



Microsoft Defender for Endpoint

Der Praxisleitfaden für Deine Konfiguration

- **Attack Surface Reduction-Regeln anwenden**
- **Endpoint Detection & Response verstehen**
- **Onboarding und Monitoring einrichten**



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

 WEBSITE siller.consulting

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

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

Inhaltsverzeichnis

Microsoft Defender für Endpunkte.....	5
Die Notwendigkeit eines intelligenteren Endpunktsschutzes	5
Was ist Microsoft Defender für Endpunkte?	6
MDE als Katalysator für Ihre Sicherheitslage	8
Die Bedeutung von KI und maschinellem Lernen.....	9
Lizenzierung	10
Defender für Endpunkte "Plan 1"	11
Microsoft Defender für Unternehmen.....	12
Lizenzen mischen	13
Datenspeicherung und Standort.....	14
Datenisolierung.....	15
Warum werden Daten in der Cloud gespeichert?	15
Konfiguration von Microsoft Defender für Endpunkte (Plattform).....	16
Zugriffsverwaltung für Defender für Endpunkte.....	16
Grundkonfiguration.....	20
Integration mit anderen Microsoft 365-Diensten.....	21
Verwaltung von Microsoft Defender für Endpunkte (Endpunkte).....	22
Bereitstellung (Onboarding)	23
Richtlinienverwaltung	51
Fehlersuche bei Defender for Endpoint auf dem Endpunkt	53
Offboarding	54
Secure Score.....	55
Next-Gen Protection	56
Cloudbasierter Schutz	57
Next-Gen-Schutz konfigurieren.....	61
Netzwerk- & Webschutz.....	71
Attack Surface Reduction	78
Attack Surface Reduction Rules	78

Application Control	87
Application Guard (App & Browser Isolation).....	87
Exploit Protection.....	92
Device Control.....	95
Endpoint Detection & Response (EDR)	99
Sysmon vs. Defender for Endpoint.....	100
Indikatoren für Kompromittierungen	101
Automatisierte Untersuchung & Reaktion (AIR)	103
Live Response.....	108
Advanced Hunting.....	109
Microsoft Defender for IoT	109
Was ist Microsoft Defender for IoT?	110
Geräte erkennen	111
Einrichten von Microsoft Defender for Enterprise IoT.....	113
IoT-Geräte überprüfen	114
Über den Endpunkt und IoT hinaus	115

Microsoft Defender für Endpunkte

Die Notwendigkeit eines intelligenteren Endpunktenschutzes

Es ist unbestreitbar: Angriffe werden immer ausgefeilter. Um uns vor solchen Angriffen zu schützen, müssen sich die Tools und Lösungen, die wir verwenden, zusammen mit den Bedrohungen weiterentwickeln – nur dann haben wir eine faire Chance. Während früher ein einfacher, signaturbasierter VirensScanner ausreichte, um die meisten Bedrohungen zu erkennen, ist das heute längst nicht mehr der Fall. Wenn du als Verteidiger deine Endpunkte angemessen absichern willst, musst du eine Vielzahl von Techniken und Lösungen einsetzen, um sicherzustellen, dass du die unzähligen Bedrohungen, denen deine Endpunkte ausgesetzt sind, abwehren, erkennen und darauf reagieren kannst.

In Bezug auf den Endpunktenschutz bedeutete die Einführung von EDR-Lösungen für viele Unternehmen einen großen Fortschritt. EDR steht für Endpoint Detection and Response und beschreibt eine Cybersicherheitslösung, die sich auf die Erkennung und Reaktion auf Bedrohungen auf Endgeräten wie Laptops, Desktops, Servern und Mobilgeräten konzentriert.

Ziel von EDR ist es, Endgeräte in Echtzeit zu schützen und Sicherheitsteams die nötige Transparenz und Werkzeuge zu geben, um Bedrohungen schnell zu erkennen und darauf zu reagieren. EDR-Lösungen kombinieren in der Regel signaturbasierte Erkennung, Verhaltensanalyse und maschinelles Lernen, um verdächtige Aktivitäten auf Endgeräten zu identifizieren. Sie bieten auch eine zentralisierte Verwaltungskonsole, mit der Sicherheitsteams die Endpunktssicherheit überwachen und in Echtzeit auf Vorfälle reagieren können.

EDR-Lösungen werden zunehmend wichtiger, da Angreifer ihren Fokus von netzwerkbasierten Angriffen auf Endpunktangriffe verlagern. Durch das Kompromittieren eines Endgeräts können Angreifer Zugriff auf sensible Informationen erlangen, Malware installieren und weitere bösartige Aktivitäten ausführen. EDR-Lösungen helfen Unternehmen dabei, solche Angriffe zu erkennen und zu verhindern – damit die Endgeräte sicher bleiben.

Im Sinne der „Assume Breach“-Denkweise reicht es nicht aus, sich nur auf das Verhindern von Viren und Malware zu verlassen. Du musst böswillige Aktivitäten erkennen können – insbesondere, weil es gut sein kann, dass dein VirensScanner in der Anfangsphase eines Angriffs die Nutzlast nicht erkennt. Das liegt nicht unbedingt an einem schlechten VirensScanner, sondern daran, dass es immer schwieriger wird, bösartige Nutzlasten zuverlässig zu erkennen.

Hinzu kommt, dass Sicherheitsprodukte selbst manchmal Schwachstellen aufweisen, über die Angreifer die Erkennung umgehen können. Als wäre das nicht schon genug, gibt es noch eine

Vielzahl weiterer Techniken, mit denen Angreifer versuchen, unentdeckt zu bleiben. Ein Beispiel ist die zunehmende Nutzung legitimer Binärdateien für illegitime Zwecke. Diese Technik, bekannt als „Living off the Land Binaries“ (LOLBins), verlangt vom Endpunktsschutz eine neue Perspektive: Die ausführende Datei ist möglicherweise legitim – aber die Aktionen, die durch sie ausgelöst werden, sind es nicht.

Trotz dieser Erkenntnisse setzen viele Unternehmen weiterhin auf klassische, signaturbasierte Antivirenlösungen – und bleiben damit anfällig für moderne, ausgeklügelte Bedrohungen. In diesem Kapitel wollen wir deshalb die Funktionen von Microsoft Defender für Endpunkte genauer unter die Lupe nehmen. Du erfährst, wie diese Lösung funktioniert und wie sie dir helfen kann, deine Sicherheitslage deutlich zu verbessern.

Was ist Microsoft Defender für Endpunkte?

Bevor wir näher auf die Funktionsweise von Defender für Endpunkte eingehen, klären wir zunächst, was eine EDR ist: eine Lösung, die potenziell schädliche Aktivitäten auf oder durch ein Gerät überwacht, Informationen dazu sammelt und dir verschiedene Möglichkeiten bietet, auf diese Ereignisse zu reagieren. Solche Aktivitäten umfassen zum Beispiel Dateioperationen, Änderungen an Registrierungsschlüsseln und vieles mehr. Die Informationen werden typischerweise an ein zentrales System gesendet, wo sie auf verdächtiges Verhalten analysiert werden. Auf Basis dieser Analyse kann das System anschließend entscheiden, ob und welche Maßnahmen erforderlich sind – das ist der „Response“-Teil von EDR.

Microsoft Defender für Endpunkte ist Microsofts moderne Endpoint-Sicherheitslösung. Sie ist weit mehr als nur ein Antivirenprogramm – und auch mehr als eine klassische EDR-Lösung. In Kombination mit anderen Sicherheitsfunktionen in Microsoft 365 wird sie zu einem zentralen Bestandteil deiner Sicherheitsstrategie und kann deine Schutzmaßnahmen deutlich verbessern.

Konkret ist Microsoft Defender für Endpunkte eine Kombination mehrerer Funktionen und Produkte, die zusammen eine umfassende Sicherheitsschicht für deine Endpunkte bilden. Dabei zählen nicht nur Laptops und Desktops als Endpunkte – auch Server und mobile Betriebssysteme werden unterstützt. Einer der großen Vorteile dieser Lösung ist die enge Integration in Microsofts moderne Betriebssysteme ab Windows 10 und Windows Server 2019. Dadurch gestaltet sich die Bereitstellung deutlich einfacher, ohne dass du zusätzliche Agenten installieren musst.

Bevor wir uns anschauen, wie du Defender für Endpunkte in deiner Umgebung nutzen kannst, werfen wir einen Blick auf die Bestandteile der Suite. Die folgende Abbildung zeigt dir, welche Funktionen unter dem Dach von Microsoft Defender für Endpunkte zusammenkommen.

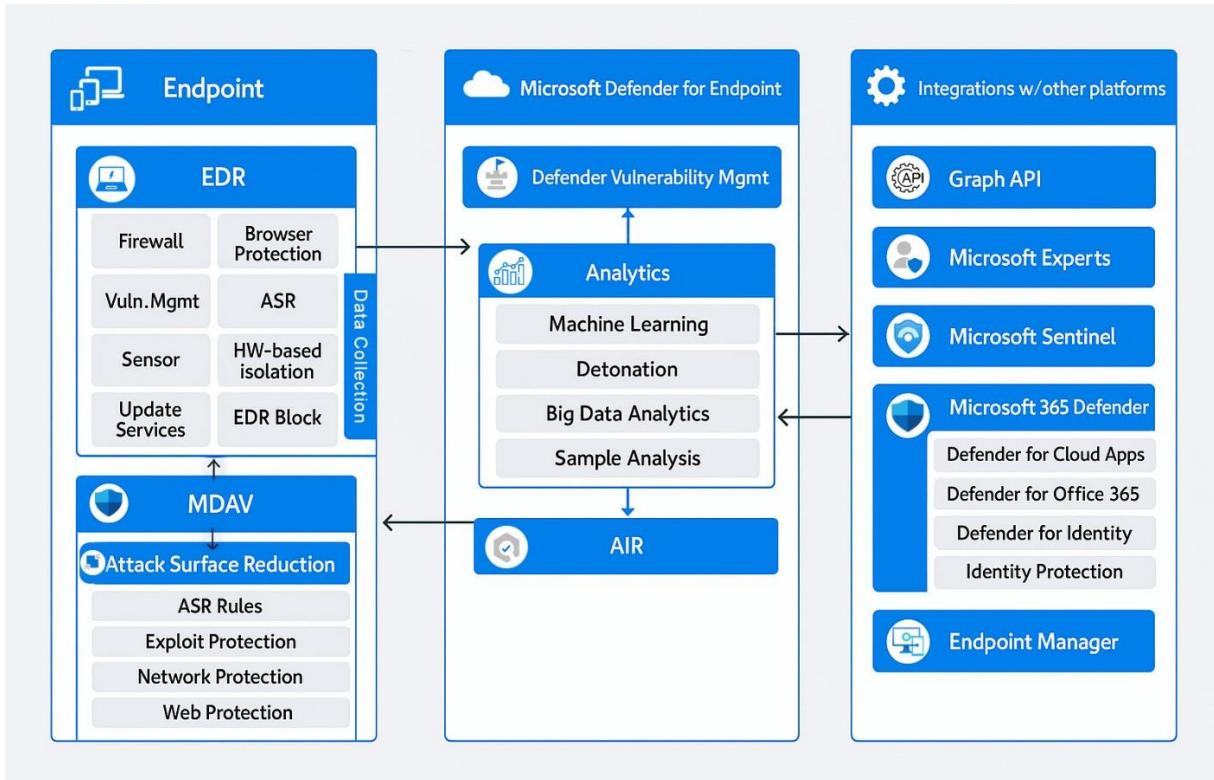


Abbildung 7-1: High-Level-Architektur von Microsoft Defender für Endpunkte

Unter der Haube besteht Microsoft Defender für Endpunkte aus mehreren Funktionen:

- **Microsoft Defender Antivirus**, manchmal auch als *Next-Gen Protection* bezeichnet. Dies ist der Kern von Defender für Endpunkte und unter anderem für das Scannen von Dateien, das Blockieren von Aktivitäten usw. verantwortlich.
- **Endpoint Detection and Response (EDR)** ist der Teil der Suite, der kontinuierlich Telemetriedaten von den Endpunkten sammelt und zur weiteren Analyse an die Cloud-Komponenten hochlädt.
- **Automated Investigation & Remediation (AIR)**, die selbstheilende Engine, die automatisch eine detailliertere Untersuchung starten und geeignete Maßnahmen auf den Endpunkten ergreifen kann.
- **Attack Surface Reduction**, eine Gruppe von Funktionen, die zusammen dazu beitragen, die Angriffsfläche des Endpunkts zu reduzieren.
- **Vulnerability Management**, bewertet kontinuierlich den Konfigurationszustand der Endpunkte, überprüft sie auf bekannte Schwachstellen und empfiehlt Anwendungen und Konfigurationsupdates, die die Gesamtsicherheit des Geräts (bzw. Betriebssystems) verbessern können. Angesichts der Bedeutung des Schwachstellenmanagements – und auch aufgrund der Existenz spezifischer Schwachstellenmanagement-Angebote von Microsoft – widmen wir diesem Thema ein eigenes Kapitel.

- **Secure Score für Geräte** ist ebenfalls Teil von Microsoft Defender für Endpunkte, wird jedoch im Kapitel „Microsoft 365 Defender“ behandelt, wo der Secure Score ausführlicher besprochen wird.

Was du in diesem Kapitel lernen wirst, ist, dass Microsoft Defender für Endpunkte eine sehr umfassende Lösung ist, mit der es zu Beginn etwas schwierig sein kann, erste Schritte zu machen. In der Cloud geboren und geschmiedet, bietet es ein ausgewogenes Schutzniveau, bei dem Offline-Funktionen mit zusätzlichen Funktionen und Schutz kombiniert werden, die von den Cloud-Gegenstücken angetrieben werden.

MDE als Katalysator für Ihre Sicherheitslage

Defender für Endpunkte kann aufgrund der vielen Funktionen und der Integrationen mit anderen Sicherheitsprodukten wie Defender für Identitäten, Defender für Cloud-Apps und Microsoft 365 Defender ein enormer Gewinn für deine Sicherheitsabläufe sein.

In Kapitel 1 haben wir beschrieben, wie du eine effektive Sicherheitsstrategie aufbauen kannst, um die verschiedenen Risiken und Bedrohungen abzudecken, mit denen dein Unternehmen konfrontiert sein kann. Defender für Endpunkte hilft dir dabei, deine Sicherheitsziele zu erreichen, da es in vielen Phasen aktiv ist – vom Schutz bis hin zur Reaktion. Um das zu veranschaulichen, sehen wir uns an, wie die verschiedenen Funktionen den Phasen der Kill Chain oder des NIST Cybersecurity Frameworks zugeordnet werden können.

Um deine Geräte vor verschiedenen Bedrohungen zu **schützen**, spielen sowohl Defender Antivirus als auch die Attack Surface Reduction eine wichtige Rolle. Sobald eine bekannte Bedrohung oder Aktivität erkannt wird, blockieren beide Produkte diese proaktiv und verhindern so, dass das Gerät kompromittiert wird – vorausgesetzt, du hast beide Funktionen entsprechend konfiguriert.

Da viele Aktivitäten überwacht werden, analysieren sowohl die lokalen Komponenten (in Microsoft Defender) als auch der Cloud-Dienst diese Ereignisse, um Unregelmäßigkeiten zu **erkennen**. Du kannst dir das wie das Sicherheitssystem eines Gebäudes vorstellen, bei dem das Sicherheitspersonal (Microsoft Defender) vor Ort ist und Kameras (Defender Cloud-Dienst) kontinuierlich alles überwachen. Der Überwachungsraum analysiert die Aufnahmen und meldet Auffälligkeiten an das Sicherheitspersonal, das sich die Situation vor Ort genauer ansieht.

Schließlich bietet Defender für Endpunkte aus Sicht der **Reaktion** eine Menge Flexibilität. Es kann nicht nur innerhalb von Sekunden automatisch reagieren, sondern auch deine Analysten und Incident Responder erhalten Tools und Funktionen wie Geräteisolierung und Live Response, um aus der Ferne mit potenziell kompromittierten Geräten zu interagieren.

Die Bedeutung von KI und maschinellem Lernen

Künstliche Intelligenz (maschinelles Lernen) spielt eine wichtige Rolle bei der Erkennung verdächtiger Aktivitäten. Da eine riesige Menge an Ereignissen aufgezeichnet wird, ist es für Menschen sehr schwierig, in der Flut an Informationen Auffälligkeiten herauszufiltern. Das ist vergleichbar mit einem Überwachungsraum, der die Aufnahmen von Hunderten von Kameras verarbeiten muss. Ohne ein ganzes Team, das alle Bildschirme ständig im Blick behält, ist es nahezu unmöglich, verdächtige Aktivitäten zuverlässig zu erkennen. Deshalb setzen moderne Überwachungssysteme oft (Gesichts-)Erkennungssoftware ein, um Informationen automatisch zu analysieren. Genauso arbeiten Sicherheitsprodukte mit maschinellem Lernen, um verdächtige Endpunktaktivitäten zu erkennen und automatisch als gutartig oder bösartig zu klassifizieren.

