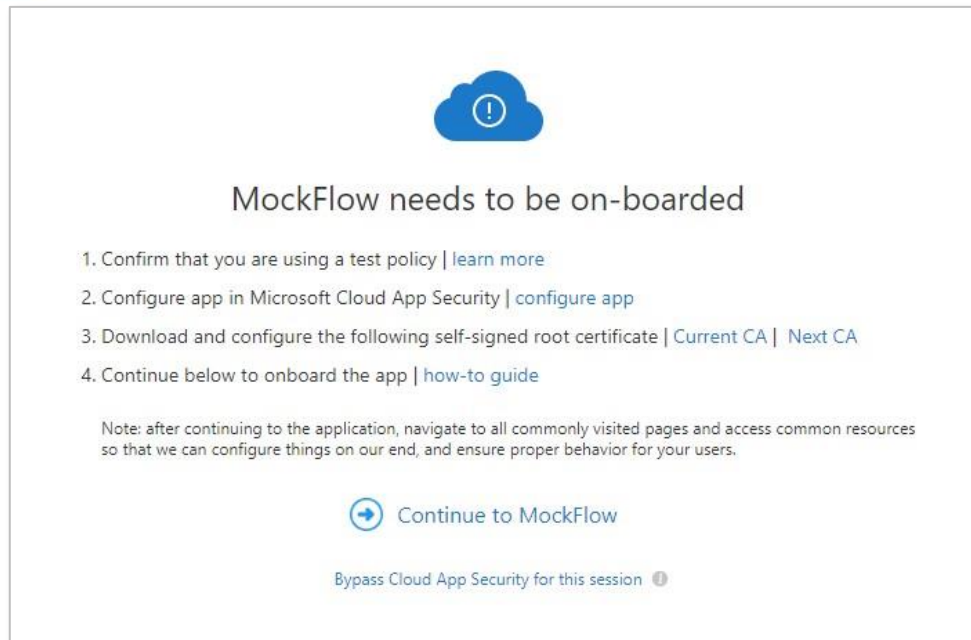


Abbildung 11-18: CAAP-Onboarding-Seite.

In diesem Beispiel habe ich die Anwendung „MockFlow“ mit CAAP verbunden. Nach dem Erstellen der Conditional-Access-Richtlinie habe ich mich mit meinem Benutzerkonto angemeldet. Am besten führst du diesen Schritt mit einem Konto durch, das auch über administrative Rechte in MDCA verfügt – das erleichtert das Onboarding erheblich.

Um TLS-Sitzungen erfolgreich über MDCA umzuleiten, musst du die entsprechenden Zertifikate von der Microsoft-Website herunterladen und installieren. Dabei handelt es sich um selbstsignierte Root-CA-Zertifikate, die erforderlich sind, um eine vertrauenswürdige Verbindung mit Domains vom Typ **\*Region>.MDCA.ms** aufzubauen. Du musst diese Zertifikate auf allen Clientgeräten installieren, die sich mit der Anwendung verbinden, die du konfigurierst.

Nachdem du diese Schritte abgeschlossen hast, öffne das Einstellungsmenü (Zahnrad), wähle **App-Connectors** und öffne die Registerkarte **Conditional Access App Control Apps**. Du solltest deine Anwendung nun dort aufgelistet sehen. Unter **Verfügbare Steuerelemente** kannst du erkennen, welche Sitzungsoptionen dir zur Verfügung stehen. Falls keine verfügbar sind, erscheint stattdessen die Option, sie anzufordern.

**Realität:** Sitzungssteuerung bedeutet nicht automatisch, dass du jede einzelne Aktion innerhalb der Anwendung steuern kannst. Welche Optionen dir zur Verfügung stehen, hängt stark von der Anwendung selbst ab. Im Beispiel MockFlow gibt es keine spezifischen Aktionen, die gesteuert werden können. Dennoch kann MDCA allgemeine Aktivitäten wie Hoch- und Herunterladen, Kopieren/Einfügen sowie Drucken überwachen und einschränken. Bei anderen Anwendungen kann MDCA deutlich differenzierter agieren – dort lassen sich beispielsweise einzelne Vorgänge wie das Erstellen eines Issues gezielt kontrollieren.

## Erstellen einer Sitzungsrichtlinie

Um eine Sitzungsrichtlinie zu erstellen, gehe zu **Richtlinien > Richtlinienverwaltung**. Klicke auf die Schaltfläche **Richtlinie erstellen** und wähle **Sitzungsrichtlinie** aus. Wenn du möchtest, kannst du mit der Auswahl einer Vorlage beginnen – sie ist ein guter Weg, um dich mit den Möglichkeiten von Sitzungsrichtlinien vertraut zu machen. Alternativ gibst du einen Namen und eine Beschreibung ein und wechselst anschließend zum Sitzungssteuerungstyp.

Der Sitzungssteuerungstyp bestimmt, welche Art von Richtlinie du erstellst. Du kannst eine Richtlinie anlegen, um Aktivitäten nur zu überwachen, oder auch eine Richtlinie definieren, die bestimmte Aktionen wie Kopieren/Einfügen oder das Herunterladen einer Datei blockiert. Die verfügbaren Optionen sind:

- **Nur überwachen** - wird verwendet, um Aktivitäten innerhalb einer Anwendung zu überwachen.
- **Aktivitäten blockieren** – blockiert bestimmte Aktionen innerhalb einer Sitzung.
- **Dateidownload steuern (mit DLP)** – steuert, was passiert, wenn eine Datei aus der Anwendung heruntergeladen wird.
- **Dateiupload steuern (mit DLP)** – funktioniert analog, aber beim Hochladen von Dateien.

Nachdem du den Typ der Richtlinie ausgewählt und deine Filter erstellt hast, um festzulegen, wann die Richtlinie gelten soll, gehe zum Abschnitt **Aktionen**. Dort stehen dir mehrere Optionen zur Verfügung:

- **Test** – überwacht nur die von dir definierten Bedingungen und lost gegebenenfalls eine Warnung aus. Es werden keine Aktionen angewendet.
- **Blockieren** – blockiert die Aktion, wenn die Bedingungen erfüllt sind.

Wenn du eine Richtlinie erstellst, die Dateidownloads steuert, wird eine zusätzliche Option sichtbar:

- **Schützen** – ermöglicht dir, Dateien beim Herunterladen zu klassifizieren (kennzeichnen) und zu schützen. Du kannst benutzerdefinierte Berechtigungen anwenden oder eine Bezeichnung verwenden, die in der Vertraulichkeitskennzeichnung (ehemals AIP) konfiguriert wurde.

**Hinweis:** Zugriffsrichtlinien zählen ebenfalls eine zu den Sitzungsrichtlinien. Zwar kannst du mit Conditional Access-Richtlinien den Zugriff auf eine Anwendung abhängig von Bedingungen wie Gruppenmitgliedschaft oder Gerätestatus steuern, doch + MDCA geht noch weiter: Die Filterfunktionen erlauben eine wesentlich genauere Kontrolle darüber, wem der Zugriff gewährt oder verweigert wird – bis hin zur Auswertung des User-Agent-Strings, des ISPs, der IP-Adresse oder einer Kombination daraus.



# Malware-Erkennung

MDCA kann bössartige Dateien in verschiedenen Cloud-Speicherplattformen erkennen. Zum Zeitpunkt der Erstellung dieses Textes wird die Malware-Erkennung für **Office 365 (SharePoint Online, OneDrive for Business)**, **Google Workspace**, **Dropbox** und **Box** unterstützt. Damit sie in Office 365 funktioniert, benötigst du eine gültige **Defender for Office 365-Lizenz** (mindestens P1). Standardmäßig ist die Malware-Erkennungsrichtlinie deaktiviert. Um sie zu aktivieren, führe die folgenden Schritte aus:

Navigiere im MDCA-Portal zu **Richtlinien > Richtlinienverwaltung**. Suche nach dem Begriff „Malware“. In der Ergebnisliste sollte die Richtlinie **Malware-Erkennung** erscheinen.