Es ist spannend zu verstehen, wie maschinelles Lernen bei Defender für Endpunkte eingesetzt wird. Neben der Fähigkeit, unendlich viele Informationen zu verarbeiten, haben sich automatisierte Systeme als deutlich präziser bei der Erkennung verschiedenster Aktivitäten erwiesen. Sie sind nicht nur schneller, sondern auch zuverlässiger.

Ohne zu sehr ins Detail zu gehen, verlässt sich Defender für Endpunkte hauptsächlich auf zwei Arten von maschinellen Lernmethoden:

- **Unüberwachte ML-Methoden** verwenden verschiedene Algorithmen, um nicht klassifizierte Datensätze zu analysieren und einzuordnen. Nicht klassifizierte Datensätze sind solche, die keine vorherige Kennzeichnung enthalten, die der ML-Methode mitteilt, mit welcher Art von Informationen sie es zu tun hat. Stattdessen schließt ein unüberwachtes Modell aus (große Mengen von) Daten auf Zusammenhänge und gruppiert bzw. trennt einzelne Elemente basierend auf ähnlichen Merkmalen. Das ist besonders nützlich bei der Anomalieerkennung, bei der abweichende Aktivitäten oder Werte erkannt werden. Innerhalb von Defender für Endpunkte werden unüberwachte Modelle eingesetzt, um ungewöhnliches Benutzerverhalten oder Netzwerkaktivitäten zu identifizieren.
- **Überwachte ML-Methoden** kommen in Defender für Endpunkte häufiger zum Einsatz. Dabei handelt es sich um Wesentlichen um trainierte Modelle, die Muster und Verhaltensweisen anhand von Beispielen erkennen, mit denen sie zuvor trainiert wurden. Du kannst dir das so vorstellen, als würdest du einem Modell Hunderttausenden von Bildern von Flugzeugen zeigen, damit es später in der Lage ist, ein Flugzeug auch auf einem neuen, unbekannten Bild korrekt zu erkennen.

Um den Unterschied zwischen den beiden Modellen besser zu erklären, schauen wir uns an, wie verdächtige Prozessaktivitäten erkannt werden können. Denk daran: Diese Erklärung ist bewusst vereinfacht und soll nur die Grundkonzepte veranschaulichen – es geht nicht darum,

tief in das maschinelle Lernen einzutauchen. Die tatsächliche Umsetzung in Produkten ist deutlich komplexer und berücksichtigt viele weitere Variablen und Feinheiten.

Ein unüberwachtes Modell, das nicht weiß, dass es sich mit Prozessen beschäftigt – und auch nicht, wie sich Prozesse üblicherweise verhalten – wäre trotzdem in der Lage, riesige Mengen an Prozessen zu analysieren und Unterschiede zu erkennen: zum Beispiel zwischen Prozessen, die selbst starten, anderen Prozessen starten, Dateien von bestimmten Orten öffnen, DLL-Dateien laden oder Artefakte in den Speicher injizieren. Und obwohl das Modell diese Aktivitäten unterscheiden kann, heißt das noch lange nicht, dass es sie als schädlich einstuft – es erkennt lediglich, dass diese Dinge passieren.

Ein überwachtes Modell dagegen wird mit verschiedenen Arten von Daten trainiert – darunter sowohl reguläre Prozesse als auch bösartige (zum Beispiel reale Malware-Proben). Dadurch hat es bereits ein Verständnis davon, wie ein normaler Prozess aussieht, welche Aktivitäten typisch sind, wie Images geladen werden usw. Gleichzeitig kennt es auch die typischen Verhaltensweisen von Schadsoftware. Dieses kombinierte Wissen darüber, wie Prozesse funktionieren sollten – und wie nicht –, erlaubt dem Modell, ein wesentlich präziseres Bild davon zu zeichnen, welche Aktivitäten abnormal sind. Zusätzlich kann Microsoft mehrere Modelle entwickeln, die speziell auf bestimmte Angriffsarten trainiert sind – etwa dateilose Angriffe, mehrstufige Angriffe oder Angriffe, die legitime Binärdateien oder Skripte missbrauchen.

Natürlich ist das Ganze in der Realität viel komplexer, und die tatsächliche Implementierung geht weit über das hinaus, was ich dir hier kurz erklärt habe. Aber ich hoffe, dass du nun besser nachvollziehen kannst, warum künstliche Intelligenz heute ein unverzichtbarer Bestandteil des modernen Endpunktenschutzes und damit auch der Sicherheitsprozesse ist.

Lizenzierung

Microsoft Defender für Endpunkte kann auf verschiedene Arten lizenziert werden. Die zahlreichen Optionen bieten viel Flexibilität und decken nahezu jedes Szenario ab. Da Defender für Endpunkte ein Bestandteil des Windows-Betriebssystems ist, ist es mit der Windows E5-SKU verfügbar. Diese ist Teil der folgenden Lizenzpakete:

- Windows 10 Enterprise E5/A5
- Microsoft 365 E5/A5
- Microsoft 365 E5 Security (Bundle)

Zusätzlich zu diesen Bundles kannst du Defender für Endpunkte auch als eigenständige Version (Add-on) oder über Microsoft Defender für Cloud im Standard-Plan erwerben (der Preis pro Server enthält hier auch die Lizenzkosten für Defender für Endpunkte).

Defender für Endpunkte "Plan 1"

Im August 2021 hat Microsoft einen neuen Plan für Defender für Endpunkte vorgestellt: „Plan 1“. Wie der Name schon andeutet, bietet Plan 1 weniger Funktionen als die Vollversion, die nun als „Plan 2“ bezeichnet wird.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL blocking	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
API's, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts **		✓

** Includes Targeted Attack Notifications (TAN) and Experts on Demand (EOD). Customers must apply for TAN and EOD is available for purchase as an add-on.

Abbildung 7-2: Unterschied zwischen Defender für Endpunkte Plan 1 und Plan 2. Bild mit freundlicher Genehmigung von Microsoft.

Eine der größten Herausforderungen für Microsoft im Vergleich zu anderen AV-Anbietern war (oder ist), dass sie bis zur Einführung von Plan 1 keine wirklich zentral verwaltete Antivirenlösung wie viele ihrer Mitbewerber hatten. Wenn man den System Center Endpoint Protection-Agenten außen vor lässt, war das lange Zeit ein großes Defizit. Umso besser ist es, dass diese Option nun existiert und Unternehmen eine zentrale Konsole nutzen können, um Geräte zu verwalten – auch wenn sie dabei nicht auf alle erweiterten Funktionen zugreifen können.

Um Defender für Endpunkte Plan 1 nutzen zu können, brauchst du trotzdem ein Tool zur Geräteverwaltung – zum Beispiel Microsoft Intune (Endpoint Manager) oder den System Center

Configuration Manager. Nur so stellst du sicher, dass deine Geräte ordnungsgemäß in die Plattform eingebunden sind.

Kleiner Unterschied: Es gibt keinen Unterschied in der Verwaltung von Geräten, die mit einer "Plan 1"- oder "Plan 2"-Lizenz ausgestattet sind. Die Portale, Tools und Berichte sind identisch. Der einzige Unterschied liegt in den verfügbaren Funktionen, wie sie weiter oben dargestellt wurden.

Microsoft Defender für Unternehmen

Auf der Microsoft Ignite im Herbst 2022 kündigte Microsoft eine neue Version von Microsoft Defender an: *Microsoft Defender für Unternehmen*, die auf kleinere Organisationen mit bis zu 300 Benutzern ausgerichtet ist und gut zu Microsofts SMB-Angebot Microsoft 365 Business (Premium) passt. In gewisser Weise ähnelt Microsoft Defender für Unternehmen eher dem Microsoft Defender für Endpunkte Plan 2 als dem Plan 1. Schließlich sind die meisten Funktionen, die Plan 2 bietet, auch für die Business Edition verfügbar, wie in der folgenden Abbildung dargestellt.

Customer size	< 300 seats			> 300 seats		
	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Endpoint capabilities\SKU						
Centralized management	✓	✓	✓			
Simplified client configuration	✓					
Threat and Vulnerability Management	✓				✓	
Attack Surface Reduction	✓	✓	✓		✓	
Next-Gen Protection	✓	✓	✓		✓	
Endpoint Detection and Response	✓ ²				✓	
Automated Investigation and Response	✓ ²				✓	
Threat Hunting and 6-months data retention					✓	
Threat Analytics	✓ ²				✓	
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓		✓	
Microsoft Threat Experts					✓	
Partner APIs	✓	✓	✓		✓	
Microsoft 365 Lighthouse for viewing security incidents across customers	✓ ³					

Abbildung 7-3: Vergleich verschiedener Versionen von Defender für Endpunkte. Bild mit freundlicher Genehmigung von Microsoft.

Lange Zeit hatte Microsoft kein starkes Angebot für den SMB-Markt. Dieses neue Angebot ist eine willkommene Ergänzung zur bereits sehr leistungsfähigen Microsoft 365 Business Premium Suite und hilft kleineren Unternehmen dabei, ihre Sicherheitslage drastisch zu verbessern. Die neuen, vereinfachten Bereitstellungsoptionen machen die Implementierung auf jeden Fall zu einem Kinderspiel. Die neue Bereitstellungsoption (Verwaltungskanal) wird später in diesem Kapitel erläutert.

Es sollte erwähnt werden, dass Microsoft Defender für Unternehmen nicht die gleichen Funktionen wie seine Enterprise-Geschwister bietet. Eines der wichtigsten Elemente, das meiner bescheidenen Meinung nach fehlt, ist die Geräte-Timeline oder die Möglichkeit, erweiterte Suchen durchzuführen – beides Funktionen, die große Speichermengen erfordern. Es scheint, dass der Speicherplatz eines der Elemente ist, die weggelassen wurden, um den niedrigeren Preis zu ermöglichen.

Nicht für jeden: Einige Unternehmen, die für Microsoft Defender für Unternehmen infrage kommen, könnten trotzdem von einem Upgrade auf die Enterprise-Version profitieren. Die fehlenden Komponenten sind entscheidend für die Reaktion auf Vorfälle, und auf sie zu verzichten, kann mehr als nur ein Ärgernis sein.

Lizenzen mischen

Bis vor Kurzem war es nicht möglich, verschiedene SKUs für Microsoft Defender für Endpunkte in einem Mandanten zu mischen. Das ist immer noch der Fall, wenn du Microsoft Defender für Unternehmen nutzt; die verfügbaren Funktionen werden dann auf Microsoft Defender für Unternehmen zurückgesetzt – selbst wenn du eine „höhere“ Lizenz wie Microsoft Defender für Endpunkte Plan 1 oder Plan 2 zugewiesen hast.

Früher erhielten alle Geräte Plan 2-Funktionen, wenn du eine Mischung aus Plan 1- und Plan 2-Lizenzen hattest. Dieses Verhalten lässt sich nun ändern. Öffne dazu das Microsoft 365 Defender-Portal, navigiere zu **Einstellungen > Endpunkte > Lizenzen** und klicke auf **Abonnementeinstellungen verwalten**. Wähle die entsprechende Option aus und klicke auf **Fertig**.

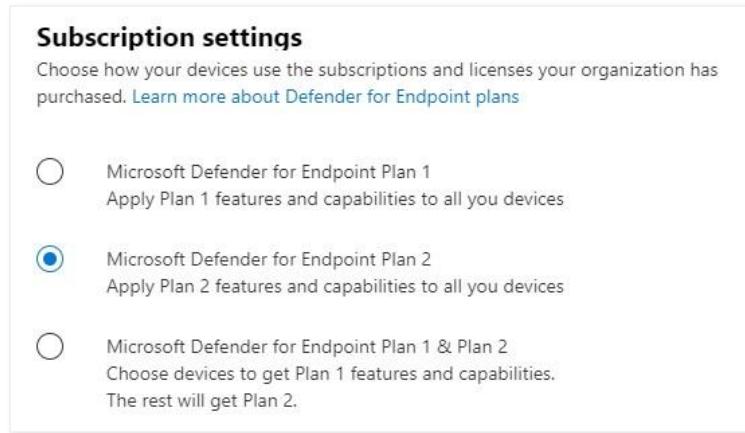


Abbildung 7-4: Mischen von Lizenzen in Microsoft Defender für Endpunkte

Um sicherzustellen, dass Geräte mit den richtigen Funktionen ausgestattet sind, musst du Geräte mit einem Tag namens **License MDE P1** versehen – für alle Geräte, die nur Microsoft Defender für Endpunkte Plan 1-Funktionen erhalten sollen.

Dieses Tag kannst du manuell oder über eine dynamische Regel vergeben, die du erstellen kannst, sobald du auf **Microsoft Defender für Endpunkte Plan 1 & Plan 2** klickst. Dynamische Regeln sind eine viel bessere und flexiblere Möglichkeit, einem Gerät Tags zuzuweisen. du kannst nicht nur mit UND/ODER-Operatoren arbeiten, sondern die Regel kann auch mehrere Eigenschaften nutzen – einschließlich des Gerätenamens, des Domänennamens, des Onboarding-Status, ob es internetfähig ist und so weiter. Du kannst sogar mehrere Gruppen mit UND/ODER-Operatoren kombinieren, wie in der folgenden Abbildung dargestellt.



Abbildung 7-5: Erstellung einer dynamischen Regel für die Tag-Zuweisung

Registrierungsschlüssel! Wenn du das Tag '**License MDE P1**' nur über die Registrierung zuweisen, wird die Änderung von der Plattform nicht erkannt. Stattdessen solltest du eine dynamische Regel erstellen, die sich auf das Tag bezieht, das du der Registrierung hinzugefügt hast. Manuelle Tags funktionieren hingegen einwandfrei.

Datenspeicherung und Standort

Basierend auf der Microsoft Azure Cloud hat jeder Kunde eine dedizierte Microsoft Defender für Endpunkte-Instanz, die von anderen Kunden getrennt ist. Das bedeutet, dass die Daten der Kunden innerhalb ihrer Mandanten isoliert und gesichert sind. Auf diese Daten kann nur über die Microsoft Entra ID-Authentifizierung zugegriffen werden, und der Zugriff wird überwacht. Microsoft Defender für Endpunkte-Daten werden maximal sechs Monate (180 Tage) aufbewahrt. Das ist äußerst hilfreich, wenn du einen Angriff untersuchen möchtest, der vor Monaten stattgefunden hat.

Aufbewahrungsduer: Nicht alle Informationen sind sechs Monate lang verfügbar. So sind beispielsweise Daten für die erweiterte Suche nur bis zu dreißig Tage zugänglich. Die Timeline eines Geräts kann dagegen bis zu sechs Monate zurückreichen.

Datenisolierung

Die Daten der verschiedenen Kunden sind logisch getrennt und mit einer separaten Authentifizierung geschützt, um auf die Informationen zuzugreifen. Die Daten selbst werden in einem der Microsoft Azure-Rechenzentren in der Europäischen Union, dem Vereinigten Königreich oder den Vereinigten Staaten gespeichert. Beachte, dass du den Speicherort deiner Daten nach der Konfiguration nicht mehr ändern kannst.

Datenspeicherung: Beachte außerdem, dass einige Daten möglicherweise in den Vereinigten Staaten verarbeitet werden - wenn auch in pseudonymisierter (verschleierter) Form.

Alle in der Cloud gespeicherten Daten sind mit mindestens 256-Bit verschlüsselt – sowohl im Ruhezustand als auch während der Übertragung.

Warum werden Daten in der Cloud gespeichert?

Wie du mittlerweile weißt, verlässt sich Microsoft Defender für Endpunkte auf die Leistungsfähigkeit der Cloud, um dir maximalen Schutz zu bieten. Dafür müssen Sicherheitsereignisse und Cyber-Telemetriedaten aus verschiedenen Gründen gespeichert werden:

- Zur Identifizierung von Anzeichen für einen Angriff (Indicators of Attack, IOAs) - auch als Bedrohungssindikatoren (Threat Indicators, TIs) bezeichnet - in deinem Unternehmen.
- Zum Auslösen von Warnungen, wenn Angriffe in deinem Unternehmen stattfinden.
- Damit das Microsoft Defender-Portal verschiedene Ansichten für verschiedene Entitäten wie Computer, Dateien und mehr anzeigen kann. Dies ermöglicht auch die Untersuchungs-Engine, mit der das Vorhandensein von Sicherheitsbedrohungen in deinem Unternehmen erforscht werden kann.
- Um die Möglichkeiten der erweiterten Suche in Microsoft Defender für Endpunkte zu unterstützen.

Datenschutz: Beim Bereitstellen von Defender für Endpunkte solltest du auch an den Datenschutz deiner Benutzer denken. Je nachdem, wo du lebst, gibt es möglicherweise gesetzliche Vorschriften, die dich verpflichten, deine Benutzer darüber zu informieren, dass Aktivitäten von ihren Endpunkten überwacht werden. Das gilt insbesondere, weil die erfassten Informationen weit über Dateinamen oder Prozessnamen hinausgehen. Sie beinhalten auch besuchte Websites, Zeitpunkte von Aktivitäten, geografische Daten und mehr. Auch wenn es gute Gründe für diese Datenerhebung gibt, solltest du den rechtlichen Rahmen im Blick behalten!

Konfiguration von Microsoft Defender für Endpunkte (Plattform)

In diesem Abschnitt geht es um die Konfigurationsoptionen für die Plattform selbst – nicht um die Gerätekonfiguration. Letztere wird in den nächsten Abschnitten behandelt.