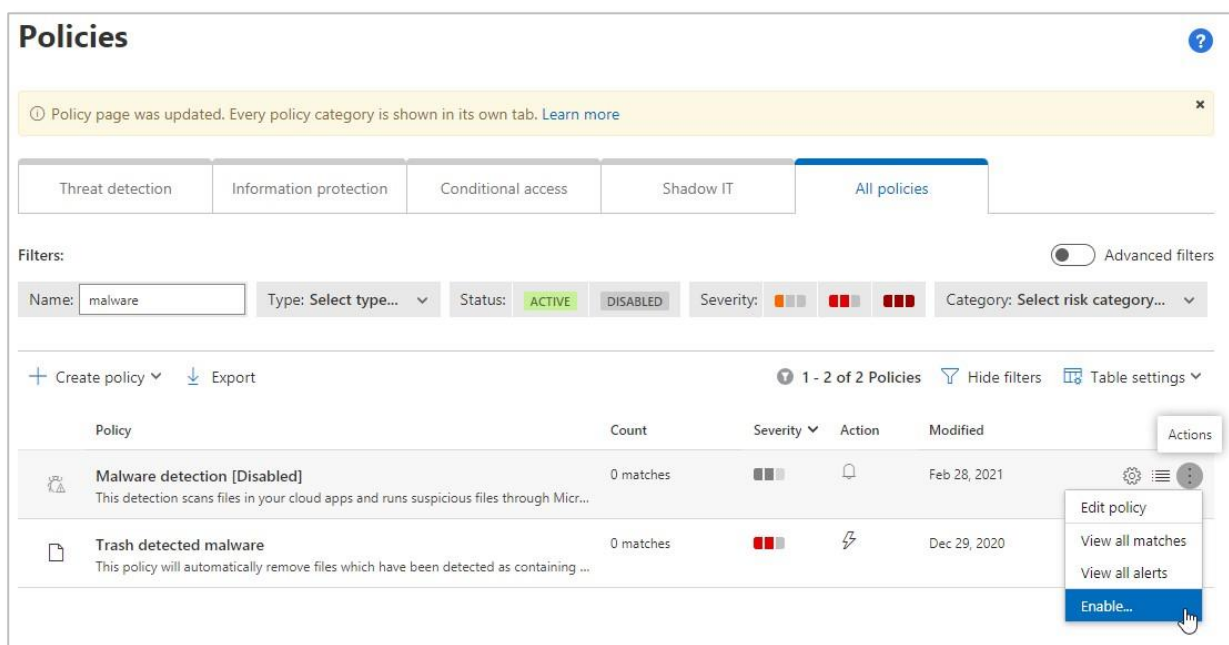


Abbildung 11-19: Aktivieren der integrierten Malware-Erkennungsrichtlinie

Klicke auf die Auslassungspunkte auf der rechten Seite und wähle **Aktivieren**. Bestätige die Abfrage erneut mit **Aktivieren**.

**Hinweis:** Das Aktivieren der Richtlinie bedeutet nicht, dass jede Datei gescannt wird. Stattdessen wird heuristische Intelligenz verwendet, um potenziell bössartige Dateien zu identifizieren.

## Auf Malware-Erkennungen reagieren

Administratoren können in der **Bedrohungsrichtlinie** festlegen, welche Maßnahmen ergriffen werden, wenn Malware erkannt wird. Für OneDrive for Business und SharePoint stehen

folgende Aktionen zur Verfügung. Diese erfolgen zusätzlich zur automatischen Sperrung des Dateizugriffs, die nicht deaktiviert werden kann:

- Externe Benutzer entfernen
- In Benutzerquarantäne stellen
- Papierkorb (Datei entfernen)

## Arbeiten mit Vertraulichkeitsbezeichnungen in MDCA

Informationsschutz hat viele Facetten. Je nach Anwendungsfall möchtest du vielleicht bestimmte Inhalte erkennen, verhindern, dass sie extern geteilt werden, Dateiaktivitäten überwachen, Benutzer warnen oder Inhalte im laufenden Betrieb durch Kennzeichnung schützen. MDCA – das Schweizer Taschenmesser für solche Szenarien – unterstützt dich dabei. In diesem Abschnitt konzentrieren wir uns auf die Integration mit Vertraulichkeitskennzeichnungen.

Microsoft ist dafür bekannt, durch Umbenennungen Verwirrung zu stiften. Die meisten kennen **Azure Information Protection (AIP)**, das in Kapitel 9 genauer behandelt wird. Obwohl AIP schon lange existiert, wurde es mittlerweile durch die **Unified Sensitivity Labels von Office 365** ersetzt. Zum Zeitpunkt des Schreibens ist das alte AIP-Portal allerdings noch nicht vollständig abgeschaltet, und nicht alle Organisationen haben bereits vollständig umgestellt. Wir gehen in diesem Abschnitt davon aus, dass du bereits von AIP auf Unified Labeling migriert hast. [diese Seite](#) an.

### Voraussetzungen

Bevor du mit Unified Labels in MDCA arbeitest, ist es wichtig zu verstehen, dass es - bis das AIP-Portal vollständig veraltet ist - einige Überlegungen gibt:

1. Wenn du Unified Labeling noch nicht aktiviert hast, ruft MDCA seine Labels von AIP ab.
2. Wenn du Unified Labeling aktiviert hast, müssen Labels über das Office 365 Security & Compliance Center veröffentlicht werden, bevor sie von MDCA verwendet werden können.

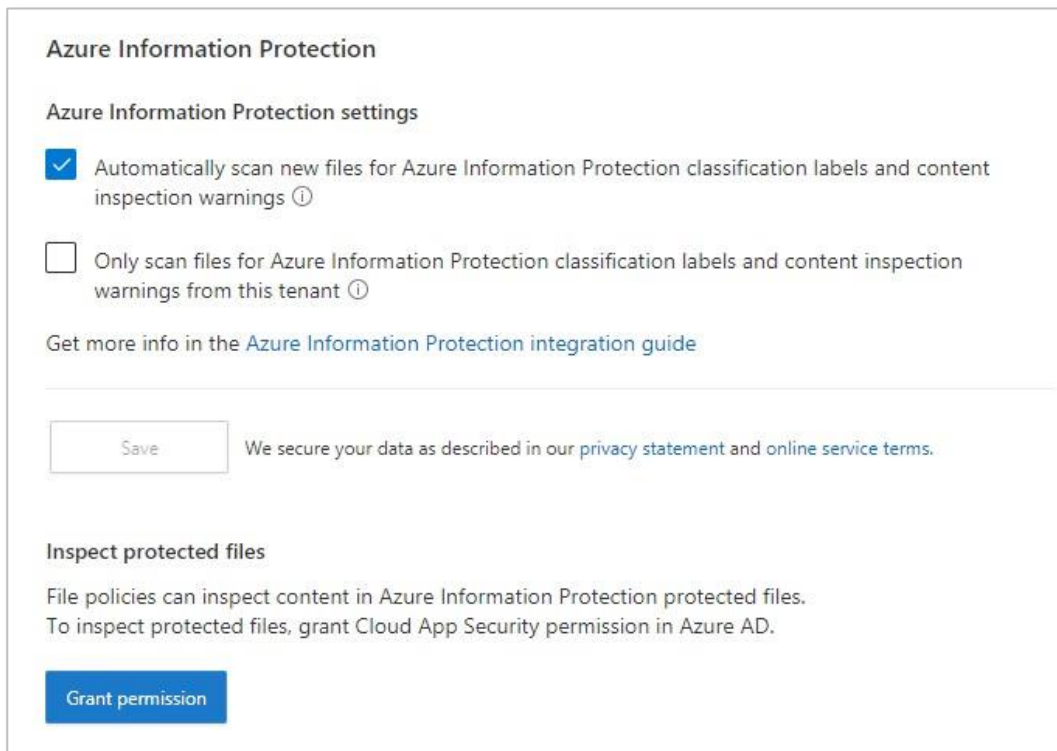
Die Unterstützung von Unified Labeling in MDCA ist auf bestimmte Dokumenttypen beschränkt. Während der Unified Labeling Client auch einen Schutz-Wrapper für generische Inhalte erzeugen kann, gilt das für MDCA nicht. Unterstützt werden derzeit folgende Formate:

- Word
- Excel

- PowerPoint
- PDF

**Hinweis:** Die Integration funktioniert nur mit SharePoint Online, OneDrive for Business, Google Workspace und Box. Weitere Plattformen könnten in Zukunft folgen.

Bevor du mit den nächsten Abschnitten fortfährst, stelle sicher, dass du **Azure Information Protection** wie zuvor im Kapitel unter **Grundlegende MDCA-Konfiguration** beschrieben aktiviert hast.



**Azure Information Protection**

Azure Information Protection settings

☒ Automatically scan new files for Azure Information Protection classification labels and content inspection warnings ⓘ

☐ Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant ⓘ

Get more info in the [Azure Information Protection integration guide](#)

[Save](#) We secure your data as described in our [privacy statement](#) and [online service terms](#).

**Inspect protected files**

File policies can inspect content in Azure Information Protection protected files.  
To inspect protected files, grant Cloud App Security permission in Azure AD.

[Grant permission](#)

Abbildung 11-20: Aktivieren von Azure Information Protection in MDCA.

**Tagging:** Wenn du die AIP-Integration aktivierst, erfasst MDCA standardmäßig auch Labels, die von außerhalb deiner Organisation stammen. Wenn du diese ausklammern möchtest, aktiviere zusätzlich die Option *Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant* aktivieren.

## Suche nach vorhandenen Dokumenten mit Labels

Standardmäßig werden in MDCA nur Dateien gescannt, die nach der Aktivierung der AIP-Integration neu hochgeladen oder geändert wurden. Bereits vorhandene Dateien bleiben unberührt. Um auch diese zu erfassen, musst du eine **Dateirichtlinie mit aktivierter**

**Inhaltsüberprüfung** erstellen. Dadurch wird sichergestellt, dass MDCA auch bestehende Dokumente erneut scannt.

Um diese Richtlinie zu erstellen, gehe zu **Richtlinien > Richtlinienverwaltung** und klicke auf **Richtlinie erstellen**. Wähle aus dem Dropdown-Menü **Dateirichtlinie** aus. Gib der Richtlinie einen passenden Namen und eine Beschreibung und konfiguriere sie entsprechend der folgenden Abbildung.

The screenshot shows the configuration interface for a new policy in MDCA. The settings are as follows:

- Policy severity:** Low
- Category:** DLP
- Create a filter for the files this policy will act on:** files matching all of the following
- Filters:**
  - App: Microsoft OneDrive for Business
  - Operator: equals
  - + Add a filter
- Apply to:** all files
- Apply to:** all file owners
- Inspection method:** Built-in DLP
- Include files that match a preset expression:**
  - Selected: All countries: Email address
  - Don't require relevant context: ☐
- Include files that match a custom expression:** ☐
- Exclude files that match:** ☐

Abbildung 11-21: Aktivieren der Inhaltsprüfung in MDCA.

Diese Richtlinie stellt sicher, dass die Inhaltsüberprüfung aktiviert ist, wodurch automatisch auch Klassifizierungsbezeichnungen auf Dateien erkannt werden. Beachte, dass in diesem Beispiel der Filter Microsoft OneDrive for Business enthielt. Stelle sicher, dass du auch andere

Speicherplattformen einbeziehst, wenn du dort gespeicherte Dateien ebenfalls katalogisieren möchtest!

**Ausdruck spielt keine Rolle:** In diesem Beispiel suchen wir nicht nach bestimmten Informationstypen. Stattdessen wollen wir einfach die generische Inhaltsüberprüfung aktivieren. Daher spielt es keine Rolle, welchen voreingestellten Ausdruck du auswählst. Wir haben uns für *Alle Länder: E-Mail-Adresse* entschieden, aber du könntest genauso gut eine andere Option wählen.

Da MDCA nun einen Katalog aller Dateien und Bezeichnungen erstellt, kannst du diese Informationen in anderen Richtlinien verwenden. Du könntest beispielsweise eine Dateirichtlinie erstellen, bei der einer der Filter eine bestimmte Bezeichnung als Bedingung verwendet.

## Anwenden von Labels auf Dateien

Es gibt zwei Möglichkeiten, eine Bezeichnung über MDCA anzuwenden. Entweder machst du es manuell über den Datei-Explorer oder du erstellst eine Richtlinie, durch die Dateien automatisch mit einer Bezeichnung versehen werden, wenn eine bestimmte Bedingung erfüllt ist.

Um eine Bezeichnung manuell anzuwenden, navigiere zu **Dateien**. Suche dort nach der Datei, die du schützen möchtest, wähle sie aus und klicke auf die Auslassungspunkte rechts. Klicke dann auf **Klassifizierungsbezeichnung anwenden**, wie unten dargestellt:

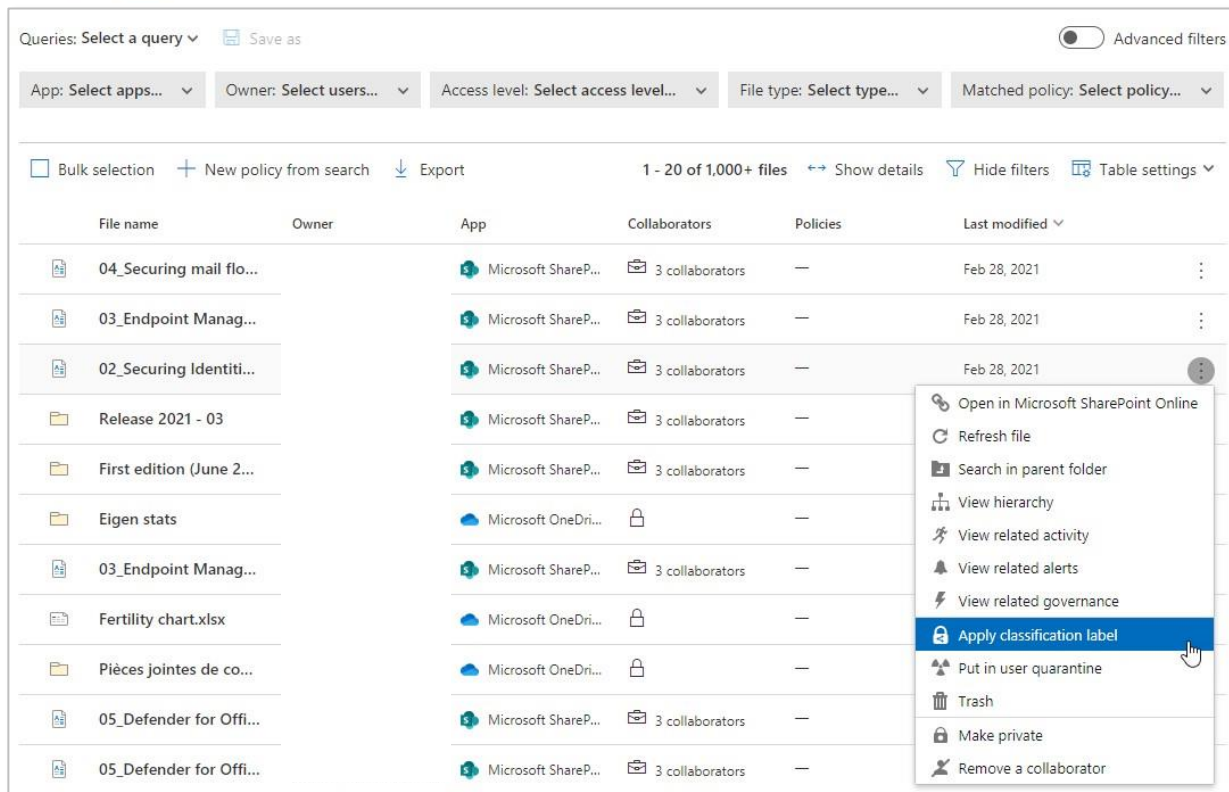


Abbildung 11-22: Manuelles Anwenden eines Klassifizierungslabls in MDCA.

Alternativ und häufiger wirst du Dateien automatisch mit einer Bezeichnung versehen wollen, wenn eine bestimmte Bedingung erfüllt ist. Dazu musst du eine Dateirichtlinie erstellen. Navigiere zuerst zu **Richtlinien > Richtlinienverwaltung**. Klicke auf **Richtlinie** erstellen und wähle im Dropdown-Menü **Dateirichtlinie** aus. Erstelle als Nächstes deine Richtlinie nach deinen Anforderungen: Füge einen Namen, eine Beschreibung und einen Filter hinzu, um anzugeben, auf welche Dateien sie angewendet werden soll.

Wähle schließlich unter **Governance-Aktionen** die gewünschte Speicherplattform (z. B. OneDrive for Business) und wähle **Klassifizierungsbezeichnung** anwenden aus. Wähle dann die Bezeichnung aus, die du anwenden möchtest:



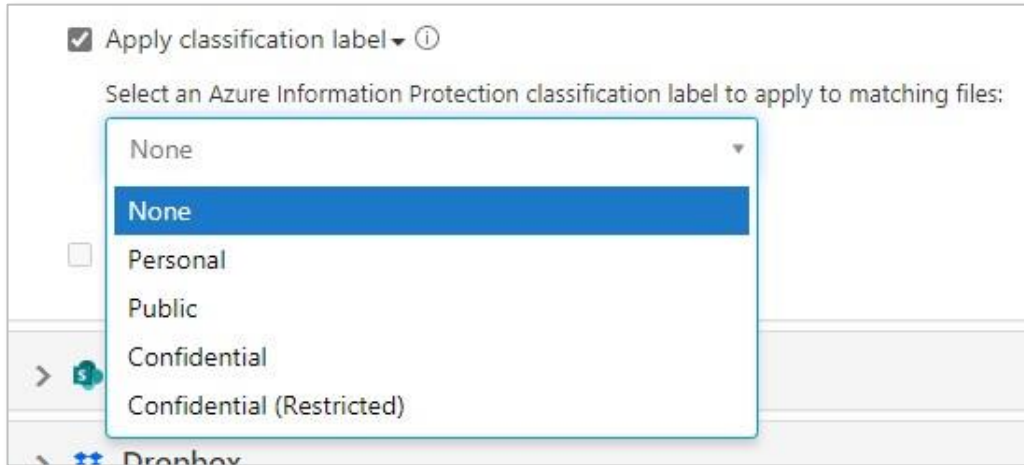


Abbildung 11-23: Automatisches Anwenden eines Klassifizierungslabels in einer Dateirichtlinie.