Um auf die Einstellungen für Microsoft Defender für Endpunkte zuzugreifen, öffne das Microsoft 365 Security Center. Navigiere im linken Menü zu **Einstellungen** und klicke dort auf **Endpunkte**, um die spezifischen Konfigurationsmöglichkeiten anzuzeigen.

Zugriffsverwaltung für Defender für Endpunkte

Standardmäßig haben mehrere Rollen Zugriff auf das Microsoft 365 Security Center – und damit auch vollen Zugriff auf Microsoft Defender für Endpunkte. Das gilt für globale Administratoren, Sicherheitsadministratoren und in gewissem Umfang auch für Sicherheitsleser. In manchen Fällen möchtest du jedoch einen differenzierteren Ansatz wählen – etwa um Rechte zu beschränken oder regionale Anforderungen zu erfüllen.

Standardzugriff: Sobald du benutzerdefinierte Rollen erstellst, verlieren einige der integrierten Rollen ihren Standardzugriff und müssen gezielt einer benutzerdefinierten Rollen zugewiesen werden. Das betrifft zum Beispiel Mitglieder der Rolle "Sicherheitsleser".

Benutzerdefinierte Rollen erstellen

Der Zugriff auf Microsoft Defender für Endpunkte lässt sich durch benutzerdefinierte Rollen gezielt steuern. Diese Rollen definieren, welchen Zugriff jemand innerhalb der Plattform erhält. Du kannst sie auch verwenden, um den Zugriff auf bestimmte Gerätetypen zu beschränken – zum Beispiel so, dass nur Mitglieder bestimmter Entra ID-Gruppen Zugriff auf bestimmte Geräte erhalten.

Um eine benutzerdefinierte Rolle zu erstellen, gehe zu **Einstellungen** und klicke unter **Berechtigungen** auf **Rollen**. Wähle dann **Element hinzufügen**, um den Assistenten zu starten. Rechts erscheint ein Bereich mit zwei Registerkarten:

- **Allgemein:** Hier gibst du der Rolle einen Namen und eine Beschreibung und legst fest, welche Berechtigungen sie erhalten soll. Eine Übersicht der verfügbaren Berechtigungen findest du in der Abbildung 7-6 unten.
- **Zugewiesene Benutzergruppen:** Hier definierst du, welche Entra ID-Gruppen Zugriff auf die Rollen erhalten. Wichtig: Die Entra ID-Gruppen müssen bereits erstellt sein, bevor du

die Rolle anlegt. Es kann auch einen Moment dauern, bis eine neu erstelle Gruppe im Portal sichtbar ist.

Im Beispiel der Abbildung erstellen wir eine Rolle für den täglichen Sicherheitsbetrieb. Da sich das Security Operations Team nur um die Bearbeitung von Warnungen kümmert – nicht aber um die Konfiguration oder das Patchen – erhält diese Rolle nur Zugriff auf Informationen über Geräte und Benutzer, auf Warnungen und Vorfälle sowie auf Live-Response-Funktionen. Damit kann das Team bei Untersuchungen per Fernzugriff auf betroffene Geräte zugreifen.

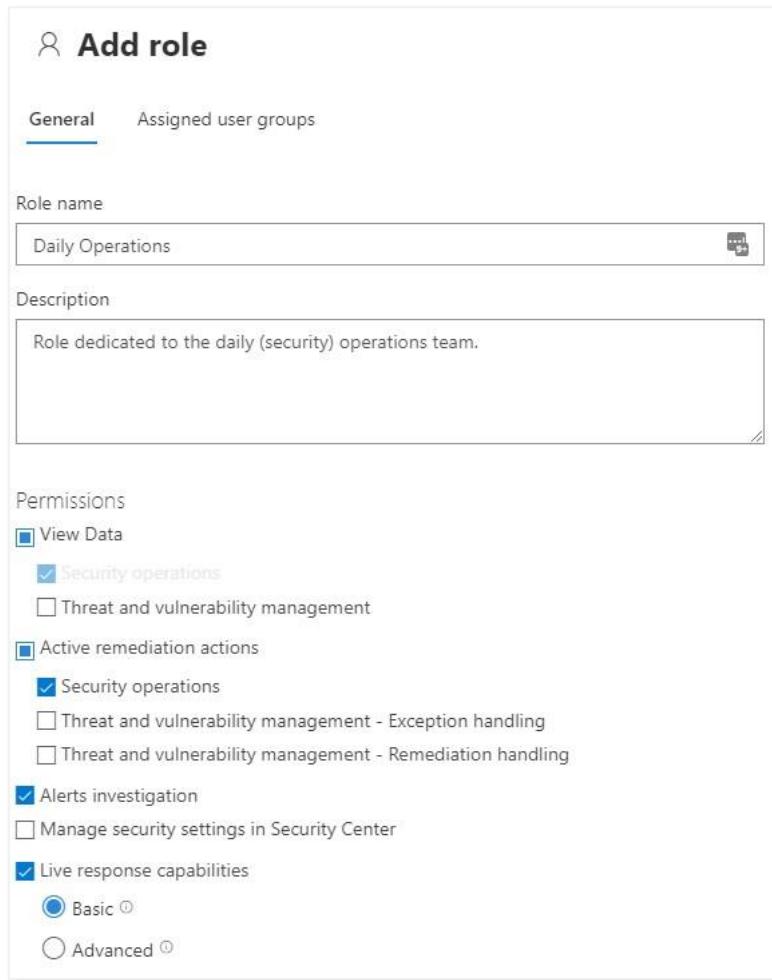


Abbildung 7-6: Erstellen einer benutzerdefinierten Rolle

Gerätegruppen & Tags

Standardmäßig haben alle Benutzer, die über Berechtigungen für den Zugriff auf Defender für Endpunkte verfügen, Zugriff auf alle integrierten Geräte. In der Regel ist das kein Problem. Einige Unternehmen sind jedoch geografisch verteilt und müssen möglicherweise die

Verwaltung von Geräten in einer Region von einer anderen trennen. Ähnlich wie du einige Geräte auf eine andere Weise konfigurieren möchtest, möchtest du vielleicht auch, dass eine bestimmte Gruppe von Geräten eine andere Auto-Remediation-Stufe hat als andere. Beide Ziele kannst du mit Gerätegruppen erreichen.

Gerätegruppen sind nichts anderes als eine logische Gruppierung von Geräten. Eine Gerätegruppe kann auf der Grundlage eines der folgenden (Geräte-)Attribute erstellt werden:

- **Name:** Du kannst den Namen eines Geräts verwenden, um Geräte zu gruppieren. Wenn du beispielsweise ein Benennungsschema hast, bei dem alle europäischen Geräte mit "EU-" beginnen, kannst du eine Gerätegruppe definieren, bei der der Operator "Beginnt mit" lautet und der Wert auf "EU-" gesetzt ist.
- **Domäne:** Verwende den (lokalen) Domänennamen, um Geräte zu gruppieren. Dies ist nur sinnvoll, wenn du mehrere Domänen hast oder zwischen domänenverbundenen und nicht domänenverbundenen Geräten unterscheiden möchtest.
- **Tag:** Wie gleich besprochen wird, kannst Tags verwendet werden, um einem Gerät ein benutzerdefiniertes Tag hinzuzufügen. Dieses Tag, das manuell, über das Portal, über einen Registrierungsschlüssel oder die Defender-API konfiguriert werden kann, ist auch für Defender für Endpunkte verfügbar. Da benutzerdefinierte Tags jeden Wert enthalten können, kannst du viel granularer sein als auf der Grundlage der anderen Attribute.
- **Betriebssystem:** Unterscheide zwischen verschiedenen Betriebssystemen, die du aus einer Dropdown-Liste auswählen kannst. Werte sind unter anderem, aber nicht beschränkt auf: Windows 10, Windows 8.1, Windows 7, Windows Server 2019, Windows Server 2016 und so weiter.

Standardgerätegruppe: Wenn du keine Gerätegruppe erstellst oder ein Gerät keiner Gerätegruppe zugeordnet werden kann, wird es in die standardmäßige Gerätegruppe mit dem Namen *Nicht gruppierte Geräte* eingeordnet. Du kannst an dieser Gerätegruppe keine Änderungen vornehmen, d. h. du kannst weder den Namen ändern noch eine andere Entra ID-Gruppe zuweisen oder die Remediation-Stufe steuern.

Um eine neue Gerätegruppe zu erstellen, klickst du auf der Einstellungsseite unter **Berechtigungen** auf **Gerätegruppen**. Klicke dort auf **Gerätegruppe hinzufügen**. Wie bei der Erstellung einer neuen Rolle erscheint auch hier eine Folie auf der rechten Seite des Bildschirms, die vier Registerkarten enthält:

- **Allgemein:** Hier gibst du den Namen, die Beschreibung und die Automatisierungsstufe der Gruppe an. Die Remediationsstufen werden im Abschnitt Automated Investigation & Response ausführlicher besprochen.
- Unter **Geräte** definierst du die Regeln, die ein Gerät erfüllen muss, um in die Gerätegruppe aufgenommen zu werden.
- **Geräte in der Vorschau** ermöglichen es dir, zu überprüfen, ob die von dir erstellten Regeln deinen Erwartungen entsprechen, indem du eine Liste (von bis zu 10 Geräten) abrufst, die in die Gerätegruppe aufgenommen würden.

- Unter **Benutzerzugriff** kannst du auswählen, welche Entra ID-Gruppen Zugriff auf diese Gerätegruppe haben. Beachte, dass du nur Entra ID-Gruppen auswählen kannst, die einer benutzerdefinierten Rolle zugewiesen wurden.

Zugriffsebene: Die Zugriffsebene, die eine ausgewählte Entra ID-Gruppe auf die Gerätegruppe hat, wird durch die benutzerdefinierte Rolle definiert. Wenn die benutzerdefinierte Rolle beispielsweise definiert, dass die Entra ID-Gruppe nur MDVM-Daten anzeigen kann, kannst du nur die MDVM-Daten für die Gerätegruppe sehen, der sie zugewiesen wurden.

Wie bereits erwähnt, benötigst du manchmal etwas mehr Flexibilität, um Gerätegruppen zu erstellen, als der Name, die Gruppenmitgliedschaft oder die Betriebssystemversion eines Geräts bietet. Hierfür kannst du Geräten ein benutzerdefiniertes Tag hinzufügen. Es gibt verschiedene Möglichkeiten, einem Gerät ein Tag zuzuweisen:

- Über das Microsoft 365 Security Center
- Festlegen eines Registrierungsschlüssels auf dem Gerät selbst
- Verwendung der Microsoft Defender für Endpunkte-API

Um ein Tag über das Portal zuzuweisen, navigierst du zu **Gerätebestand**, wählst ein Gerät aus der Liste aus und klickst dann im Menü auf der rechten Seite des Bildschirms auf **Tags verwalten**. Wähle dort entweder bereits vorhandene Tags aus oder klicke auf **(Neu erstellen)**, um ein neues Tag zu erstellen.



Abbildung 7-7: Zuweisen eines Tags zu einem Gerät über das Portal

Alternativ kannst du auch einen bestimmten Registrierungsschlüssel auf dem Gerät setzen. Das kann auf viele verschiedene Arten erfolgen, zum Beispiel über Microsoft Intune. Die Details des Registrierungsschlüssels sind:

- Registrierungsschlüssel:** HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection\DeviceTagging\
- Registrierungsschlüsselwert (REG_SZ):** Group
- Registrierungsschlüsseldaten:** Name des Tags, den du setzen möchtest.

Schließlich kannst du auch die Microsoft Defender API nutzen. Der genaue Prozess wird [hier](#) erläutert. Du kannst die API über PowerShell oder dein bevorzugtes Automatisierungstool wie Azure Logic Apps oder Microsoft Power Automate ansprechen. Ein anschauliches Beispiel, wie du eine solche Automatisierung aufbaust, findest du in [diesem Artikel](#) von Thijs Lecomte.

Sobald Geräte mit einem Tag versehen sind, werden sie der entsprechenden Gerätgruppe automatisch zugeordnet. Du kannst aber auch eigene Gerätetypen erstellen, um die angezeigten Informationen auf dem Bildschirm einzuschränken. Klicke dazu auf der Seite **Gerätebestand** auf **Filter** und scroll dann zum passenden Abschnitt, wie in der folgenden Abbildung dargestellt.

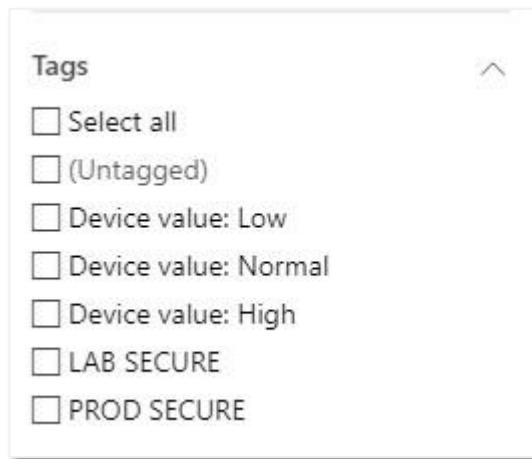


Abbildung 7-8: Zuweisen eines Tags zu einem Gerät über das Portal

Mehr als nur Gerät-Gruppierung: Gerätetypen dienen mehrere Zwecke in Defender für Endpunkte. Sie erscheinen auch auf der Entitätsseite des jeweiligen Geräts. So kannst du gezielt Suchabfragen verfeinern oder dein Betriebsteam auf bestimmte Geräte aufmerksam machen, indem ihr einheitliche Tags verwendet.

Grundkonfiguration

Auch wenn es auf der Microsoft Defender für Endpunkte-Plattform insgesamt nur wenige Konfigurationspunkte gibt, solltest du einige zentrale Einstellungen im Blick behalten. Diese findest du im Microsoft 365 Security Center unter **Einstellungen > Endpunkte**:

- **Datenaufbewahrung:** Hier siehst du, in welcher Region deine Instanz erstellt wurde und kannst einstellen, wie lange die Daten aufbewahrt werden. Standardmäßig sind es 180 Tage. Beachte, dass sich diese Frist auf Informationen innerhalb der Gerätetimeline bezieht. Jagddaten sind z. B. nur 30 Tage lang zugänglich und lassen sich nicht anpassen.
- **E-Mail-Benachrichtigungen:** Damit steuerst du, wer welche Art von Benachrichtigungen erhält. Du kannst beispielsweise einstellen, dass Warnmeldungen an eine bestimmte E-

Mail-Adresse gehen, während Benachrichtigungen zum Bedrohungs- und Schwachstellenmanagement an eine andere gesendet werden. Innerhalb der Konfiguration kannst du sogar spezifisch eine Adresse für eine bestimmte Gerätegruppe oder einen bestimmten Schweregrad von Warnungen definieren.

- **Auto Remediation-Einstellungen:** Hier legst du fest, wie Defender für Endpunkte auf Warnungen reagiert – abhängig von den zugewiesenen Gerätegruppen. Du kannst damit steuern, ob Bedrohungen automatisch behoben werden oder nicht. Wie du später sehen wirst, bieten Gerätegruppen die notwendige Flexibilität und Granularität. So möchtest du zum Beispiel möglicherweise nicht, dass Defender automatisch Maßnahmen auf einem produktiven Gerät durchführt, wohl aber auf einem regulären Office-Client.
- **Erweiterte Funktionen:** Auf dieser Seite verwaltet du verschiedene globale Einstellungen, darunter Integrationen mit anderen Plattformen und Funktionen, die aktiviert oder deaktiviert sein können. In der Regel gibt es wenig Grund, diese Optionen zu deaktivieren – es sei denn, du erfüllst bestimmte Voraussetzungen nicht oder unterliegst speziellen rechtlichen Vorgaben, die dich an der Nutzung hindern. Gegebenenfalls werden Details zu den Einstellungen in den entsprechenden Abschnitten später in diesem Kapitel erläutert.

Automatisierte Uploads

In diesem Abschnitt steuerst du außerdem, ob die **Speicher- und Dateiinhaltsanalyse** aktiviert sein soll. Sobald eine automatisierte Untersuchung gestartet wird, kann Defender sowohl relevante Dateien als auch die Speicherinhalte analysieren, die mit den untersuchten Prozessen verknüpft sind. Ist die Option aktiviert, werden die betroffenen Inhalte in den Cloud-Dienst hochgeladen, um sie genauer auszuwerten.

Beide Funktionen – die Analyse von Dateien und Speicherinhalten – sind sehr wertvoll und sollten in der Regel aktiviert bleiben. Der einzige nachvollziehbare Grund, sie zu deaktivieren, sind spezifische gesetzliche Vorgaben, die es dir untersagen, solche Informationen an Microsoft zu senden. Dabei ist wichtig zu wissen: Zwar könnten theoretisch sensible Inhalte sichtbar werden, sie sind jedoch ausschließlich den maschinellen Lernsystemen und automatisierten Inhaltsanalysen zugänglich. Kein Mensch wertet diese Daten manuell aus.