## Achtung, Einschränkungen!

Beachte folgende Einschränkungen bei der Kennzeichnung in MDCA:

1. Standardmäßig wendet MDCA maximal 100 Labels pro Arbeitslast und Tag an, um einen versehentlichen Schutz aller Dateien zu verhindern. Eine Erhöhung dieses Limits ist per Supportanfrage möglich.
2. MDCA kann nur Dateien bis zu einer Größe von 50 MB kennzeichnen.
3. MDCA kann keinen Schutz (Verschlüsselung) entfernen oder Bezeichnung löschen, wenn die Datei bereits durch den Unified Labeling Client geschützt oder damit beschriftet wurde. Entfernen von Schutz ist nur bei Dateien möglich, die ausschließlich über MDCA gekennzeichnet wurden und keinen bestehenden Schutz enthalten.
4. Fügt MDCA ein Label mit einer visuellen Markierung (z. B. Kopf- oder Fußzeile) hinzu, wird diese Markierung erst beim ersten Öffnen der Datei sichtbar. Der Unified Labeling Client wendet dann die sichtbare Markierung basierend auf dem Label an.

Richtlinien sind nicht der einzige Weg, um Bezeichnungen auf eine Datei anzuwenden. Mithilfe von Sitzungsrichtlinien kannst du auch steuern, wann Bezeichnungen auf eine Datei angewendet werden. Wenn du beispielsweise die Option **Dateidownload steuern** verwendest, kannst du unter **Aktionen** die Option **Schützen (Klassifizierungsbezeichnung auf Download anwenden und alle Aktivitäten überwachen)** auswählen:

**Actions**

Select an action to be applied when user activity matches the policy.

☐ **Test**  
Monitor all activities

☐ **Block**  
Block file download & monitor all activities

☒ **Protect**  
Apply classification label to downloads & monitor all activities

☒ **Apply label**  
Select an Azure Information Protection classification label to apply to matching files:

Confidential

Label will be applied to any supported file.

☐ Apply custom permissions to downloading user

☐ Block download of any file that is unsupported by native protection or where native protection is unsuccessful.

Abbildung 11-24: Anwenden eines Labels über eine Sitzungsrichtlinie.

## Integrationen von Drittanbietern und Automatisierung

Es gibt mehrere Möglichkeiten, bestimmte Aufgaben und Aktionen in MDCA (teilweise) zu automatisieren.

### Integration mit einem SIEM von Drittanbietern

Zusätzlich zur Integration über die Graph Security API, über die MDCA-Warnungen von Microsoft Sentinel abgerufen werden können, kannst du auch Discovery-Daten mit Microsoft Sentinel teilen. Die Bereitstellung dieser Informationen in Microsoft Sentinel kann die Arbeit eines Sicherheitsanalysten erleichtern, da er Informationen über neu entdeckte Anwendungen bei der Suche nach Anomalien und verdächtigen Aktivitäten verwenden kann. Neben der Möglichkeit, Informationen über mehrere Quellen hinweg zu korrelieren, ermöglicht Microsoft Sentinel (Log Analytics) auch eine längere Aufbewahrung von Daten.

Die Synchronisierung von MDCA zu Microsoft Sentinel fasst die Daten pro 24 Stunden zusammen. Das bedeutet, dass Microsoft Sentinel möglicherweise nicht immer die neuesten Informationen zur Verfügung stehen. Obwohl dies im Allgemeinen für diese Art von Informationen kein Problem darstellt, solltest du daran denken, MDCA für Untersuchungen zu verwenden, die die Verwendung der neuesten aktuellen Informationen erfordern.

Warnungen von Microsoft Defender for Cloud Apps werden vom Microsoft 365 Defender Data Connector in Sentinel gesteuert. Cloud Discovery-Protokolle erfordern dagegen die Verwendung des Microsoft Defender for Cloud Apps-Datenconnectors. Wie man einen Datenconnector aktiviert, wird in Kapitel 12 erläutert.

Sobald du die Schritte abgeschlossen hast, sollten die Discovery-Protokollinformationen innerhalb weniger Minuten in Microsoft Sentinel angezeigt werden. Die Daten sollten in zwei verschiedene Tabellen innerhalb des SecurityInsights-Protokolls geschrieben werden:

- **MDCAShadowItReporting**, das die Discovery-Daten enthält
- **SecurityAlerts**, das die von MDCA ausgelösten Warnungen enthält.

Im obigen Abschnitt wurde beschrieben, wie man mit Microsofts nativer Cloud-SIEM, Microsoft Sentinel, integriert. Offensichtlich nutzen oder wollen nicht alle Organisationen Microsoft Sentinel nutzen, und sie verlassen sich möglicherweise bereits auf ihre eigene SIEM-Umgebung – entweder in der Cloud oder vor Ort.

Um die zusätzliche Integration mit anderen SIEM-Plattformen zu ermöglichen, navigiere zu **Einstellungen > Cloud-Apps** und klicke auf **SIEM-Agents**. Klicke dann auf **SIEM-Agent hinzufügen**. Im Pop-upfenster kannst du entweder ein generisches Common Event Format (CEF) oder ein spezielles Format für ArcSight auswählen. Andere SIEM-Anbieter sind (noch?) nicht standardmäßig enthalten.

Die SIEM-Integration dieser Art verwendet einen Agenten und einen Syslog-Server – vermutlich dein SIEM. Der Agent ruft Informationen von MDCA ab und leitet sie an deinen definierten Syslog-Server weiter. Das eignet sich besonders für SIEM-Lösungen, die möglicherweise keine API zum Abrufen von Warnungen und Ereignissen nutzen können. Dein eigenes SIEM könnte genauso gut die Graph Security API oder die MDCA API nutzen, um Warnungen und Aktivitäten abzurufen, ohne dass ein Agent eingerichtet oder ein Syslog-Server für diesen Zweck gepflegt werden muss.

Weitere Informationen zur Integration oder zur Einrichtung findest du auf [dieser](#) Seite.

**Realität:** Je nachdem, welche Workloads du verwendest und wie oder wo du Ereignisse von diesen Workloads sammelst, gibt es verschiedene Möglichkeiten, wie du dein eigenes SIEM anbinden kannst. Was hier beschrieben wird, ist nur eine Methode und konzentriert sich ausschließlich auf Defender for Cloud Apps. Beachte, dass die Warnungen von Microsoft Defender for Identity automatisch mit einbezogen werden, wenn du dein SIEM mit MDCA integrierst- vorausgesetzt du hast Microsoft Defender for Identity in MDCA integriert. Wenn du bereits Warnungen von Microsoft Defender for Identity in dein SIEM über die Graph Security API einspeist, kann es zu Duplikate kommen - eine Warnung über die API und eine über MDCA.

## Erstellen von API-Integrationen

Es ist nicht ungewöhnlich, dass Anwendungen von Drittanbietern mit Defender for Cloud Apps interagieren möchten, um Informationen auszulesen oder vielleicht Warnungen zu lesen und zu aktualisieren. Neben der Integration mit der Graph Security API, die Zugriff auf die ausgelösten Warnungen bietet, verfügt MDCA auch über eine eigene API, die eine umfangreichere Reihe von Funktionen bietet.

Unter anderem ermöglicht die MDCA-API die Interaktion mit Warnungen, die Nutzung von Discovery-Daten, die Erstellung von IP-Adressbereichen und die Arbeit mit Aktivitätsdaten. Um eine Verbindung zur API herzustellen, musst du zunächst ein API-Token erstellen. Im Gegensatz zu vielen anderen Anwendungen wird die API nicht über Entra ID verwaltet oder gesteuert. Stattdessen musst du MDCA verwenden, um das Token zu erstellen.

Öffne dazu die Einstellungen und klicke auf „**API-Token**“. Klicke anschließend auf „**Token hinzufügen**“. Gib einen aussagekräftigen Namen für dein Token ein und klicke auf „**Generieren**“. Du siehst nun dein API-Token. Beachte, dass du den Token-Wert nach dem Schließen des Fensters nicht mehr abrufen kannst. Stelle also sicher, dass du die Informationen zusammen mit dem Endpunkt (URL) kopierst. Das Token übernimmt die Berechtigungen des Benutzers, der es generiert hat. Wenn dieser Benutzer nur Leseberechtigungen hat, gilt dies auch für das Token.

Obwohl die API-Token-Zeichenfolge nicht leicht zu erraten ist, solltest du vorsichtig sein, wie und wo du sie speicherst. Es gibt keine integrierten Governance-Möglichkeiten wie das automatische Ablaufen oder die Neugenerierung des Tokens. Du solltest Token daher regelmäßig selbst erneuern. Wie oft du das machst, hängt von deiner Risikobereitschaft oder davon ab, wie häufig du ein neues Token generieren und deine Integrationen damit aktualisieren möchtest.

## Reale Szenarien

Nachdem du nun weißt, was die verschiedenen Funktionen von MDCA sind, schauen wir uns an, wie du sie kombinieren kannst, um reale Probleme zu lösen.

# Überwachung der Nutzung sensibler oder hoch privilegierter Konten

## Szenario

Trotz aller Bemühungen, die einfache Authentifizierung mit Benutzername und Passwort abzuschaffen, verwendet deine Organisation wahrscheinlich immer noch einige intern entwickelte Anwendungen, die ein Benutzerkonto zur Interaktion mit Office 365 benötigen. Um die Sache noch schlimmer zu machen, verfügen einige dieser Konten über mächtige Berechtigungen, wie zum Beispiel die eines globalen Administrators. Damit sind sie ideale Ziele für Angreifer. Um sicherzustellen, dass diese Konten nicht missbraucht werden, möchtest du ihre Aktivitäten überwachen und eine Warnung generieren, wenn ein Konto außerhalb des Unternehmensnetzwerks verwendet wird. Langfristig soll das Ziel sein, Anmeldungen zu blockieren, die möglicherweise von nicht zulässigen Standorten stammen.

## Lösung

Um das umzusetzen, brauchst du ein paar Dinge. Zunächst wäre es hilfreich, wenn alle zu überwachenden Konten Teil einer Gruppe wären. So musst du die Richtlinie nicht jedes Mal aktualisieren, wenn ein Konto erstellt oder entfernt wird – du musst es lediglich zur Gruppe hinzufügen oder daraus entfernen.

1. Erstelle zunächst eine Gruppe in Entra ID mit der Bezeichnung *Sensible Konten*. Füge dieser Gruppe deine sensiblen Benutzerkonten hinzu.
2. Navigiere als Nächstes im [Microsoft 365 Defender-Sicherheitsportal](#) zu **Einstellungen > Cloud-Apps** und klicke auf **Benutzergruppen**.
3. Klicke auf der Seite *Benutzergruppen* auf **Benutzergruppe importieren**.
4. Wähle in der Liste der Anwendungen **Office 365 (Entra ID)** aus und wähle die Gruppe aus, die du importieren möchtest. Suche nach *Sensible Konten*, um sie schnell zu finden.
5. Klicke auf **Importieren**.

**Hinweis:** Das Importieren von Gruppen kann einige Zeit in Anspruch nehmen. Du musst warten, bis der Import abgeschlossen ist, bevor du mit den nächsten Schritten fortfahren kannst. Größere Gruppen benötigen in der Regel länger zum Importieren.

Als Nächstes musst du deine Unternehmens-IP-Adressen der Kategorie „Unternehmen“ zuordnen. Das erleichtert später die Erstellung der Richtlinie. Du könntest die IP-Adressen auch manuell in die Richtlinie eintragen, das ist aber keine saubere Vorgehensweise.

1. Navigiere im [Microsoft 365 Defender-Sicherheitsportal](#) zu **Einstellungen > Cloud-Apps** und klicke auf **IP-Adressbereiche**.

2. Klicke auf der Seite *IP-Adressbereiche* auf das Pluszeichen, um einen neuen IP-Adressbereich hinzuzufügen.
3. Gib im Assistenten *Neuer IP-Adressbereich* die IP-Adressbereiche ein, die du hinzufügen möchtest. Dies sollten die externen IP-Adressen sein, die von den (physischen) Standorten verwendet werden, die du von der später zu erstellenden Richtlinie ausnehmen möchtest. Stelle sicher, dass du im Feld *Kategorie* **Unternehmen** auswählst.
4. Klicke schließlich auf **Erstellen**.

**Viele Wege führen nach Rom:** Im diesem Beispiel haben wir die IP-Adresskategorie *Unternehmen* verwendet, um unsere Unternehmens-IP-Adressen einzubeziehen. Du könntest aber auch eine andere Kategorie wählen und oder zusätzliche Tags vergeben. Diese Tags, die wir im Abschnitt "IP-Adressbereiche und Tags" besprochen haben, helfen dir dabei, bestimmte IP-Adressen weiter zu differenzieren – selbst wenn sie derselben Kategorie zugeordnet sind.

Jetzt brauchst du eine Richtlinie, um Anmeldeaktivitäten zu überwachen. Du hast mehrere Möglichkeiten. Je nach Art der Konten könntest du eine Zugriffsrichtlinie verwenden, was jedoch die Nutzung von **Conditional Access App Control** erfordert. Diese Methode leitet die Sitzung über MDCA weiter. Alternativ kannst du eine **Aktivitätsrichtlinie** einsetzen. Diese ist völlig transparent, allerdings dauert es etwas, bis Aktivitäten in MDCA erscheinen – das führt zu einer gewissen Verzögerung bei der Warnung. Wenn du Aktivitäten blockieren möchtest, sobald sie auftreten, musst du unbedingt eine Zugriffsrichtlinie mit Conditional Access App Control verwenden.

Da wir bereits beschrieben haben, wie man eine Conditional Access App Control-Richtlinie mit einer Sitzungsrichtlinie verknüpft, werden wir hier der Einfachheit halber eine Aktivitätsrichtlinie einsetzen.

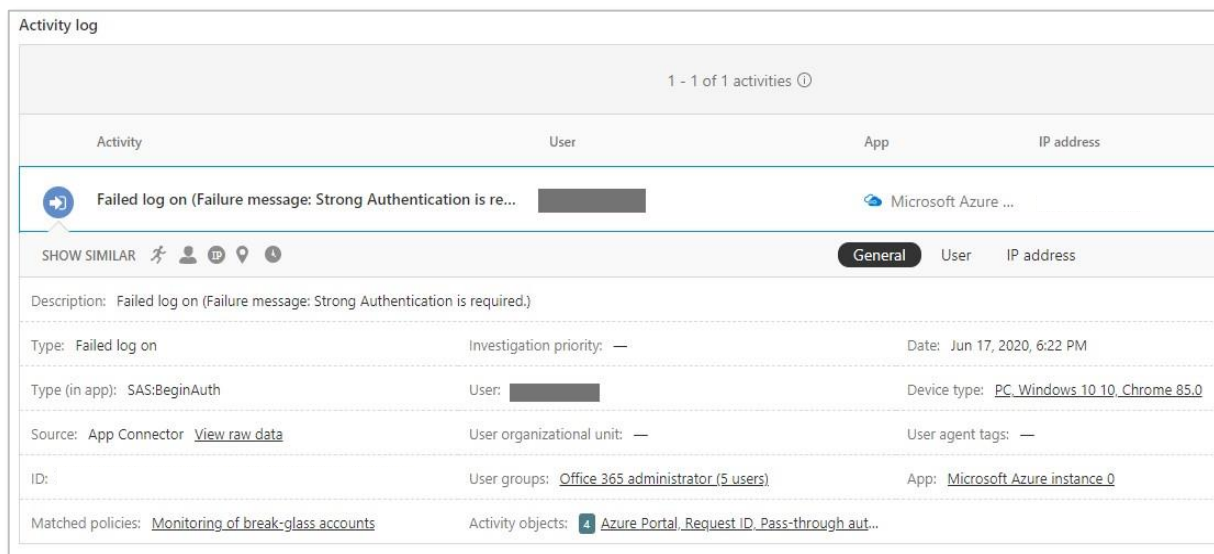
- 1) Navigiere im [Microsoft 365 Defender-Sicherheitsportal](#), zu **Richtlinien > Richtlinienverwaltung**.
- 2) Klicke auf **Richtlinie erstellen** und wähle **Aktivitätsrichtlinie** aus.
- 3) Gib im nächsten Schritt folgende Informationen ein:
  - a) Richtlinienname: **Nutzung sensibler Konten überwachen**
  - b) Schweregrad: **Hoher Schweregrad**
  - c) Kategorie: **Zugangskontrolle**
  - d) Anwenden auf: **Einzelne Aktivität**
  - e) Beschreibung: **Diese Richtlinie wird verwendet, um Anmeldeaktivitäten für sensible Konten zu überwachen.**
  - f) Erstelle den folgenden Filter:
    - i) **Benutzer + Aus Gruppe + ist gleich + "Sensible Konten"**
    - ii) **IP-Adresse + Kategorie + ist nicht gleich + Unternehmen**
    - iii) **Aktivitätstyp + ist gleich + Fehlgeschlagene Anmeldung, Anmeldung**



Wähle zur Alarmierung den Mechanismus, der für dich am besten funktioniert. Du könntest auch einen Power Automate Flow erstellen, der automatisch ein Ticket in deinem Service-Desk-System erzeugt.