Integration mit anderen Microsoft 365-Diensten

Microsoft Defender für Office 365

Diese Funktion ermöglicht die Integration zwischen Microsoft Defender für Office 365 und Microsoft Defender für Endpunkte. Dabei werden Informationen aus beiden Plattformen geteilt, um die Untersuchungserfahrung zu verbessern, indem Warnungen und Vorfälle aus Defender für Office 365 mit Informationen aus Microsoft Defender für Endpunkte angereichert werden.

Die Integration musst du an beiden Enden konfigurieren. Wie du dies für Defender für Office 365 machst, wurde in Kapitel 5 besprochen. Um die Integration von Microsoft Defender für Endpunkte aus zu aktivieren, navigierst du zu **Einstellungen > Endpunkte > Erweiterte Funktionen**. Suche in der Liste die Option **Office 365 Threat Intelligence-Verbindung** und aktiviere oder deaktiviere die Funktion.

Microsoft Defender für Cloud-Apps

Die Integration mit Cloud App Security ist sowohl entscheidend als auch extrem nützlich. Wenn sie aktiviert ist, leitet Microsoft Defender für Endpunkte seine Telemetriedaten an Cloud App Security weiter, das wiederum die Informationen analysieren kann, um die Nutzung von Cloud-Anwendungen zu erkennen. Die Integration und wie du sie aktivierst, wird ausführlicher in Kapitel 8 beschrieben.

Microsoft Intune

Abgesehen von der offensichtlichen Integration zwischen Microsoft Intune und Defender für Endpunkte zur Bereitstellung des Sensors und zur Verwaltung von Sicherheitsrichtlinien können Informationen von Microsoft Defender für Endpunkte mit Intune geteilt werden. Diese Informationen können dann verwendet werden, um den Compliance-Status eines Geräts zu bestimmen. Der Gerätestatus kann wiederum in anderen Funktionen wie bedingten Zugriffsrichtlinien genutzt werden.

Um die Integration zu aktivieren, navigierst du zu **Einstellungen > Endpunkte > Erweiterte Funktionen**. Suche in der Liste der Funktionen nach **Microsoft Intune-Verbindung** und aktiviere oder deaktiviere die Funktion.

Verwaltung von Microsoft Defender für Endpunkte (Endpunkte)

Bevor wir fortfahren und um die folgenden Inhalte besser zu verstehen, lass uns eine Unterscheidung zwischen verschiedenen Arten von administrativen Aktivitäten in Bezug auf Microsoft Defender für Endpunkte treffen. Die Konfiguration der Plattform und die globalen Einstellungen wurden bereits im vorherigen Abschnitt behandelt.

- **Bereitstellung** bezieht sich auf die Aktivierung der Microsoft Defender für Endpunkte-Dienste oder die Bereitstellung der Binärdateien auf einem Gerät, um sicherzustellen, dass Informationen erfasst und an die richtige Instanz gesendet werden.
- **Client-Konfiguration** und **Richtlinienverwaltung** stellen sicher, dass die richtigen Einstellungen für verschiedene Aspekte von Microsoft Defender für Endpunkte korrekt

konfiguriert sind. Dazu gehören unter anderem Antiviren-Einstellungen und Attack Surface Reduction-Regeln. Heute kannst du diese Einstellungen auf vielfältige Weise verwalten, zum Beispiel über Gruppenrichtlinien, PowerShell, Microsoft Intune, Microsoft Configuration Manager, Tools von Drittanbietern wie Jamf für macOS oder Ansible/Puppet für Linux - und inzwischen auch direkt über Microsoft Defender für Endpunkte.

- **Tägliche Abläufe** wie das Untersuchen und Reagieren auf Vorfälle und Warnungen, das Überprüfen von Integritätsproblemen, die Fehlerbehebung bei Leistungsproblemen am Client und letztendlich das Offboarding von Geräten, die nicht mehr verwendet werden.

Bereitstellung (Onboarding)

In diesem Abschnitt geht es um die verschiedenen Bereitstellungsaktivitäten – auch Onboarding genannt –, bei denen Geräte für Microsoft Defender für Endpunkte aktiviert werden. Wie dieser Prozess aussieht, hängt stark vom Typ des Betriebssystems und der Art der Integration ab: manuell oder über das Konfigurationsverwaltungstool deiner Wahl.

Anforderungen

Wie bei jeder anderen Anwendung, die du in Deinem Netzwerk einfürst, gibt es ein paar Voraussetzungen, die du erfüllen musst, bevor du Defender für Endpunkte bereitstellen kannst. Im Folgenden findest du eine allgemeine Übersicht über diese Anforderungen. Da sich diese im Laufe der Zeit ändern können, solltest du immer auch die aktuelle Microsoft-Dokumentation konsultieren.

Unterstützte Plattformen

Zum Zeitpunkt des Schreibens wird Defender für Endpunkte auf einer Vielzahl von Betriebssystemen unterstützt. Eine vollständigere und aktuellere Version dieser Liste findest du [hier](#):

- Windows (7, 8.1, 10, 11)
- Windows Server (2012 R2, 2016, 2019, 2022)
- macOS
- iOS 11.0 und höher
- Android 6.0 und höher
- Linux (spezifische Versionen)

Keine Funktionsparität: Es ist wichtig zu verstehen, dass nicht alle Funktionen auf allen Plattformen verfügbar sind. Der volle Funktionsumfang unter Windows 10 und Windows Server 2019 verfügbar. Von dort an nimmt er jedoch ab – abhängig von der verwendeten Version des Betriebssystems. Beispielsweise fehlen die Funktionen zur Verhinderung von Datenverlust und

Live-Reaktion sowohl unter macOS als auch unter Linux. Den Überblick über die Funktionen jeBetriebssysteme zu behalten, kann sehr aufwendig sein. Glücklicherweise hat sich Fellow-MVP Ru Campbell die Mühe gemacht und pflegt eine solche Liste [hier](#). Sehr zu empfehlen!

Auch die Art und Weise, wie du Defender für Endpunkte bereitstellst, unterscheidet sich je nach Betriebssystem. Weitere Details dazu findest du im Abschnitt „*Verwaltungsplattformen und Onboarding*“ in diesem Kapitel.

Mindestanforderungen an Geräte

Im Allgemeinen kannst du auf jedem Gerät, auf dem Windows 10 läuft, auch Defender für Endpunkte ausführen. Einige Funktionen, wie zum Beispiel Defender Application Guard, haben jedoch zusätzliche Anforderungen, hauptsächlich weil sie spezielle Hardware-Abhängigkeiten haben. Um Defender Application Guard zu unterstützen, muss ein Gerät 64-Bit-fähig sein (was heutzutage ohnehin Standard ist) und CPU-Virtualisierungserweiterungen unterstützen: SLAT (Second Level Address Translation) und VT-x oder AMD-V.

Netzwerkverbindung

Um Telemetriedaten in den Cloud-Dienst hochzuladen, muss der Sensor auf deinem Gerät in der Lage sein, eine Verbindung zum Cloud-Dienst deiner Defender für Endpunkte-Instanz herzustellen. Die von den Diensten verwendeten URLs sind [hier](#) dokumentiert.

Vorsicht bei Proxy-Servern: Die Verbindung zu diesen Endpunkten kann entweder direkt (über das Internet) oder über einen Proxyserver erfolgen. Im letzteren Fall ist es wichtig zu verstehen, dass die Verbindung im Gerätekontext und nicht des Benutzerkontext hergestellt wird. Wenn dein Proxy-Server also eine Authentifizierung erfordert, stelle sicher, dass er den Geräteauthentifizierungskontext verarbeiten kann. Wenn nicht, sollte der Datenverkehr zum Cloud-Dienst nicht authentifiziert sein.

Überprüfung der Netzwerkverbindung

Microsoft stellt ein nützliches Skript zur Überprüfung der Installation von Microsoft Defender für Endpunkte und der Netzwerkverbindung zum Cloud-Dienst zur Verfügung. Das [Skript](#), namens **MDEClientAnalyzer.cmd** verwendet PowerShell, um zu versuchen, eine Verbindung zu den verschiedenen URLs herzustellen, die es für den korrekten Betrieb benötigt.

Um das Skript auszuführen, führst du einfach den folgenden Befehl mit (lokalen) Administratorrechten aus:

```
[PS] C:\> .\MDEClientAnalyzer.cmd
```

Sobald das Skript erfolgreich abgeschlossen wurde, schreibt es die Ergebnisse in einen Protokollordner mit dem Namen **MDEClientAnalyzerResult**. Von dort aus kannst du die Testergebnisse genauer einsehen. Die Datei **MDEClientAnalyzer.html** im Stammverzeichnis bietet dir einen allgemeinen Überblick über die Testergebnisse, wie in der folgenden Abbildung dargestellt:

Check Results Summary					
		Error	Warning	Informational	
0	2	1			
Detailed Results					
Category	Severity	Id	Test Name	Results	Guidance
Connectivity	Warning		EDRCloud	EDR Cloud checks have not run successfully.	Ensure PsExec is not blocked in your environment and then try again. If you cannot allow PsExec to be run in your environment due to security reasons, then you can try log collection via Live Response as explained here: LiveAnalyzer
Connectivity	Warning		CertRevocation	Certificate revocation was not tested.	If the device is in 'Impaired communications' status, try manually running 'certutil.exe -verify -urlfetch winatp.cer' using PsExec -s, to ensure the revocation checks are working when executed in system context. Note that both PsExec.exe and winatp.cer files are inside available inside the 'Tools' directory of the analyzer.
Connectivity	Informational		AVCloud	Test connection to the Microsoft Defender Antivirus cloud service completed successfully.	N/A

Abbildung 7-9: Überprüfung der Ergebnisse des MDE Client Analyzers

Attack Surface Reduction: In der obigen Abbildung wirst du feststellen, dass einige Tests fehlgeschlagen sind. Das liegt daran, dass auf den Systemen, auf denen ich das Skript ausgeführt habe, Attack Surface Reduction-Regeln aktiv waren und einige der Tests blockiert haben, die das Skript auszuführen versuchte. Um die Tests erfolgreich durchzuführen, must du die ASR-Regel deaktivieren, die Prozesserstellungen von PSEXEC- und WMI-Befehlen blockiert.

Die Bedeutung der Netzwerkverbindung

Wie im vorherigen Abschnitt beschrieben, stützt sich ein Teil der Erkennung durch Microsoft Defender für Endpunkte auf die Fähigkeit, Signale (Telemetrie) in die Cloud-Plattform hochzuladen, damit sie dort auf verdächtiges Verhalten analysiert werden können. Wenn keine Verbindung verfügbar ist, greift Microsoft Defender für Endpunkte auf die Offline-Funktionen zurück, wie zum Beispiel den Next-Gen-Schutz von Microsoft Defender.

In der Zeit, in der ein Gerät offline ist, werden Telemetriedaten lokal auf dem Gerät zwischengespeichert. Sobald das Gerät wieder online ist, werden diese zwischengespeicherten Informationen zur Analyse an den Cloud-Dienst gesendet. Auf diese Weise können Aktivitäten immer noch korreliert werden, wenn auch nachträglich. Es versteht sich von selbst: Während EDR-Erkennungen in der Regel innerhalb von Sekunden bis Minuten erfolgen – was der Zeit entspricht, die für das Hochladen von Daten auf die Microsoft Defender-Plattform benötigt wird –, gibt es keine Erkennungen durch die Plattform, solange das Gerät offline ist. Für maximalen Schutz sollte ein Gerät möglichst immer online sein.

Leider wissen auch Angreifer, dass Konnektivität – oder deren Fehlen – ihnen helfen kann, Erkennungen zu umgehen, selbst wenn es nur für einen Moment ist. Betrachte Folgendes: Ein Angreifer schafft es irgendwie, erfolgreich Zugriff auf ein Gerät zu erlangen. Bevor er weitere Angriffe startet, versucht er, Firewall-Regeln zu erstellen, die den ausgehenden Zugriff auf die Microsoft Defender-Plattform blockieren. Auf diese Weise verhindert er, dass Prozesse mit der Online-Plattform kommunizieren, und blockiert so das Hochladen von Telemetriedaten. Dadurch neutralisiert er die erweiterten Erkennungen und erhöht die Chancen, unentdeckt zu bleiben. Durch maßgeschneiderte Firewall-Regeln kann ein Angreifer sicherstellen, dass nur Microsoft Defender für Endpunkte betroffen ist; andere ausgehende Verbindungen bleiben unbeeinträchtigt, sodass es für den Benutzer schwieriger ist, etwas Verdächtiges zu bemerken.

Wenn überhaupt, ist dieses Szenario ein gutes Beispiel dafür, warum eine Defense-in-Depth-Strategie notwendig ist. Und auch wenn Microsoft Defender für Endpunkte über Anti-Tamper-Schutzfunktionen verfügt, verhindert das nicht, dass Firewall-Regeln lokal aktualisiert werden. Glücklicherweise hat Microsoft eine Logik in Microsoft Defender Antivirus eingebaut, die solche Änderungen erkennt, eine Toast-Benachrichtigung ausgibt und eine Warnung in Microsoft Defender für Endpunkte auslöst.

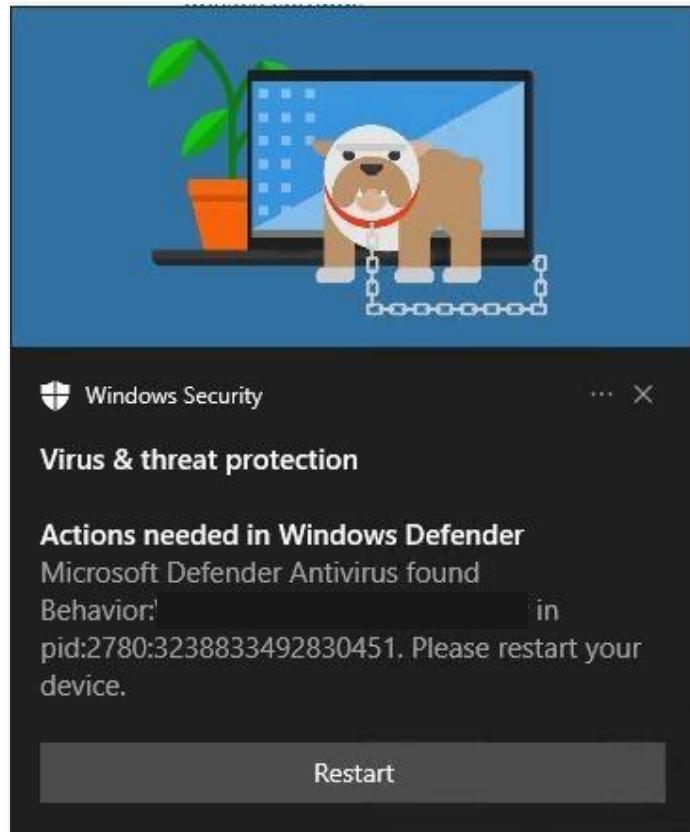


Abbildung 7-10: Toast-Benachrichtigung bei Manipulation der Firewall-Regeln

Beachte den Hinweis zum Neustart des Computers: Damit Defender die Firewall-Änderungen „beheben“ kann, musst du die Maschine neu starten. Wenn du das aufgrund des Toasts noch nicht getan hast, wäre es ratsam, dies ebenfalls zu überprüfen – nur um sicherzugehen.

Wie in der Abbildung unten gezeigt, wird im Microsoft 365 Security Center eine Warnung mit dem Namen „BlockMsav“-Malware wurde verhindert ausgelöst. Leider liefert die Warnung nicht viel Kontext darüber, warum sie ausgelöst wurde. Glücklicherweise findest du zusammen mit der Warnung einen Vorfall, wie unten dargestellt:

✓	Incident name	Severity	Investigation state	Categories
▼	Suspicious 'WDBlockFirewallRule' behavior was blocked on one endpoint	Low	Unsupported alert type	Suspicious activity
	Suspicious 'WDBlockFirewallRule' behavior was blocked	Low	Unsupported alert type	Suspicious activity

Abbildung 7-11: Firewall-Manipulations-Vorfall im Microsoft 365 Security Center.

Die Art und Weise, wie Microsoft Defender für Endpunkte über Offline-Geräte berichtet, macht die Sache nicht einfacher – zumindest nicht, wenn es darum geht, zwischen Geräten zu

unterscheiden, die legitim offline sind, und solchen, an denen manipuliert wurde. Wenn ein Gerät sieben aufeinanderfolgende Tage offline war, ändert sich sein Status im Portal von aktiv in inaktiv – unabhängig davon, ob dies daran lag, dass das Gerät ausgeschaltet war oder einfach nicht mehr gemeldet hat, weil Firewall-Regeln die Aktivität blockiert haben.