Nachdem du die Regel gespeichert hast, kannst du sie testen, indem du dich mit einem Konto aus der Gruppe **Sensible Konten** von einer IP-Adresse anmeldest, die nicht der Kategorie **Unternehmen** zugeordnet ist. Nach einigen Minuten sollte die entsprechende Warnung in MDCA erscheinen.

Das ist nicht ganz ideal. Dir ist vielleicht aufgefallen, dass wir sowohl fehlgeschlagene als auch erfolgreiche Anmeldungen überwachen. Auch wenn du theoretisch nur bei einer erfolgreichen Anmeldung eine Warnung erwartest, meldet Entra ID manche Aktivitäten auf eine Weise an MDCA, die wie eine fehlgeschlagene Anmeldung aussieht – wie in Abbildung 11-27 dargestellt:









Activity log			
1 - 1 of 1 activities ⓘ			
Activity	User	App	IP address
 <b>Failed log on</b> (Failure message: Strong Authentication is re... <span style="background-color: black; color: black;">[REDACTED]</span>		 Microsoft Azure ...	
SHOW SIMILAR    			
Description: Failed log on (Failure message: Strong Authentication is required.)			
Type: Failed log on	Investigation priority: —	Date: Jun 17, 2020, 6:22 PM	
Type (in app): SAS:BeginAuth	User: <span style="background-color: black; color: black;">[REDACTED]</span>	Device type: <a href="#">PC_Windows 10 10_Chrome 85.0</a>	
Source: App Connector <a href="#">View raw data</a>	User organizational unit: —	User agent tags: —	
ID:	User groups: <a href="#">Office 365 administrator (5 users)</a>	App: <a href="#">Microsoft Azure instance 0</a>	
Matched policies: <a href="#">Monitoring of break-glass accounts</a>		Activity objects: <a href="#">4 Azure Portal_Request ID_Pass-through aut...</a>	

Abbildung 11-27: Details des Aktivitätsprotokolls.

Wenn du nicht genau hinschaust, könntest du eine tatsächlich erfolgreiche Anmeldung fälschlicherweise als Fehlversuch interpretieren. Der Grund dafür liegt oft darin, dass während der Multi-Faktor-Authentifizierung eine alternative Methode gewählt wurde, wodurch der erste Authentifizierungsversuch fehlschlägt. Danach erfolgt sofort eine erfolgreiche Anmeldung. Entra ID stellt diese Information korrekt dar, MDCA allerdings nicht. Deshalb solltest du auch fehlgeschlagene Anmeldeversuche in deine Richtlinie aufnehmen. Wenn du das vermeiden möchtest, verwende lieber eine Zugriffsrichtlinie.

# Verhindern, dass Gastbenutzer Word-Dateien aus SharePoint Online herunterladen

## Szenario

Du arbeitest für eine Gesundheitsorganisation und weißt, wie sensibel die Daten sind, die du verwaltest. Deine Organisation arbeitet auch mit externen Anbietern zusammen, die gelegentlich Zugriff auf Patientenakten benötigen, die typischerweise in Word-Dateien gespeichert sind. Der einfachste Weg, diesen Zugriff zu gewähren, ist es, den Gastbenutzern Zugriff auf die entsprechende SharePoint-Bibliothek zu geben. Leider hast du bisher weder Labels noch dokumentenbasierten Schutz implementiert. Daher brauchst du eine andere Möglichkeit, die Daten zu schützen. In diesem Fall soll das Herunterladen von Dateien durch Gastbenutzer verhindert werden.

## Lösung

Es gibt mehrere Wege, das zu erreichen. SharePoint Online bietet die Möglichkeit, Downloads auf nicht verwalteten Geräten zu blockieren. Es wäre zwar plausibel anzunehmen, dass Gastbenutzer kein verwaltetes Gerät verwenden, aber das allein reicht nicht aus, um das Herunterladen sicher zu unterbinden.

Was wir mit Sicherheit brauchen, ist eine **Sitzungsrichtlinie**. Denn wir wollen Downloads verhindern – nicht erst im Nachhinein reagieren. Letzteres wäre der Anwendungsfall für eine Aktivitätsrichtlinie.

Erstelle daher zunächst eine Richtlinie für bedingten Zugriff, die ausgelöst wird, wenn ein Gastbenutzer auf SharePoint Online zugreift. Öffne das Entra ID-Portal und gehe zu **Bedingter Zugriff**. Klicke auf **Neue Richtlinie** und konfiguriere sie wie folgt:

- **Name:** Sitzungsrichtlinie: Download von SPO für Gastbenutzer einschränken
- **Zuweisungen:** Ausgewählte Benutzer und Gruppen > **Alle Gast- und externen Benutzer**
- **Cloud-Apps oder -Aktionen:** Cloud-Apps > Apps auswählen > **Office 365 SharePoint Online**
- **Zugriffssteuerung:** *Sitzung* > **Conditional Access App Control verwenden** und *Benutzerdefinierte Richtlinie verwenden* auswählen.

Optional kannst du zusätzliche Bedingungen konfigurieren, z. B. ob die Richtlinie für alle Anwendungen oder nur für Browser gilt. Beachte, dass sie derzeit für alle SharePoint-Websites gilt. Es gibt keine Möglichkeit, bestimmte Steuerelemente nur auf eine einzelne Website anzuwenden. Microsoft hat jedoch angekündigt, dass zukünftig daran gearbeitet wird, einzelne SharePoint-Websites gezielt auswählen zu können. Bis dahin gilt: alles oder nichts.

Nachdem du die Richtlinie für bedingten Zugriff erstellt hast, wechsele zu Defender for Cloud Apps, um die Sitzungsrichtlinie zu erstellen. Klicke auf „**Richtlinien**“ > „**Richtlinienverwaltung**“ und dann auf „**Richtlinie erstellen**“. Wähle „**Sitzungsrichtlinie**“ aus. In diesem Beispiel verwenden wir keine Vorlage, daher wähle für die Richtlinienvorlage „**Keine Vorlage**“ aus.

Achte darauf, deiner Richtlinie einen Namen zu geben, den du später leicht wiederfindest. Vergiss auch nicht, eine Beschreibung zum Zweck der Richtlinie hinzuzufügen. Du weißt vielleicht beim Erstellen genau, worum es geht – aber was ist, wenn du sie ein paar Monate später erneut aufrufst? Oder wenn ein Kollege damit arbeitet?

Wähle als Sitzungssteuerungstyp die Option „**Dateidownload steuern (mit Überprüfung)**“. Konfiguriere dann die Aktivitäten wie in Abbildung 11-25 dargestellt:

The screenshot shows the configuration interface for a session policy in Microsoft Defender for Cloud Apps. It is divided into three main sections:

- Activity source:**
  - Header: "Add activity filters to the policy"
  - Summary: "activities matching all of the following" with an "Edit and preview results" link.
  - Filters:
    - Filter 1: Device (dropdown), Tag (dropdown), does not equal (dropdown), Intune compliant, Hybrid Azure AD joined (dropdown), and an info icon.
    - Filter 2: App (dropdown), equals (dropdown), Select apps... (dropdown).
    - Link: "+ Add a filter"
- File filters:**
  - Header: "Add file filters to the policy"
  - Summary: "files matching all of the following"
  - Filters:
    - Link: "Select a filter..." with a dropdown arrow.
    - Link: "+ Add a filter"
- Inspection method:**
  - Dropdown menu currently set to "None".

Abbildung 11-25: Konfigurieren einer Sitzungsrichtlinie in MDCA.

- Die App sollte Microsoft SharePoint Online entsprechen

- Da wir Downloads von Word-Dateien nur einschränken wollen, muss die Erweiterung > *doc* oder *docx* entsprechen.

**Hinweis:** Es ist nicht notwendig, die Inhaltsüberprüfung zu aktivieren, da lediglich die Dateierweiterung betrachtet wird.

Wähle unter **Aktionen** unbedingt „**Blockieren**“ aus. Es ist außerdem sinnvoll, eine benutzerdefinierte Nachricht hinzuzufügen, die mehr Kontext liefert, wenn die Blockierungsmeldung angezeigt wird.

**Begrenzter Platz:** Da der Textumfang für eine angepasste Blockierungsmeldung begrenzt ist, empfiehlt es sich, einen Link oder einen Verweis auf eine Kontaktperson einzufügen, an die sich betroffene Benutzer wenden können.

#### Actions

Select an action to be applied when user activity matches the policy.

☐ **Test**

Monitor all activities

☒ **Block**

Block file download & monitor all activities

☐ Also notify user by email

☒ Customize block message ⓘ

You are not authorized to download from this website. Please get in touch with your liaison at our organization for more information.

Abbildung 11-26: Konfigurieren von Aktionen in einer Sitzungsrichtlinie.

## Benutzererfahrung

Eine Sitzungsrichtlinie erfordert einen etwas genaueren Blick auf die Benutzererfahrung. Sobald du die oben beschriebenen Richtlinien konfiguriert hast und sich ein Gastbenutzer bei SharePoint Online anmeldet, wird er zunächst darüber informiert, dass die Sitzung über Defender for Cloud Apps überwacht wird:

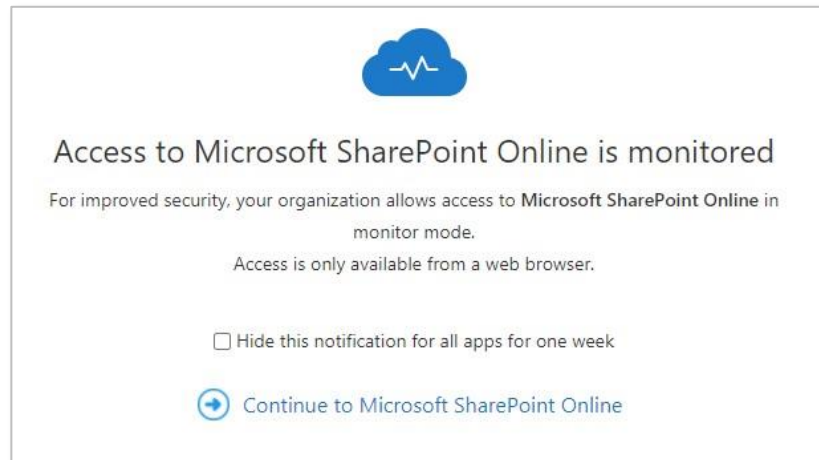


Abbildung 11-27: Benutzerbenachrichtigung zur Sitzungsüberwachung über MDCA.

Anschließend kann der Benutzer SharePoint Online weitgehend wie gewohnt verwenden. Beachte jedoch, dass die URL der Seite auf \*.mcas.ms verweist, was zeigt, dass der Datenverkehr über die MDCA-Infrastruktur geleitet wird. Der Benutzer kann weiterhin beliebige Aktionen ausführen und sogar Dateien herunterladen, die nicht von der Richtlinie betroffen sind. Versucht er jedoch, eine Word-Datei mit der Erweiterung .doc oder .docx herunterzuladen, wird ihm eine Warnung wie in Abbildung 11-28 angezeigt. Die Datei kann jedoch weiterhin im Browser geöffnet werden.

**Desktop-Apps:** Beachte, dass die Einschränkung von Downloads auch die Verwendung von Desktop-Apps einschränkt. Wenn versucht wird, eine Datei in einer Desktop-App zu öffnen, wird normalerweise eine temporäre Kopie der Datei lokal gespeichert. Da dies blockiert ist, erscheint beim Benutzer die Meldung, dass die erforderlichen Informationen nicht heruntergeladen werden konnten. Leider wird keine benutzerdefinierte Fehlermeldung angezeigt.

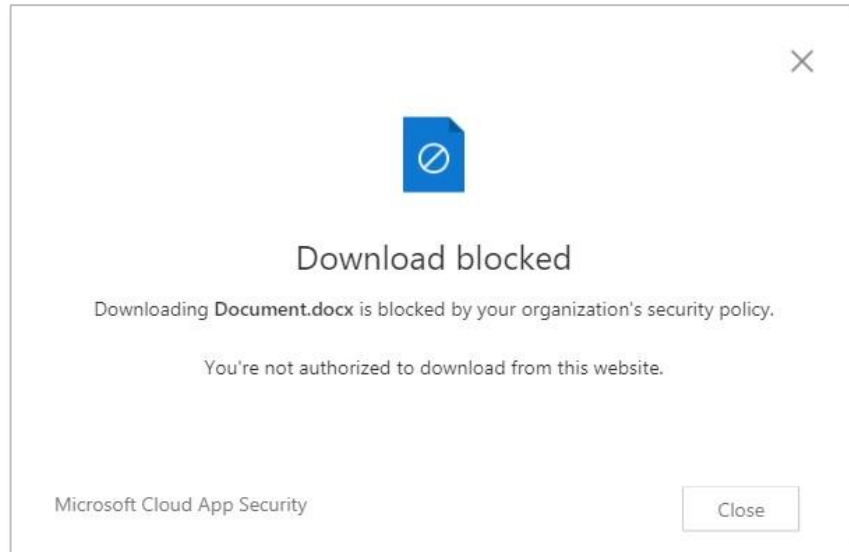


Abbildung 11-28: Blockierter Download durch eine MDCA-Sitzungsrichtlinie.

## Downloads von nicht verwalteten Geräten in Exchange Online blockieren

In Kapitel 3 haben wir gezeigt, wie du mit integrierten Funktionen in SharePoint Online und Exchange Online den Zugriff von nicht verwalteten Geräten einschränken kannst. Leider bieten nur diese beiden Workloads solche integrierten Funktionen. Für alle anderen Workloads musst du auf einen alternativen Mechanismus wie Sitzungsrichtlinien zurückgreifen, um das Verhalten nicht verwalteter Geräte zu steuern.

Um eine Sitzungsrichtlinie zu erstellen, öffne das Defender for Cloud Apps-Portal, navigiere zu „**Richtlinien**“ > „**Richtlinienverwaltung**“ und klicke auf „**Richtlinie erstellen**“. Wähle „**Sitzungsrichtlinie**“ aus dem Dropdown-Menü. Gib anschließend einen Namen, eine Beschreibung, einen Richtlinienschweregrad und eine Kategorie an. Diese Einstellungen beeinflussen nicht direkt die Funktionsweise der Richtlinie, sind aber wichtig, vor allem wenn du mit vielen verschiedenen Richtlinien arbeitest.

Wähle unter **Sitzungssteuerungstyp** erneut „**Dateidownload steuern (mit Überprüfung)**“ aus. Dadurch erscheint der Abschnitt zur Konfiguration des Aktivitätsfilters. Der vorgeschlagene Filter deckt das Szenario möglicherweise bereits ab. Falls nicht, achte darauf, dass du in der Dropdown-Liste die Optionen „Intune-konform“ und „Hybrid Entra ID-beigetreten“ auswählst:



activities matching all of the following Edit and preview results

Filters:

- X App equals Microsoft Exchange Online
- X Device Tag does not equal Hybrid Azure AD joined, Intune compliant ⓘ

+ Add a filter

Abbildung 11-29: Ausrichtung auf nicht verwaltete Geräte mit MDCA

Stelle sicher, dass du Exchange Online als Anwendung hinzufügst. Wenn Exchange Online nicht in der Liste der Anwendungen erscheint, wurde die App noch nicht als App Control-fähige Anwendung erkannt. In diesem Fall genügt es, eine Richtlinie für bedingten Zugriff zu erstellen, die die Sitzung über MDCA umleitet, und sich einmal bei der Anwendung anzumelden. Danach steht sie zur Auswahl.

Nachdem du die App-Details definiert hast, wähle „**Keine**“ als Überprüfungsmethode und „**Blockieren**“ unter **Aktionen**. Konfiguriere bei Bedarf zusätzliche Benachrichtigungen und aktiviere die Generierung von Warnungen.

Inspection method

None

**Actions**

Select an action to be applied when user activity matches the policy.

☐ **Test**  
Monitor all activities

☒ **Block**  
Block file download & monitor all activities

☐ Also notify user by email

☐ Customize block message ⓘ

☐ **Protect**  
Apply classification label to downloads & monitor all activities

Figure 11-30: blocking download activities in a session policy.

Wir gehen hier davon aus, dass du bereits eine Richtlinie für bedingten Zugriff erstellt hast, die den Datenverkehr über Microsoft Defender for Cloud Apps leitet.