Eine Möglichkeit, zu verhindern, dass Angreifer die lokale Firewall missbrauchen, um zu verhindern, dass Microsoft Defender mit der Cloud-Plattform kommuniziert, besteht darin, die Erstellung von (lokalen) Firewall-Regeln zu überwachen. Wenn eine Änderung an der lokalen Firewall vorgenommen wird, wird im Ereignisprotokoll „Microsoft-Windows-Windows Firewall With Advanced Security“ ein Ereignis 2004 eingetragen:



Abbildung 7-12: Anzeige der Erstellung einer Firewall-Regel im Ereignisprotokoll

Es gibt verschiedene Möglichkeiten, wie du diese Informationen sammeln kannst, von denen einige in diesem Buch beschrieben werden. Du könntest beispielsweise die Windows-Ereignisprotokollweiterleitung verwenden, um diese Ereignisse aus der Ferne zu sammeln und eine Warnung auszugeben, wenn eine Änderung der Firewall-Regel erkannt wird – insbesondere, wenn eine davon die Blockierung von Prozessen im Zusammenhang mit Microsoft Defender für Endpunkte betrifft. Eine andere Möglichkeit wäre die Verwendung des Microsoft Monitoring Agent, um bestimmte Ereignisprotokollspeicherorte zu erfassen und an einen Azure Log Analytics-Arbeitsbereich zu senden, wo diese Ereignisse analysiert werden können. Dies könnte sehr gut der Arbeitsbereich sein, der mit deiner Microsoft Sentinel-Instanz verbunden ist, die in Kapitel 11 ausführlicher besprochen wird.

Schließlich könntest du, wenn du eine Geräteverwaltungslösung wie Microsoft Intune verwendest, das letzte Check-in-Datum des Geräts nutzen, um festzustellen, ob ein Gerät online war und mit Intune, aber nicht mit Microsoft Defender für Endpunkte verbunden war. Das Problem bei diesem Ansatz ist, dass Geräte nur gelegentlich (standardmäßig alle acht Stunden) bei Microsoft Intune einchecken, und du bei Verwendung dieser Methode somit mehrere Stunden zurückliegen kannst. Außerdem ist ein Gerät, das bei Microsoft Intune, aber nicht bei Microsoft Defender für Endpunkte eincheckt, nicht unbedingt kompromittiert. Eine Diskrepanz könnte lediglich eine weitere Untersuchung auslösen, um herauszufinden, ob etwas nicht stimmt. Allerdings ist keine dieser Methoden zu 100 Prozent sicher: Wenn ein Angreifer Firewall-Regeln hinzufügen kann, um den Datenverkehr von Microsoft Defender für Endpunkte zu blockieren – was hindert ihn dann daran, dasselbe für zum Beispiel den Verwaltungskanal, die Ereignisprotokollweiterleitung usw. zu tun...?

Luftdicht abgeschottete Netzwerke: Bei einigen Geräten ist eine direkte Verbindung zum Internet nicht immer möglich oder erlaubt. Auch wenn keine direkte Internetverbindung verfügbar ist, kann Microsoft Defender für Endpunkte zusätzlichen Schutz bieten, da die meisten Funktionen auch ohne Zugriff auf die Cloud funktionieren können - allerdings mit Einschränkungen. Weitere Informationen zum Umgang mit solchen Szenarien findest du in [diesem Whitepaper](#).

Onboarding von Windows 10/11-Endpunkten

Für diesen Abschnitt gehen wir davon aus, dass die Geräte, die mit Microsoft Defender für Endpunkte integriert werden sollen, bereits bei Microsoft Intune registriert wurden.

Das Onboarding von Geräten wird durch die EDR-Richtlinie gesteuert, die du findest, wenn du zum Microsoft **Endpoint Manager-Portal** navigierst > **Endpoint Security** > **Endpoint detection and response**. Klicke dort auf „**Richtlinie erstellen**“.

Wähle im Assistenten „**Windows 10 und höher**“ als Plattform und „**Endpoint Detection and Response**“ als Profiltyp. Klicke dann auf „**Erstellen**“. Gib auf der ersten Registerkarte (Grundlagen) einen Namen und eine Beschreibung für die Richtlinie ein und klicke auf „**Weiter**“.

Die Richtlinie selbst verfügt nicht über viele Konfigurationsoptionen:

- **Beispelfreigabe für alle Dateien** steuert, ob Dateien zur weiteren Analyse an Microsoft gesendet werden können. Das ähnelt der Cloud-Schutzfunktion von Microsoft Defender Antivirus.
- **Beschleunigte Telemetrie-Berichtsfrequenz** erhöht die Häufigkeit, mit der der Sensor mit dem Cloud-Dienst kommuniziert.

Sobald du diese Einstellungen konfiguriert hast, gehst du durch die restlichen Schritte des Assistenten, um den Geltungsbereich der Richtlinie festzulegen. Sobald du die Richtlinie erstellt

hast, werden deine Geräte langsam im Security Center unter **Gerätebestand** angezeigt. Beachte, dass der Integritätsstatus „**Aktiv**“ und der Onboarding-Status „**Onboarded**“ lauten sollte – wie in der folgenden Abbildung dargestellt:

Device name	Domain	OS platform	Health state	Onboarding status	Last device update ⓘ
desktop-ld81acl		Windows 10	Active	Onboarded	8/8/2021, 12:36 AM

Abbildung 7-13: Übersicht der onboarded Geräte

Onboarding- oder Sensorintegritätsprobleme

Es scheint fast unrealistisch, aber das Onboarding von Geräten in Defender für Endpunkte ist wirklich so einfach. Natürlich gibt es eine Fülle anderer Elemente, wie zum Beispiel das Fehlen einer ordnungsgemäßen Konnektivität, die dir einen Strich durch die Onboarding-Erfahrung machen könnten. Wenn ein Gerät erfolgreich integriert wurde, aber nicht ordnungsgemäß mit dem Defender für Endpunkte-Dienst kommunizieren kann, siehst du möglicherweise verschiedene *Integritätszustände*, darunter:

- **Keine Sensordaten** bezieht sich auf ein Gerät, das erfolgreich integriert wurde, Zugriff auf den Cloud-Dienst hat, aber keine oder nur unvollständige Informationen sendet. Meist liegt das daran, dass der Windows 10-Diagnosedatendienst auf dem Gerät nicht läuft, weil er z. B. durch eine andere Richtlinie deaktiviert wurde. Ein weiteres Problem ist, dass nur Teile der Endpunkte, auf die zugegriffen werden soll, vom Gerät aus erreichbar sind.
- **Beeinträchtigte Kommunikation** weist auf ein Konnektivitätsproblem hin. Das bedeutet, dass ein Gerät zuvor möglicherweise ordnungsgemäß mit dem Cloud-Dienst kommuniziert hat, dies aber aus irgendeinem Grund nicht mehr tut. Wenn ein Gerät über einen Zeitraum von sieben aufeinanderfolgenden Tagen nicht mit dem Cloud-Dienst kommuniziert, wird es als *Inaktiv* markiert.
- **Inaktiv** wird für alle Geräte verwendet, die in den letzten sieben Tagen nicht beim Cloud-Dienst eingecheckt haben. Dafür kann es mehrere Gründe geben: Ein Gerät ist möglicherweise für einen längeren Zeitraum vom Internet getrennt, aber es könnte auch neu installiert, umbenannt oder außer Betrieb genommen worden sein, ohne ordnungsgemäß aus dem Dienst ausgebucht zu werden.

Windows 10 versions	Health state ↓	Onboarding status
1909	No sensor data, impaired communi...	Onboarded
1909	Impaired communications	Onboarded
1909	Impaired communications	Onboarded
1909	Impaired communications	Onboarded
1909	Inactive	Onboarded

Abbildung 7-14: Geräte mit verschiedenen Sensorproblemen auf der Seite

Überprüfung von Informationen zur Geräteintegrität

Informationen zum Onboarding-Status eines Geräts sowie Details zur auf dem Gerät laufenden Engine-Version kannst du entweder auf der Entitätsseite des Geräts oder über die erweiterte Suche abrufen.

Um den aktuellen Status der Geräteintegrität anzuzeigen, navigierst du zu **Assets > Devices** und klickst auf ein Gerät. Suche auf der Übersichtsregisterkarte der Geräteseite den Abschnitt **Geräteintegritätsstatus**, wie unten dargestellt.

Device health status		
Type	State	Date & time
Last full scan	● No scan performed	
Last quick scan	● Completed	Sep 2, 2022, 1:26:38 AM
Security intelligence	● Version 1.373.1371.0	Sep 1, 2022, 6:11:01 PM
Engine	● Version 1.1.19500.2	Sep 1, 2022, 6:11:01 PM
Platform	● Version 4.18.2205.7	Jul 4, 2022, 8:23:07 AM
Defender Antivirus mode	● Active	Sep 4, 2022, 4:25:16 AM

Abbildung 7-15: Überprüfung des Integritätsstatus eines Geräts

Diese Informationen sind nützlich bei der Fehlerbehebung von spezifischen Onboarding- oder Sensorproblemen auf einem Endpunkt. Um dieselben Informationen in der erweiterten Suche zu überprüfen, wirf einen Blick auf die Tabelle *DeviceTvmInfoGather* und suche nach den Werten in der Eigenschaft *AdditionalFields*. Dazu kannst du die folgende Abfrage verwenden:

```
DeviceTvmInfoGathering
| extend parsed = parse_json(AdditionalFields)
| project
    DeviceName,
    AvEngineVersion=tostring(parsed.AvEngineVersion),
    AvMode=tostring(parsed.AvMode),
    AvSignatureVersion=tostring(parsed.AvSignatureVersion),
    AvPlatformVersion=tostring(parsed.AvPlatformVersion)
```

Wenn du dir schließlich nicht die Mühe machen möchtest, die Geräte einzeln zu überprüfen oder eigene Abfragen zu erstellen, um die gewünschten Informationen abzurufen, kannst du auch zum Bericht **Geräteintegrität** navigieren, der unter **Berichte** verfügbar ist. In diesem Bericht kannst du zwischen den verschiedenen Elementen wechseln, die sich auf die Integrität des MDE-Sensors und den Status von Microsoft Defender Antivirus beziehen – wie in der folgenden Abbildung dargestellt.



Abbildung 7-16: Überprüfung des Geräteintegritätsberichts im Microsoft 365 Defender

Onboarding von Servern mit dem einheitlichen Installationspaket

Für **Windows Server 2012 R2** und **Windows Server 2016** kannst du das neue einheitliche Installationspaket verwenden. Vor der Verfügbarkeit dieses Pakets war das Onboarding für diese Betriebssystemversionen etwas kompliziert. Mit dem neuen Paket wurden die Schritte auf 1) Installation des Agenten und 2) Ausführung des Onboarding-Pakets (Skript) reduziert. Darüber hinaus stellt das neue Lösungspaket sicher, dass mehr Funktionen, die bisher nicht verfügbar waren, nun auch funktionieren. Einen detaillierteren Überblick darüber, welche Funktionen verfügbar sind und welche nicht, findest du [hier](#).

Um das neueste Installationspaket abzurufen, öffnest du das **Microsoft 365 Security Center** und navigierst zu **Einstellungen > Endpunkte**. Klicke dort auf **Onboarding** unter **Geräteverwaltung**. Wähle als Nächstes im Dropdown-Menü für das Betriebssystem **Windows Server 2012 R2 und 2016** aus und klicke auf **Installationspaket herunterladen**, wie in Abbildung 7-17 dargestellt.

Sobald du das Installationspaket heruntergeladen hast, kannst du es auf verschiedene Arten bereitstellen:

1. Du führst die Installation manuell durch
2. Du stellst das Installationspaket über ein Konfigurationsverwaltungstool wie z.B. MEMCM bereit.

Bei der Ausführung führt das Installationspaket je nach Betriebssystem verschiedene Schritte durch. Für Windows Server 2012 R2 installiert es Defender Antivirus sowie die erforderlichen EDR-Komponenten. Für Windows Server 2016 werden nur die EDR-Komponenten installiert, da Defender Antivirus bereits Bestandteil des Betriebssystems ist. Vergiss also nicht, Defender AV in Windows Server 2016 zu aktivieren, falls das noch nicht geschehen ist!

Select operating system to start onboarding process:

Windows Server 2012 R2 and 2016

1. Install Agent and Onboard a device

First device onboarded: Completed ✓

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read [Onboard and set up](#).

Before downloading the installation package, review the [instructions](#).

Deployment method

Local Script (for up to 10 devices)

You can configure a single device by running a script locally.
Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above. For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see [Configure devices using a local script](#) section in the Microsoft Defender for Endpoint guide.

[Download installation package](#) [Download onboarding package](#)

Abbildung 7-17: Herunterladen der Installations- und Onboarding-Pakete

Das Installationspaket besteht aus einer einzigen Datei mit dem Namen md4ws.msi. Um die Lösung zu installieren, führst du entweder die Datei manuell aus oder verwendest die folgende Befehlszeile. Beachte, dass durch die Hinzufügung des Schalters /quiet keine Benutzeroberfläche angezeigt wird und die Lösung somit mit einem Konfigurationstool wie MEMCM installiert werden kann.

Msieexec /i md4ws.msi /quiet

Eine weitere Option ist die Verwendung von Microsofts Hilfsskript, das einige zusätzliche Aufgaben ausführt, wie zum Beispiel sicherzustellen, dass alle Voraussetzungen vor der Installation des Pakets korrekt auf dem Server installiert wurden. Das Skript ist auf [GitHub](#) verfügbar und wird von Microsoft gepflegt. Da ich es schon verwendet habe, kann ich sagen, dass es ein sehr nützliches Skript ist – besonders, wenn du die Installation manuell durchführst. Es spricht jedoch nichts dagegen, dasselbe Skript mit deinem bevorzugten Bereitstellungstool zu verwenden. Ein Vorteil des Hilfsskripts ist, dass es das Onboarding-Skript als Eingabeparameter nimmt und es automatisch ausführt, nachdem das MSI korrekt installiert wurde. Wenn du das Skript nicht verwendest, ist dies ein Schritt, den du selbst (oder über ein Tool) ausführen musst. Erkennung von Geräten, die integriert werden können

Im Jahr 2021 veröffentlichte Microsoft die **Geräteerkennung**, eine Funktion von Microsoft Defender für Endpunkte, die jedes integrierte Gerät in eine Art Wächter verwandelt, der nach anderen Geräten im Netzwerk sucht und über deren Status und Sicherheitsrisiken berichtet. So kannst Du 1) Geräte integrieren, die aus irgendeinem Grund nicht zuvor integriert wurden, und 2) Informationen zur Bedrohungs- und Schwachstellenverwaltung für diese Geräte überprüfen. Schließlich können nicht verwaltete Geräte in Deinem Netzwerk eine erhebliche Bedrohung für

das Unternehmen darstellen. Zum Zeitpunkt des Schreibens gibt es zwei Arten der Geräteerkennung:

- **Grundlegende Erkennung**, bei der integrierte Endpunkte passiv Netzwerkereignisse sammeln, um andere Geräte im selben Netzwerk (oder in denselben Netzwerken) zu identifizieren.
- **Standarderkennung**, die integrierte Geräte in Beacons verwandelt, die aktiv nach anderen Geräten im Netzwerk suchen, indem sie (begrenzte) Netzwerkkommunikation senden. Während die grundlegende Erkennung in den Defender-Binärdateien enthalten ist, wird die Standarderkennung durch PowerShell-Skripte durchgeführt, die von Microsoft Defender für Endpunkte ausgeführt werden.

Geräte, die mit der Geräteerkennung entdeckt wurden, werden ebenfalls in der Liste "Gerätebestand" angezeigt und können anhand ihres *Onboarding-Status* gefiltert werden, der einen der folgenden Werte haben kann:

- **Kann integriert werden** bedeutet, dass die Geräte von Microsoft Defender für Endpunkte unterstützt werden und in Microsoft Defender für Endpunkte integriert werden könnten, dies derzeit aber nicht sind.
- **Nicht unterstützt** wird für Geräte verwendet, die im Netzwerk aktiv sind, aber von Microsoft Defender für Endpunkte nicht unterstützt werden.
- **Unzureichende Informationen** wird verwendet, wenn ein Gerät erkannt wurde, aber keine zusätzlichen Informationen abgerufen werden konnten, um festzustellen, ob das Gerät unterstützt wird. Normalerweise sinkt die Anzahl der Geräte mit diesem Status, wenn die Standarderkennung verwendet wird.

OS platform	Windows 10 versions	Health state ↓	Onboarding status
Windows		Active	Insufficient info
Windows 10	Future	Active	Can be onboarded
Windows		Active	Insufficient info
iOS		Active	Unsupported
Windows		Active	Insufficient info
Windows		Active	Insufficient info
Windows		Active	Insufficient info

Abbildung 7-18: Ein Auszug aus entdeckten Geräten im Netzwerk und ihr jeweiliger Onboarding-Status

Konfiguration der Geräteerkennung

Die Geräteerkennung kannst du konfigurieren, indem du zu **Einstellungen > Geräteerkennung** navigierst. Dort stehen dir mehrere Optionen zur Verfügung.

Auf der Seite **Erkennungseinrichtung** legst du fest, welche Art der Erkennung (Basic oder Standard) aktiviert ist und welche Geräte die Erkennung durchführen sollen. Im Modus der grundlegenden Erkennung lauschen alle integrierten Geräte automatisch auf Geräte im Netzwerk. Im Standardmodus kannst du auswählen, ob alle oder nur Geräte mit einem bestimmten Tag die aktive Erkennung übernehmen sollen.

Die Seite **Ausschlüsse** ermöglicht es dir, IP-Adressen oder -Bereiche innerhalb deines Netzwerks zu definieren, die von der Geräteerkennung ausgeschlossen werden sollen. Das ist sinnvoll, wenn die Erkennung andere Probleme verursacht, etwa Fehlalarme auf einem Netzwerkscanner, oder wenn du einfach nicht möchtest, dass bestimmte Geräte erkannt werden. Möchtest du ganze Netzwerke von der Überprüfung ausschließen, solltest du die Seite **überwachte Netzwerke** verwenden.

Nicht ideal: Beim Ausschluss von IP-Adressbereichen handelt es sich um globale Ausschlüsse. In bestimmten Szenarien können sich die IP-Adressbereiche von Heimnetzwerken mit denen deines Unternehmens überschneiden. In diesem Fall solltest du nicht auf Basis von IP-Adresse ausschließen, sondern die Funktion *überwachte Netzwerke* verwenden.

Auf der Seite **überwachte Netzwerke** findest du eine Übersicht über die verschiedenen erkannten Netzwerke. Beachte, dass hier auch Netzwerke außerhalb deiner Unternehmensgrenzen erscheinen können. Defender für Endpunkte ignoriert automatisch Netzwerke, die nicht eindeutig als Teil des Unternehmensnetzwerks identifiziert werden konnten. Die Liste zeigt nur die fünfzig Netzwerke mit den meisten erkannten Geräten und ist entsprechend sortiert, wie in der Abbildung dargestellt.

Network name	Onboarded devices
DCVH-Wireless	⋮ 1
Network	⋮ 1
	⋮ 1
	⋮ 1
	⋮ 1
	⋮ 1
	⋮ 1

Abbildung 7-19: Anzeige einer Liste von Netzwerken im Abschnitt Überwachte Netzwerke der Geräteerkennung.

Als Administrator kannst du ein ignoriertes Netzwerk aktiv überwachen oder ein Netzwerk ignorieren, das zuvor automatisch einbezogen oder manuell aktiviert wurde. Klicke dazu auf die Auslassungspunkte neben dem Netzwerknamen und wähle die passende Option.

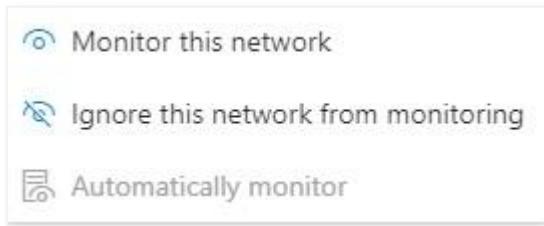


Abbildung 7-20: Ein- oder Ausschließen von Netzwerken von der Überwachung

Neben der Erkennung anderer Geräte über bereits integrierte Endpunkte kannst du auch zusätzliche Datenquellen sowie die Integration mit Microsoft Defender für IoT konfigurieren. Da diese Integrationen in erster Linie der Bewertung von Sicherheitsrisiken anderer Geräte im Netzwerk dienen, findest du nähere Informationen dazu in Kapitel 8: Microsoft Defender Vulnerability Management.

Onboarding von Legacy-Endpunkten

Wenn von Legacy-Endpunkten die Rede ist, sind alle nicht-Windows-10-Geräte gemeint, die von Microsoft Defender für Endpunkte unterstützt werden – zum Zeitpunkt des Schreibens also Windows 7 und Windows 8.1. Wichtig: Diese Betriebssysteme verfügen nicht über Microsoft Defender Antivirus. Möchtest du dennoch einen Virenschutz bereitstellen, musst du System Center Endpoint Protection oder eine andere Drittanbieter-Lösung installieren.

Trotz des fehlenden Defender-Antivirus werden beide Windows-Versionen vom Defender für Endpunkte zumindest im Hinblick auf den EDR-Teil unterstützt. Der Onboarding-Prozess ist allerdings etwas aufwändiger als bei Windows 10. Da die erforderlichen Komponenten nicht ins Betriebssystem integriert sind, musst du den Microsoft Monitoring Agent (MMA) installieren. Dieser sammelt die nötigen Informationen vom Gerät und sendet sie an den mit deiner Defender-Instanz verbundenen Arbeitsbereich.

Bevor du mit der Integration beginnst, solltest du sicherstellen, dass folgende Voraussetzungen erfüllt sind:

- Die neuesten verfügbaren Updates sind installiert (auch wenn sie nicht zwingend erforderlich sind).
- Das Update für [Benutzererfahrung und Diagnosetechnologie](#) ist vorhanden.
- .NET Framework 4.5 oder höher ist installiert.

Sobald alle Voraussetzungen erfüllt sind, kannst du die passende Version des Windows MMA-Agents ([64-Bit](#) oder [32-Bit](#)) herunterladen und installieren. Während der Installation wirst du nach der **Log Analytics Workspace-ID** und dem **Workspace-Schlüssel** gefragt. Diese findest du im **Microsoft 365 Security Center** unter **Einstellungen > Endpunkte > Onboarding**. Wähle oben im Bildschirm Windows 7 SP1 und 8.1 aus und kopiere die Informationen unter Schritt 3 (siehe Abbildung 7-21).

MMA vs. AMA: Der Microsoft Monitoring Agent (MMA) befindet sich am Ende seiner Lebensdauer und wird durch den Azure Monitoring Agent (AMA) ersetzt. Auch wenn AMA derzeit (noch) nicht alle Funktionen von MMA abdeckt, wirst du mittelfristig auf AMA umsteigen müssen. Die Entwicklung bleibt abzuwarten.

Sobald du die Workspace-Daten eingegeben und den Agent erfolgreich installiert hast, ist das Gerät integriert. Die zugehörigen Informationen sollten innerhalb weniger Minuten auf der Gerätebestandsseite in Defender für Endpunkte erscheinen.

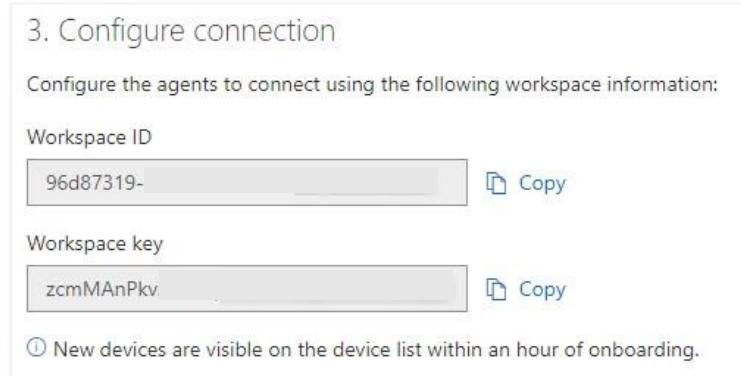


Abbildung 7-21: Abrufen der Workspace-ID und des Schlüssels für den MMA-Agent

Onboarding von Servern in Defender for Endpoint

Der Onboarding-Prozess von Windows-Servern ist fast identisch mit dem von Windows-Client-Betriebssystemen. Der Hauptunterschied besteht darin, dass du Intune nicht für Server-Betriebssysteme nutzen kannst. Andererseits kannst du Server in Azure über das Azure Security Center einbinden, was dir eine vergleichbare Anzahl von Möglichkeiten zur Durchführung des Onboardings bietet. Ähnliche Einschränkungen wie bei den Client-Betriebssystemen gelten auch für Server. Derzeit benötigen ältere Server-Betriebssysteme (alles vor Server 2019) noch den Microsoft Monitoring Agent. Dieser Agent kann über den Configuration Manager oder das Azure Security Center installiert werden. Von diesen Betriebssystemen können nur Windows Server 2016 und neuer Microsoft Defender Antivirus nutzen. Jedes Betriebssystem davor benötigt den System Center Endpoint Protection Agent oder eine Drittanbieterlösung.

Beachte, dass eine neue Vorschauversion verfügbar ist, die das Erlebnis für ältere und neuere Server-Betriebssysteme vereinheitlicht. Diese Vorschau bietet nicht nur ein neues Onboarding-Erlebnis, das die Installation des Microsoft Monitoring Agents überflüssig macht, sondern fügt auch Unterstützung für Funktionen hinzu, die zuvor für Windows Server 2012 R2 und Windows Server 2016 nicht verfügbar waren. Diese neuen Funktionen umfassen unter anderem Attack-Surface-Reduction-Regeln, PUA-Blocking, EDR im Block-Modus und Live Response – kurz gesagt: alle wichtigen Funktionen von Microsoft Defender for Endpoint. Einige Einschränkungen bestehen jedoch weiterhin. Zum Beispiel sind nicht alle Attack-Surface-Reduction-Regeln, die für Windows Server 2019 verfügbar sind, auch für ältere Versionen nutzbar.

Windows Server 2019 und 2022 kannst du entweder über ein Onboarding-Paket einbinden, das per Configuration Manager verteilt wird, oder direkt über die Integration mit dem Azure Security Center. Letzteres funktioniert nur für Server, die in Azure gehostet werden oder für lokale Server, die mit Azure Arc verwaltet werden.

Vorsicht bei aktivem vs. passivem Modus: Im Gegensatz zu Windows 10, das automatisch in den passiven Modus wechselt, wenn ein Antivirenprogramm von Drittanbietern erkannt wird, musst du dies bei Windows Server 2019 manuell tun. Dafür musst du einen neuen Registrierungsschlüssel namens ForceDefenderPassiveMode mit dem Wert 1 an folgendem Speicherort erstellen: HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection.

Server, die in Azure Defender registriert sind, werden automatisch in Microsoft Defender for Endpoint eingebunden. Die Lizenz für Azure Defender beinhaltet auch die Lizenz für Defender for Endpoint. Neben dem automatischen Onboarding tauschen Azure Defender und Defender for Endpoint auch Informationen miteinander aus. Das bedeutet, dass Administratoren, die Server in Azure verwalten, auch die Warnungen und Vorfälle sehen können, die von Defender for Endpoint generiert wurden. Entsprechend erscheinen Server, die über Azure Defender eingebunden wurden, ebenfalls im Gerätebestand.

Azure: Die einheitliche Lösung wird automatisch für Server bereitgestellt, die Windows Server 2012 R2 und Windows Server 2016 ausführen und in Azure bereitgestellt oder über Azure Arc verbunden sind.

Microsoft Defender for Cloud

Microsoft Defender for Cloud ist gewissermaßen das Azure-Pendant zu Microsoft 365 Defender. Es bietet mehrere Funktionen und Dienste für den erweiterten Schutz von Azure-Workloads, darunter virtuelle Maschinen, App Services, Key Vaults und vieles mehr. Eine ausführliche Erklärung der Funktionen von Defender for Cloud würde den Rahmen dieses Buches sprengen. Da jedoch viele Organisationen virtuelle Maschinen in Azure betreiben und diese ebenfalls mit Defender for Endpoint schützen möchten, lohnt es sich, kurz auf die Integration einzugehen.

Wenn du den Schutz virtueller Maschinen über Microsoft Defender for Cloud aktivierst, wird automatisch eine passende Erweiterung für virtuelle Maschinen hinzugefügt. Diese Erweiterung – spezifisch für Windows oder Linux – übernimmt das Onboarding der jeweiligen virtuellen Maschine in Microsoft Defender for Endpoint. Dies ist wichtig zu wissen, da – je nachdem, wie diese virtuellen Maschinen verwaltet werden – sie ihre Antiviren- und Firewall-Richtlinien entweder über ihren bisherigen Verwaltungskanal oder über den MDE-Verwaltungskanal erhalten. Im letzteren Fall musst du sicherstellen, dass du deine Richtlinien korrekt eingerichtet hast, bevor du die VMs einbindest, um mögliche Störungen durch fehlende Konfigurationen oder notwendige Ausschlüsse zu vermeiden.

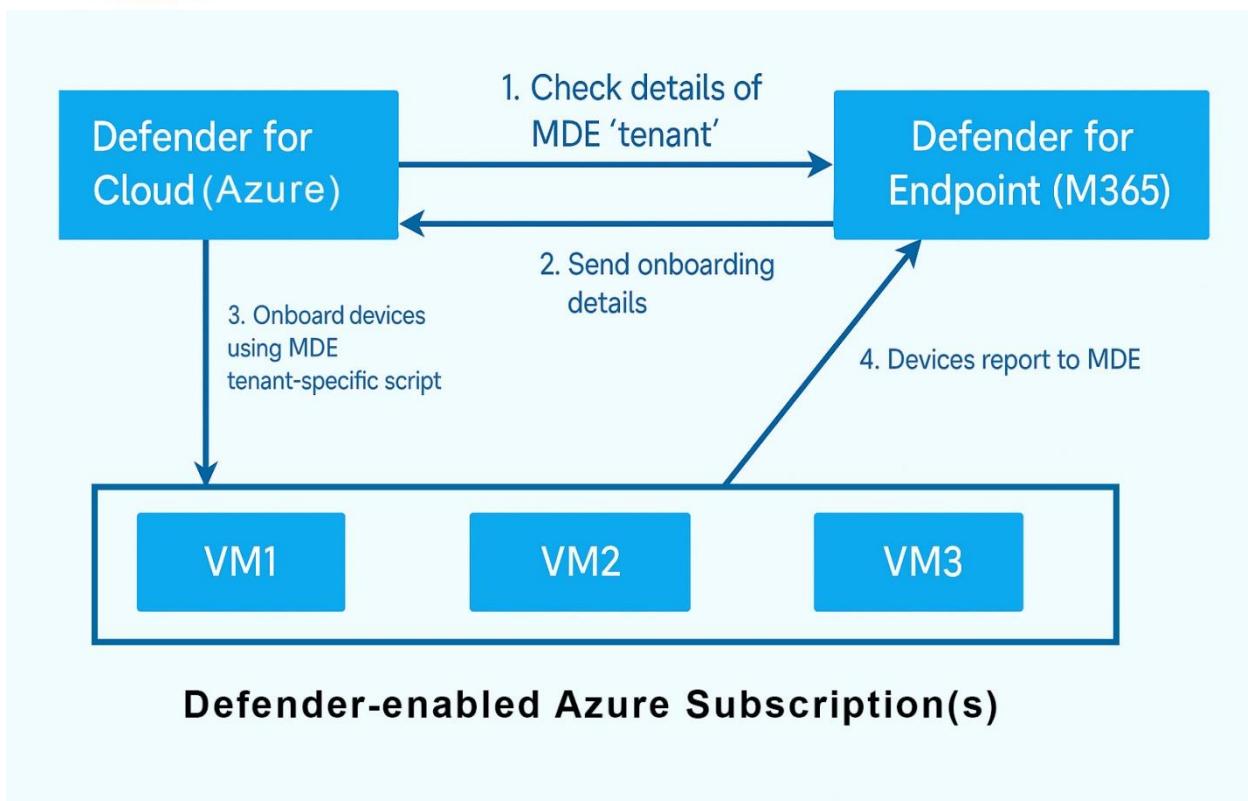


Abbildung 7-22: Überblick über die Integration zwischen Defender for Cloud und MDE

Client-Konfiguration und Richtlinienverwaltung

Bis Mitte 2023 war die Verwaltung von Microsoft Defender for Endpoint noch recht umständlich. Im Gegensatz zu vielen anderen EDR- und Antivirenlösungen wurde Microsoft Defender for Endpoint nicht (und wird teilweise noch nicht) zentral von einem einzigen Ort aus verwaltet. Aber es geht voran.

Vor der (inzwischen veröffentlichten) nativen Sicherheitsverwaltung durch Microsoft Defender for Endpoint war man auf andere Geräteverwaltungsplattformen wie Microsoft Intune angewiesen, um sicherzustellen, dass die Geräte die gewünschten Sicherheitseinstellungen erhielten. Alternativ konnten Einstellungen über Gruppenrichtlinien verteilt oder manuell per PowerShell-Skripte konfiguriert werden – beides wenig ideal, vor allem für große Organisationen mit getrennten Teams für Bereitstellung, Konfiguration und Sicherheitsoperationen.

Zwar ist üblicherweise das Sicherheitsteam für die Definition von Richtlinien, Ausnahmen und anderen sicherheitsrelevanten Einstellungen zuständig, die sich auf die Antiviren- und/oder EDR-Lösungen auswirken. Dieses Team hat aber oft keinen Zugriff auf Microsoft Intune oder andere verwendete Verwaltungsplattformen. Mit der Einführung der nativen Konfigurationsverwaltung in Microsoft Defender for Endpoint ist das nun nicht mehr

erforderlich, und Microsoft hat in dieser Hinsicht endlich zu einigen seiner Konkurrenten aufgeschlossen.

Im Folgenden findest du einen Überblick über die verschiedenen Möglichkeiten, wie Richtlinien in Microsoft Defender for Endpoint verwaltet werden können. Die Informationen basieren auf einer Mischung aus bereits allgemein verfügbaren Funktionen und einigen Features, die sich noch in der Public Preview befinden. Besonders wenn wir über die native Konfigurationsverwaltung sprechen, beziehen wir uns auf diese Vorschau, da sie den umfassendsten Funktionsumfang und die breiteste Unterstützung für verschiedene Betriebssysteme bietet.

Microsoft Defender for Endpoint Sicherheitseinstellungen-Verwaltung

Die Notwendigkeit, Defender for Endpoint über eine klassische Endpunktverwaltung wie Microsoft Endpoint Manager zu steuern, war bislang eine Herausforderung – insbesondere, wenn deine Geräte nicht in Intune eingebunden sind oder du alternative Lösungen wie Altiris verwendest. Bisher bestand die einzige Möglichkeit darin, Gruppenrichtlinien bereitzustellen, PowerShell-Skripte zu verwenden oder mit Drittanbiertools eigene Lösungen zu bauen.