Sobald deine Sitzungsrichtlinie aktiv ist, wird jede Sitzung beim Anmelden bei Exchange Online zu Defender for Cloud Apps umgeleitet. Versuchst du nun, eine Datei herunterzuladen, wird die gleiche Fehlermeldung angezeigt wie im vorherigen Beispiel.

## MFA beim Herunterladen sensibler Dateien von nicht verwalteten Geräten anfordern

Angelehnt an das vorherige Beispiel hat Defender for Cloud Apps kürzlich die Vorschaufunktion Step-up-Authentifizierung eingeführt. Diese neue Funktion ermöglicht es, bei bestimmten Bedingungen innerhalb einer Sitzung eine zusätzliche Authentifizierung anzufordern. Du könntest etwa MFA verlangen, wenn ein Benutzer eine sensible Datei herunterladen möchte oder wenn ein Download von einem nicht verwalteten Gerät aus erfolgt.

Um eine Step-up-Authentifizierung zu erzwingen, musst du eine entsprechende Sitzungsrichtlinie erstellen. Damit diese funktioniert, musst du sicherstellen, dass die Benutzersitzung über Defender for Cloud Apps umgeleitet wird. Üblicherweise geschieht das über eine Richtlinie für bedingten Zugriff, in der du die Aktion „Conditional Access App Control verwenden“ auswählst. Mit der Einführung der Step-up-Authentifizierung hat Entra ID auch den sogenannten Authentifizierungskontext eingeführt. Dieser definiert Kriterien, die verwendet werden können, um Ressourcen wie SharePoint-Websites zu kennzeichnen und darauf basierend spezifische Bedingungen auszulösen, die du in der entsprechenden Richtlinie für bedingten Zugriff definierst. Ein Authentifizierungskontext kann somit als Auslöser in einer Richtlinie verwendet werden – entweder auf Basis einer App, einer Benutzeraktion oder eben eines Kontexts.

Um einen Authentifizierungskontext zu erstellen, navigiere im Entra ID-Portal zu „**Sicherheit**“ > „**Bedingter Zugriff**“ > „**Authentifizierungskontext**“. Klicke dort auf „**Neuer Authentifizierungskontext**“ und gib die erforderlichen Details ein. Weitere Informationen zum Authentifizierungskontext findest du in Kapitel 2.

Sobald du den Kontext erstellt hast, kehre zurück zu Defender for Cloud Apps und erstelle eine Sitzungsrichtlinie mit den folgenden Details:

**Session control type \***  
Select the type of control you want to enable:

Control file download (with inspection) ▼

**Activity source**  
Add activity filters to the policy

activities matching all of the following 👁 Edit and preview results

**Filters:**

✕ App ▼ equals ▼ Microsoft SharePoint Online ▼

+ Add a filter

Abbildung 11-31: Konfigurieren einer Sitzungsrichtlinie.

Wähle dann unter **Aktionen** die Option **Step-up-Authentifizierung** anfordern und wähle den Authentifizierungskontext aus, den du zuvor erstellt hast, wie in Abbildung 11-33 dargestellt:

☒ **Require step-up authentication** PREVIEW FEATURE ⓘ

Re-evaluate Azure AD Conditional Access policies based on the authentication context.  
Unpublished authentication context will not be enforced

[Configure authentication context](#) ⓘ

Sensitive Information ▼

Abbildung 11-32: Konfigurieren einer Sitzungsrichtlinie.

Sobald du die Richtlinie erstellt hast, wirst du beim nächsten Anmelden bei einer SharePoint Online-Website feststellen, dass sie über Defender for Cloud Apps umgeleitet wird. Wenn du eine Datei herunterladen möchtest (zum ersten Mal), siehst du eine Meldung wie in Abbildung 11-33 dargestellt. Sobald du auf „**OK, fortfahren**“ klickst, wird der Benutzer aufgefordert, MFA durchzuführen.

Wichtig zu beachten ist, dass keine zusätzliche MFA erforderlich ist, wenn ein Benutzer bereits bei der ersten Anmeldung MFA durchgeführt hat. Dasselbe gilt, wenn sich ein Benutzer mit Hello for Business bei einem Gerät angemeldet hat. Da die Anmeldung bereits die MFA-Anforderung erfüllt (Hello for Business ist schließlich MFA), ist keine zusätzliche Authentifizierung erforderlich.

**Vorschau:** Da sich die Funktion derzeit in der Vorschau befindet, ist Folgendes zu beachten: Obwohl du einen Authentifizierungskontext erstellt musst, bevor du eine Sitzungsrichtlinie erstellen kannst, die eine Step-up-Authentifizierung erfordert, scheint es, dass du deine SharePoint-Website(s) nicht „kennzeichnen“ musst, um die Aktion auszulösen, und auch keine Richtlinie für bedingten Zugriff anwenden musst. Dies kann zunächst etwas verwirrend sein. Es könnte sich um eine Besonderheit der Vorschaufunktion handeln oder um das erwartete Verhalten in dieser Phase. Stelle auf jeden Fall sicher, dass du deinen Anwendungsfall gründlich testest. Es gibt natürlich auch andere Anwendungsfälle, in denen ein Authentifizierungskontext selbst nützlich sein könnte und für die du möglicherweise eine Richtlinie für bedingten Zugriff benötigst. Aber das ist ein Thema, das wir zu einem späteren Zeitpunkt näher betrachten können.

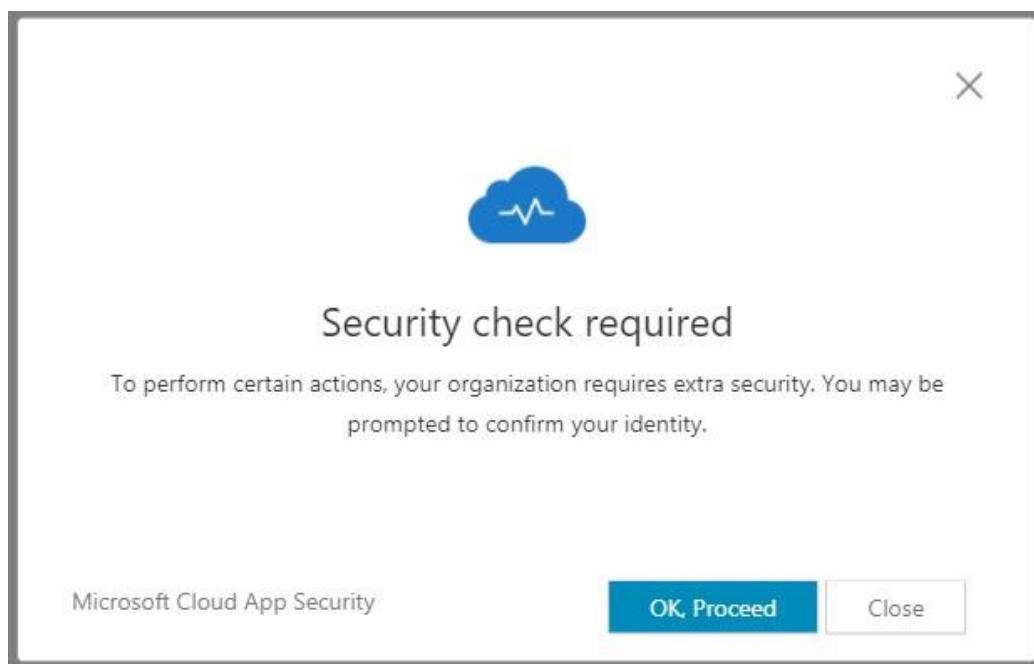


Abbildung 11-33: Anfordern einer zusätzlichen Sicherheitsüberprüfung.

## Microsoft 365 Defender

In diesem Kapitel haben wir fast jeden Aspekt von Microsoft Defender for Cloud Apps behandelt. Wir haben versucht, so viel wie möglich hervorzuheben, aber es gibt noch viel zu entdecken! Inzwischen solltest du erkennen, dass MDCA eine sehr leistungsfähige Lösung ist, die dir nicht nur enorme Einblicke in das Geschehen innerhalb (und sogar außerhalb!) deines Netzwerks gibt, sondern es dir auch ermöglicht, zu überwachen und zu steuern, wie Cloud-Anwendungen innerhalb deiner Organisation verwendet werden. Einer der größten Vorteile von MDCA ist die Möglichkeit einer nahtlosen Integration mit anderen Microsoft-Produkten wie Microsoft Defender for Endpoint, Identity Protection und Microsoft Defender for Identity. Lass uns im nächsten Kapitel mit Microsoft 365 Defender fortfahren, um mehr über

produktübergreifende Integrationen zu sprechen und warum es so wichtig ist, eine End-to-End-Lösung anbieten zu können.