Mit der neuen Sicherheitseinstellungen-Verwaltung in Microsoft Defender for Endpoint hast du jetzt einen „Out-of-Band“-Verwaltungskanal zur Verfügung, über den du – abhängig vom verwendeten Betriebssystem – eine Vielzahl an Sicherheitseinstellungen verwalten kannst.

Policy	Windows (client, server)	macOS	Linux
Antivirus	X	X	X
Antivirus-Ausnahmen	X	X	X
Attack Surface Reduction Rules	X		
Endpoint Detection and Response	X	X	X
Firewall	X		
Firewall-Regeln	X		

Tabelle 7-1: Unterstützte Richtlinien durch Microsoft Defender for Endpoint Sicherheitseinstellungen-Verwaltung

Andere Elemente wie BitLocker erfordern weiterhin ein vollständiges Onboarding in Microsoft Endpoint Manager oder die Verwendung von Gruppenrichtlinien oder Skripten. Im Hintergrund nutzt der neue Verwaltungskanal weiterhin die MEM-Komponenten (wie die Registrierung des

Geräts in Entra ID), aber dies geschieht für dich unsichtbar und wird ausschließlich zur Übermittlung der Richtlinien verwendet.

Wenn du die Sicherheitseinstellungen-Verwaltung aktivierst, verwaltet du die Konfigurationsprofile für die oben genannten Elemente entweder über Microsoft Intune oder das Microsoft 365 Defender-Portal, ohne dass die Geräte in Intune registriert sein müssen. So funktioniert es:

1. Geräte werden in Microsoft Defender for Endpoint eingebunden, zum Beispiel über ein Skript, das auf dem Gerät ausgeführt wird.
2. Die eingebundenen Geräte kommunizieren mit Microsoft Intune. So kann Intune beim Check-in Richtlinien an das Gerät zu verteilen.
3. Im Hintergrund wird eine Geräteregistrierung für das Gerät in Entra ID erstellt. Wenn das Gerät bereits vollständig registriert ist, wird diese Registrierung verwendet. Wenn nicht, wird eine sogenannte *synthetische* Registrierung durchgeführt: Ein Geräteobjekt wird in Entra ID erstellt, um das Targeting von Richtlinien zu ermöglichen. Wenn synthetische Registrierungen vorhanden sind und Geräte später vollständig registriert oder mit Entra ID-verbunden werden, wird die synthetische Registrierung ersetzt.

Die Public Preview unterstützt derzeit eine Vielzahl von Betriebssystemen. Beachte, dass je nach Betriebssystem spezifische Updates/Patches erforderlich sein können:

- Windows 10/11, Windows Server 2012 R2, 2016, 2019, 2022.
- macOS 11, 12, 13
- Linux. Die folgenden oder höhere Versionen davon: Red Hat Enterprise 7.2, CentOS 7.2, Ubuntu 16.04, Debian 9, SLES 12, Oracle Linux 7.2, Amazon Linux 7.2, Fedora 22

Nicht unterstützt: Die Einstellungsverwaltung auf nicht-persistenten virtuellen Desktops und Domänencontrollern wird nicht unterstützt.

Um den neuen Verwaltungskanal zu aktivieren, musst du dich am Microsoft 365 Security Center anmelden, zur Konfigurationsverwaltung unter **Einstellungen > Endpunkte** navigieren und anschließend auf **Durchsetzungsbereich** klicken. Von dort aus kannst du die Aktivierung für die verschiedenen unterstützten Betriebssysteme wählen. Hier kannst du auch die MDE-Verwaltung für Defender for Cloud-aktivierte Geräte einschalten.

Melde dich zuletzt am Microsoft Intune-Portal an und navigiere zu **Endpoint Security > Setup > Microsoft Defender for Endpoint**. Auf dieser Seite schaltest du den Schalter für „Microsoft Defender for Endpoint erlauben, Endpoint Security-Konfiguration durchzusetzen“ auf „Ein“.

Verwaltungsrollen: Die neue Verwaltungsrolle führt auch neue Funktionen in den Rollendefinitionen für Microsoft Defender ein. Wenn du zuvor benutzerdefinierte Rollen erstellt hast, stelle sicher, dass du die Berechtigung *Endpoint Security-Einstellungen in Microsoft*

Endpoint Manager verwalten hinzufügst, damit Admins auch die notwendigen Sicherheitsrichtlinien in MEM erstellen und verwalten können!

Nachdem du das Backend für die Unterstützung der Verwaltung über Microsoft Defender for Endpoint konfiguriert hast, solltest du Entra ID-Gruppen erstellen, die die Geräte enthalten, die du verwalten möchtest. Es liegt bei dir, Gruppen pro Betriebssystem, pro Gerätetyp, pro Verwaltungstyp usw. zu erstellen.

Erstellen und Bereitstellen von Richtlinien

Mit der Defender-Einstellungsverwaltung-Bereitstellung kannst du sowohl Intune als auch Microsoft 365 Defender verwenden, um Richtlinien zu erstellen und bereitzustellen. Hier schauen wir uns die Option mit Microsoft 365 Defender genauer an. Um eine Richtlinie zu erstellen, öffne das Microsoft 365 Defender-Portal und navigiere zu **Endpunkte > Konfigurationsverwaltung > Endpoint Security-Richtlinien**. Richtlinien, die bereits in Intune erstellt wurden, werden hier ebenfalls angezeigt.

Klicke als Nächstes auf „**Neue Richtlinie erstellen**“ und wähle die Plattform (Betriebssystem) sowie die Art der Richtlinie aus, die du erstellen möchtest – zum Beispiel Microsoft Defender Antivirus. Klicke dann auf „**Richtlinie erstellen**“ und gehe durch den Assistenten, um die gewünschten Einstellungen zu konfigurieren. Sobald du zum Abschnitt **Zuweisungen** kommst, wähle die entsprechende(n) Entra ID-Gruppe(n), die du anvisieren möchtest. Geräte in dieser oder diesen Gruppen erhalten die Richtlinie.

Mit der Einführung der Einstellungsverwaltung wurde auch die Geräteentitätsseite aktualisiert und enthält einen neuen Tab namens „**Sicherheitsrichtlinien**“. Von dort aus kannst du alle Sicherheitsrichtlinien einsehen, die an das Gerät gesendet wurden, und ob sie erfolgreich angewendet wurden oder nicht:

Policy Name ↑	Policy type	Status
EDR Onboarding Policy	Endpoint detection and response	● Success
SEC_WIN_Attack Surface Reduction Rules	Settings Catalog	● Success
SEC_WIN_Bitlocker	BitLocker	● Error
SEC_WIN_Default Account Protection p...	Account protection (preview)	● Success
SEC_WIN_Default Antivirus Policy	Microsoft Defender Antivirus	● Conflict
SEC_WIN_Default Antivirus Policy	Microsoft Defender Antivirus	● Conflict
SEC_WIN_Default Firewall Policy	Endpoint Security	● Success
SEC_WIN_Default Firewall Policy	Microsoft Defender Firewall	● Success

Abbildung 7-23: Anzeigen von Geräte-Sicherheitsrichtlinien im Microsoft 365 Defender-Portal

Vorsicht bei doppelten Richtlinien: Eine allgemeine Empfehlung ist es, die Anwendung mehrerer Richtlinien zu vermeiden, die dieselbe Einstellung auf einem Gerät konfigurieren, um widersprüchliche Richtlinien und möglicherweise nicht übereinstimmende Einstellungen zwischen dem, was du auf dem Gerät landen möchtest, und dem, was tatsächlich angewendet wird, zu verhindern. Der Screenshot oben ist ein typisches Beispiel dafür, was man nicht tun sollte.

Geräte, die ihre Einstellungen von Microsoft Intune erhalten, bekommen automatisch neue Richtlinien und Updates bei ihrer nächsten Abfragezeit. Um den Prozess zu beschleunigen, kannst du als Administrator manuell eine Abfrage vom Gerät aus initiieren oder eine **Richtliniensynchronisation** von Intune aus anfordern. Eine ähnliche Option steht dir auch im Microsoft 365 Defender-Portal zur Verfügung. Wenn ein Gerät von der Microsoft Defender for Endpoint-Einstellungsverwaltung verwaltet wird, ist die Option zur Synchronisierung einer Richtlinie im Aktionsmenü eines Geräts verfügbar. Um auf das Menü zuzugreifen, öffne die Geräteseite und klicke auf die Auslassungspunkte in der oberen rechten Ecke der Seite.

Koexistenz mit Microsoft Configuration Manager

Wenn du Microsoft Configuration Manager verwendest, um Geräte in deiner Umgebung zu konfigurieren und zu verwalten, musst du dich entscheiden, ob du diesen oder einen anderen

Kanal zur Konfiguration von Sicherheitsrichtlinien verwenden möchtest. Standardmäßig übernimmt die Defender-Einstellungsverwaltung, wenn du sie aktiviert hast, die Konfiguration von Sicherheitseinstellungen – auch wenn Geräte mit dem Microsoft Configuration Manager verwaltet werden. Um Geräte stattdessen mit dem Microsoft Configuration Manager zu konfigurieren, gehe wie folgt vor:

Melde dich am Microsoft 365 Defender-Portal an, navigiere zu **Einstellungen > Endpunkte > Konfigurationsverwaltung** und klicke dann auf **Durchsetzungsbereich**. Aktiviere am unteren Rand der Seite die Einstellung **Sicherheitseinstellungen mit Configuration Manager verwalten**.

Microsoft Intune

Der beste Weg, um Richtlinien für Defender for Endpoint zu verwalten, ist die Nutzung von Microsoft Endpoint Manager (Intune). Von allen verfügbaren Verwaltungskanälen ist dies der vollständigste. Er unterstützt alle Funktionen und Konfigurationsmöglichkeiten. Natürlich müssen Geräte bei Intune registriert sein – entweder nativ oder im Co-Management mit Microsoft Configuration Manager (MEM-CM) –, bevor sie über Intune für Microsoft Defender for Endpoint verwaltet und konfiguriert werden können. Mit Intune kannst du Geräte verwalten, die Windows-Client-Betriebssysteme, macOS, iOS und Android ausführen. Linux hingegen benötigt einen anderen Ansatz, der später besprochen wird.

Um Microsoft Defender for Endpoint-Funktionen und -Richtlinien zu konfigurieren, navigiere zum [Microsoft Endpoint Manager-Portal](#). Klicke von dort aus auf **Endpoint Security**, um auf den sicherheitsbezogenen Bereich des Portals zuzugreifen. Dort kannst du die folgenden Defender for Endpoint-Funktionen verwalten:

- **Antiviruseinstellungen**, einschließlich der Kern-Antivirus- und Benutzeroberflächen-einstellungen;
- **BitLocker (Laufwerksverschlüsselung)**;
- **Defender Firewall** und Firewall-Regeln;
- **Endpoint Detection & Response**, umfasst das Onboarding von Geräten;
- **Attack Surface Reduction-Funktionen**, einschließlich Attack Surface Reduction-Regeln, Exploit-Schutz, Web-Schutz, Anwendungs- steuerung, Gerätekontrolle, etc.

Weitere Details zur Konfiguration jeder dieser Funktionen findest du in den entsprechenden Abschnitten später in diesem Kapitel. Die Plattform kombiniert mehrere Produkte und Funktionen und erstreckt sich damit über mehr als nur Defender for Endpoint. Deshalb werden zum Beispiel BitLocker, Defender Firewall und Windows Hello for Business auch von hier aus konfiguriert.

Server-Betriebssysteme: Da Microsoft Intune Server-Betriebssysteme nicht nativ unterstützt, musst du diese anders als deine Windows-Clients verwalten. Der empfohlene Weg ist die Verwaltung über den Configuration Manager (siehe unten). Wenn du Configuration Manager nicht zur Verfügung hast, sind Gruppenrichtlinien deine nächstbeste Option. Eine Ausnahme ist

die Verwendung der Defender for Endpoint-Sicherheitskonfigurationsverwaltung. In solchen Fällen gelten Richtlinien, die du im Portal konfiguriert hast, auch für Server. Dies gilt jedoch nur für bestimmte Richtlinien, die später in diesem Kapitel beschrieben werden.

Microsoft System Center Configuration Manager (SCCM)

Viele Organisationen verwenden Microsoft Endpoint Manager Configuration Manager zur Verwaltung ihrer Geräte. Mit der Weiterentwicklung von Microsoft Intune bewegen sich diese Organisationen allmählich in Richtung Cloud oder verfolgen einen hybriden Ansatz mit Co-Management zwischen Intune und Configuration Manager. Beide Optionen können für die Bereitstellung und Konfiguration von Microsoft Defender for Endpoint genutzt werden. Trotz der Verbreitung des Configuration Managers konzentrieren wir uns in diesem Kapitel nicht darauf, wie man ihn zur Verwaltung von Defender for Endpoint nutzt. Stattdessen liegt der Fokus auf der Cloud-basierten Verwaltung mit Intune. Es gibt viele Vorteile bei der Verwendung von Intune gegenüber anderen Bereitstellungsmethoden: Es ist nicht nur erheblich einfacher, Richtlinien zu erstellen und Geräte einzubinden, sondern auch Updates sind schneller verfügbar, ASR-Regeln lassen sich leichter bereitstellen und die Berichterstattung ist deutlich besser. Daher wirst du im weiteren Verlauf dieses Kapitels keine detaillierten Informationen darüber finden, wie bestimmte Aufgaben mit dem Configuration Manager ausgeführt werden. Wo nötig, werden jedoch wichtige Unterschiede oder Einschränkungen genannt.

Unterstützung älterer Systeme: Ein Bereich, in dem Configuration Manager einen Vorteil gegenüber Microsoft Intune hat, ist die Unterstützung für ältere Betriebssysteme - insbesondere Windows Server 2008 R2, Windows 7 und Windows 8. Diese Betriebssysteme haben keinen Zugriff auf Microsoft Defender. Daher musst du bei der Bereitstellung von Microsoft Defender for Endpoint eine andere Antivirenlösung nutzen oder auf System Center Endpoint Protection zurückgreifen.

Co-Management

Nur weil du möglicherweise bereits den Configuration Manager einsetzt, heißt das nicht, dass du Microsoft Intune nicht zusätzlich verwenden kannst – im Gegenteil. In Organisationen, die bereits den Configuration Manager nutzen, ist es relativ einfach, Co-Management zu aktivieren und einzelne Workloads von Configuration Manager zu Microsoft Intune zu verschieben. Das bedeutet: Der Configuration Manager wird weiterhin für bestimmte Aufgaben verwendet, während Microsoft Intune beispielsweise für die Verwaltung sicherheitsbezogener Einstellungen zuständig ist.

Um Co-Management erfolgreich zu nutzen und die volle Funktionalität von Microsoft Defender for Endpoint über Intune freizuschalten, müssen mindestens die folgenden Workloads so konfiguriert sein, dass sie über Microsoft Intune verwaltet werden können:

- Compliance-Richtlinien

- Gerät konfiguration
 - Endpoint Protection
 - Ressourcenzugriffs- Richtlinien

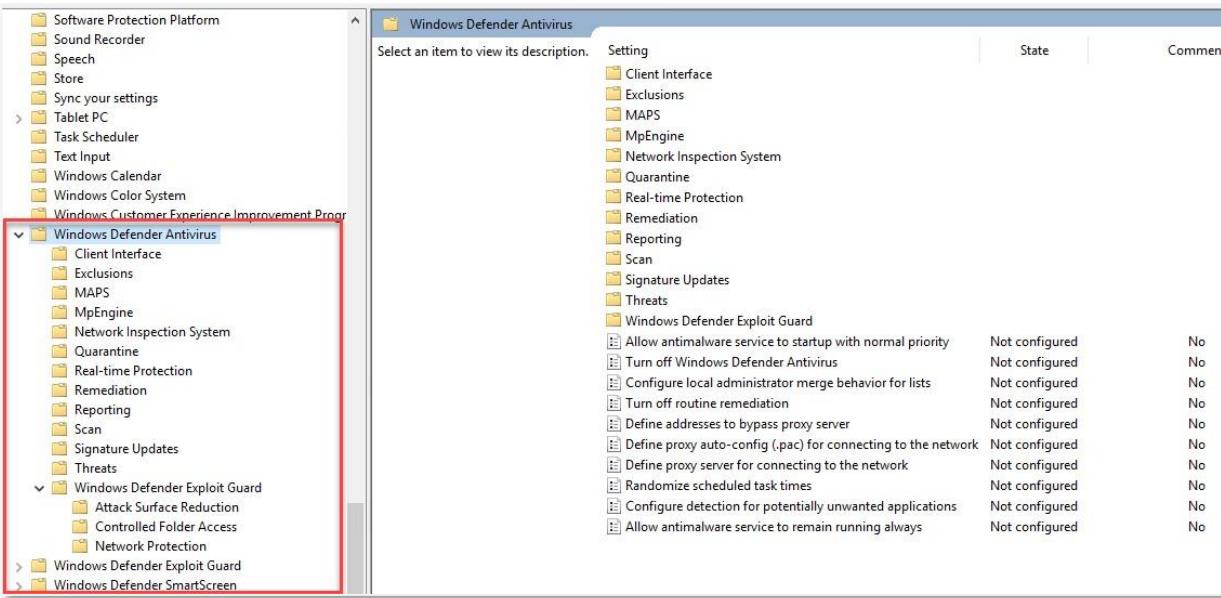
Indem du in Configuration Manager die Konfiguration auf **Pilot Intune** umstellst, kannst du kontrollieren, welche Geräte wie für die oben genannten Workloads verwaltet werden. So musst du nur Geräte einbeziehen, die in Defender for Endpoint eingebunden sind; andere Geräte bleiben weiterhin wie bisher verwaltet.

Plane entsprechend: Je nachdem, wie du den Configuration Manager heute verwendest, musst du möglicherweise mehr als nur Defender for Endpoint in Intune konfigurieren. Betrachte zum Beispiel den *Endpoint Protection*-Workload: Wenn du diesen zu Microsoft Intune verschiebst, BitLocker aber zuvor bereits über den Configuration Manager verwaltet hast, musst du sicherstellen, dass BitLocker nun auch über Intune verwaltet wird. Aufgrund der unterschiedlichen Funktionsweise zwischen beider Systeme kann daraus zusätzlicher Aufwand für dich entstehen. Die meisten dieser Änderungen haben keine Auswirkungen auf den Benutzer, können jedoch beeinflussen, wie du Geräte bereitstellst, Fehler behebst und anderweitig verwaltet.

Gruppenrichtlinie

Bis heute sind Gruppenrichtlinien ein weit verbreiteter Weg, um Geräte in Unternehmensumgebungen zu konfigurieren. Sie sind einfach zu verwenden, sehr umfassend und sowohl in Windows-Client- als auch Server-Betriebssysteme integriert. Allerdings gelten sie mittlerweile als etwas veraltet. Während Gruppenrichtlinien früher der einzige effiziente Weg zur Konfiguration von Geräten waren, gibt es heute bessere Optionen. Abgesehen davon, dass dein Gerät mit einer Active Directory-Domäne verbunden sein muss, fehlt Gruppenrichtlinien die Möglichkeit zur Berichterstattung. Du kannst nicht nachvollziehen, ob Richtlinien korrekt oder überhaupt angewendet wurden – ein erheblicher Nachteil bei sicherheitskritischen Einstellungen wie Antiviren- oder EDR-Konfigurationen. Schließlich möchtest du sicherstellen, dass jedes Gerät deiner Organisation korrekt eingebunden ist – und du möchtest dies auch belegen können.

Die meisten relevanten Einstellungen findest du in der **Computerkonfiguration** einer Gruppenrichtlinie – insbesondere unter **Administrative Vorlagen > Windows-Komponenten > Microsoft Defender Antivirus, Microsoft Defender SmartScreen und Microsoft Defender Exploit Guard**.



The screenshot shows the Group Policy Management console. On the left, a navigation tree lists various Windows components, with 'Windows Defender Antivirus' expanded and highlighted with a red box. To the right, a table displays configuration settings for 'Windows Defender Antivirus'. The columns are 'Setting', 'State', and 'Comment'. Most settings are listed as 'Not configured'.

Setting	State	Comment
Client Interface	Not configured	No
Exclusions	Not configured	No
MAPS	Not configured	No
MpEngine	Not configured	No
Network Inspection System	Not configured	No
Quarantine	Not configured	No
Real-time Protection	Not configured	No
Remediation	Not configured	No
Reporting	Not configured	No
Scan	Not configured	No
Signature Updates	Not configured	No
Threats	Not configured	No
Windows Defender Exploit Guard	Not configured	No
Allow antimalware service to startup with normal priority	Not configured	No
Turn off Windows Defender Antivirus	Not configured	No
Configure local administrator merge behavior for lists	Not configured	No
Turn off routine remediation	Not configured	No
Define addresses to bypass proxy server	Not configured	No
Define proxy auto-config (.pac) for connecting to the network	Not configured	No
Define proxy server for connecting to the network	Not configured	No
Randomize scheduled task times	Not configured	No
Configure detection for potentially unwanted applications	Not configured	No
Allow antimalware service to remain running always	Not configured	No

Abbildung 7-24: Konfiguration von Microsoft Defender über Gruppenrichtlinien

Wir werden nicht näher darauf eingehen, wie Microsoft Defender for Endpoint über Gruppenrichtlinien konfiguriert wird. Für den Moment genügt es, dass du weißt, dass sie eine Option zur Konfiguration und Verwaltung der Lösung darstellt. Die Empfehlung, bei Microsoft Intune zu bleiben, gilt weiterhin – es ist eine flexiblere Lösung mit vielen Vorteilen gegenüber Gruppenrichtlinien. Die einzige Ausnahme ist die Verwaltung von Defender for Endpoint für Server-Betriebssysteme, da Microsoft Intune diese nicht unterstützt.

PowerShell

Viele der Funktionen von Microsoft Defender for Endpoint kannst du auch über PowerShell verwalten. Das ist besonders praktisch beim Testen, zur Fehlerbehebung oder wenn du keinen Zugriff auf andere Verwaltungskanäle hast. Das könnte der Fall sein, wenn du kein Active Directory nutzt und eine andere Geräteverwaltungslösung im Einsatz ist. In solchen Fällen bietet es sich an, eigene Skripte zu erstellen und sie über die dir zur Verfügung stehende Verwaltungslösung auf deine Geräte zu verteilen. Auch eine manuelle Bereitstellung der Skripte ist möglich – wird aber absolut nicht empfohlen, da sie nicht skalierbar ist.

Die meisten Funktionen werden über die *-MpPreference-Cmdlets gesteuert:

- **Add-MpPreference**, um neue Konfigurationselemente zum Gerät hinzuzufügen
- **Set-MpPreference**, um Konfigurationselemente zu aktualisieren
- **Get-MpPreference**, um die aktuelle Konfiguration abzurufen
- **Remove-MpPreference**, um bestimmte Konfigurationselemente zu entfernen.

Neben diesen Cmdlets gibt es weitere, mit denen du z. B. Warnungen abrufen oder Scans starten kannst. Einen Überblick über diese Cmdlets kannst du dir [hier](#) holen.

Je nachdem, welche Funktion(en) du konfigurieren möchtest, können die PowerShell-Befehle sehr einfach oder auch etwas komplexer sein. Da der Fokus dieses Buches auf Microsoft Intune liegt, wirst du hier keine umfassenden Informationen zur Verwaltung von Microsoft Defender for Endpoint mit PowerShell finden. Zwei einfache Beispiele möchte ich dir aber dennoch zeigen:

Um einen bestimmten Ordner zur Ausschlussliste von Defender Antivirus hinzuzufügen, verwende das Cmdlet Add-MpPreference.

Add-MpPreference -ExclusionPath "C:\ExcludedFolder"

Um einen On-Demand-Scan zu starten, führst du einfach den entsprechenden Befehl aus:

Start-MpScan

Linux verwalten

Diese Optionen sind hervorragend geeignet, um Windows-Betriebssysteme zu verwalten. Für Linux sieht die Situation allerdings anders aus. Zum Zeitpunkt des Schreibens kann Microsoft Intune zwar (einige) Linux-Endpunkte verwalten, die Konfiguration von Antivirus-Richtlinien ist aber noch nicht möglich. Wenn du also eine größere Flotte von Linux-basierten Geräten einsetzt, brauchst du eine andere Methode, um Defender for Endpoint bereitzustellen und zu verwalten.

Wie bei anderen Betriebssystemen solltest du zunächst die Systemanforderungen überprüfen, um sicherzugehen, dass deine Linux-Distribution von Microsoft Defender for Endpoint [unterstützt](#) wird und alle weiteren Systemanforderungen erfüllt sind.

Für die Bereitstellung und Verwaltung von Defender for Endpoint unter Linux hast du folgende Optionen:

- Manuell, über Shell-Skripte, die du auf dem Gerät ausführst
- Verwendung einer Automatisierungslösung für Linux wie Chef, Puppet oder Ansible.

Andere Lösungen: Microsoft stellt Anleitungen zur Konfiguration mit diesen Automatisierungstools bereit. Das heißt aber nicht, dass du nicht auch anderen Lösungen wie z.B. Foreman, Nagios, Salt und so weiter verwenden könntest.

Wie bei den anderen Betriebssystemen eignet sich die manuelle Konfiguration von Defender for Endpoint über lokale Skripte gut für Tests, ist aber kein skalierbarer Ansatz. Es ist deutlich

sinnvoller, auf ein Automatisierungssystem zu setzen, um Konfigurationsabweichungen zu vermeiden und sicherzustellen, dass dein gesamter Gerätebestand konsistent eingebunden ist.

Herausfordernd: Da ich selbst kein Linux-Experte bin, finde ich die Bereitstellung von Microsoft Defender for Endpoint für Linux durchaus herausfordernd. Nicht, weil die Bereitstellung an sich schwierig wäre - das ist sie nicht! – sondern weil Linux Allerdings selten auf typischen Benutzergeräten eingesetzt wird. In der Regel kommt es in Produktionsumgebungen oder bei Entwicklern im Einsatz. Diese Szenarien bringen oft spezielle Anforderungen und Software mit, die sich nicht immer für eine Standardkonfiguration eignen. Daher empfehle ich dir, mit einer lokalen (Test-) Installation zu starten und dort eine Konfiguration mit Skripten zu entwickeln. Sobald diese stabil läuft, kannst du sie auf deinen restlichen Gerätebestand ausrollen.

Richtlinienverwaltung

Bevor du den Defender for Endpoint-Sensor auf deinen Geräten bereitstellst, ist es sinnvoll, einen übergeordneten Bereitstellungsplan zu erstellen. Es gibt viele Möglichkeiten, wie du Defender for Endpoint und seine Funktionen einführen kannst. Ich persönlich bevorzuge es, Geräte möglichst schnell in Defender for Endpoint einzubinden – auch wenn noch nicht alle Funktionen konfiguriert sind. So erhältst du sehr schnell Sichtbarkeit über deine Umgebung. Danach kannst du dich Schritt für Schritt um die individuelle Anpassung der Funktionen kümmern.

Beim Onboarding in Defender for Endpoint – und damit dem Start der Telemetriedaten-Erfassung – konfiguriere ich in der Regel auch die folgenden Funktionen. Beachte dabei, dass ihre Einrichtung in den jeweiligen Abschnitten dieses Kapitels erläutert wird und nicht zwangsläufig im Onboarding-Teil enthalten ist:

- Attack Surface Reduction-Regeln im Audit-Modus
- Netzwerkschutz im Audit-Modus

Wenn auf deinen Geräten bereits eine andere Antivirenlösung aktiv ist, besteht der erste Schritt nach dem Onboarding in Defender for Endpoint darin, diese zu ersetzen. Das kann zeitaufwendig sein, da du die bisherige Lösung zuerst vollständig entfernen musst, bevor Microsoft Defender Antivirus seine volle Wirkung entfalten kann.

Defender for Endpoint und Defender Antivirus: zusammen besser

Obwohl Microsoft eine leistungsstarke Marketingabteilung hat, frage ich mich manchmal, woher sie ihre Ideen nehmen... Obwohl Microsoft Defender for Endpoint Microsoft Defender Antivirus nutzt, schließen sich die beiden nicht gegenseitig aus. Du könntest Defender for Endpoint auch über einer anderen Antivirenlösung laufen lassen, ohne Microsoft Defender Antivirus wirklich zu aktivieren. Das sorgt oft für Verwirrung bei Kunden, da beide als

„Defender“ bezeichnet werden, aber unterschiedliche Aufgaben erfüllen – EDR auf der einen, lokales Antivirus auf der anderen Seite.

Beide Produkte gehören zur gleichen Suite und funktionieren am besten, wenn sie gemeinsam genutzt werden. Wenn die Cloud-Plattform zum Beispiel beschließt, bestimmte Aktivitäten zu blockieren, sendet sie die Anfrage zur Blockierung oder Quarantäne einer Datei oder eines Prozesses an den Sensor auf dem Gerät – den Microsoft Defender. Ist der Sensor nicht vorhanden oder nicht aktiv, kann das EDR zwar Aktivitäten erkennen, aber nicht aktiv eingreifen.

Aktiver vs. Passiver Modus

In Windows 10 und Windows Server 2019 läuft Microsoft Defender Antivirus im aktiven Modus, wenn keine andere Antivirensoftware installiert ist. Das bedeutet, dass er als primäres Antivirus für den Geräteschutz zuständig ist. Wird hingegen eine Antivirenlösung eines Drittanbieters installiert, wechselt Microsoft Defender Antivirus automatisch in den passiven Modus. In diesem Zustand verarbeitet der Sensor weiterhin Dateien beim Zugriff, übernimmt jedoch keine weiteren Aufgaben, um nicht mit der anderen Sicherheitslösung zu kollidieren.

EDR im Block-Modus

Die Aussage, dass Defender for Endpoint bei Verwendung eines anderen Antivirus nicht eingreifen könne, ist nicht ganz korrekt. Dank des EDR-Blockmodus kann Defender for Endpoint auch mit einem im passiven Modus befindlichen Defender Antivirus bestimmte Aktivitäten blockieren, sobald diese vom Cloud-Dienst erkannt wurden. So bleiben die EDR-Funktionen zumindest teilweise erhalten, auch wenn eine andere Sicherheitslösung aktiv ist.

Manipulationsschutz

Böswillige Akteure versuchen häufig, die Erkennung zu umgehen – etwa durch das Deaktivieren der Sicherheitssoftware, das Ausnutzen vorhandener Ausschlüsse oder das Hinzufügen neuer. Um das zu verhindern, schützt der Manipulationsschutz (Tamper Protection) vor Änderungen, die die Funktionalität von Microsoft Defender beeinträchtigen könnten.

Zum Zeitpunkt des Schreibens ist der Manipulationsschutz für Windows 10, Windows 11, Windows Server 2012 R2, 2016, 2019, 2022 sowie für macOS verfügbar. Unter Windows ist er standardmäßig aktiviert und lässt sich über Microsoft Defender for Endpoint sowie die Microsoft Defender-Sicherheitskonfiguration verwalten. Unter macOS muss er manuell aktiviert werden – beispielsweise über JAMF oder Microsoft Intune (Endpoint Manager).

Unified Solution Package: Beachte, dass die Verfügbarkeit des Manipulationsschutzes für Server 2012 R2 eine Verwendung des vereinheitlichten Lösungspakets erfordert.

Auf Windows-Systemen verhindert der Manipulationsschutz – unabhängig davon, ob Änderungen interaktiv, per CLI, PowerShell, Registry-Editor oder über Gruppenrichtlinien erfolgen – unter anderem:

- das deaktivieren von Antivirus, Echtzeitschutz und Verhaltensüberwachung;
- das Stoppen oder Neustarten von Defender Windows-Diensten;
- das Deaktivierung des cloudbasierten Schutzes;
- das Entfernen von Sicherheitsinformationsupdates (Definitionen);
- das Deaktivieren automatischer Aktionen bei erkannten Bedrohungen;
- der Schutz von Microsoft Defender Antivirus-Ausschlüssen.

Für macOS werden folgende Aktivitäten verhindert:

- das Deinstallieren des Defender for Endpoint-Agents;
- das Bearbeiten oder Ändern von Defender for Endpoint-Dateien;
- das Erstellen neuer Dateien unter dem Defender for Endpoint-Speicherort;
- das Löschen oder Umbenennen von Defender for Endpoint-Dateien;
- das Stoppen des Agents per Befehl.

Schutz von Ausschlüssen: Ausschlüsse werden nur dann geschützt, wenn eine [Reihe von Bedingungen erfüllt ist](#). Dazu gehört unter anderem, dass *DisableLocalAdminMerge* aktiviert ist, Intune die MDAV-Ausschlüsse verwaltet und die Schutzfunktion explizit aktiviert wurde.

Fehlersuche bei Defender for Endpoint auf dem Endpunkt

Manchmal laufen die Dinge nicht wie erwartet, und du musst möglicherweise untersuchen, warum sich ein Gerät nicht korrekt einbinden ließ, warum sich eine bestimmte Richtlinie nicht wie erwartet verhielt oder warum eine Richtlinie eine Anwendung daran hinderte, etwas zu tun. In solch einem Fall kann es vorkommen, dass ein bestimmtes Konfigurationselement oder eine Richtlinie dir das Leben etwas schwerer macht als gedacht. Noch schwieriger wird es, wenn der Manipulationsschutz aktiviert ist, da ein lokaler Administrator die Konfiguration nicht (vorübergehend) umgehen kann, um die Ursache des Problems zu finden.

Um das zu ermöglichen, kann ein (Sicherheits-)Administrator den Fehlersuchmodus für jedes eingebundene Gerät aktivieren. Sobald der Modus aktiv ist, können lokale Administratoren (die mindestens das lokale Recht „Sicherheitseinstellungen verwalten“ auf der Workstation oder dem Server besitzen) Richtlinien ändern, die sonst durch den Manipulationsschutz gesperrt wären. Sie können jedoch Microsoft Defender Antivirus nicht deaktivieren oder andere Konfigurationsänderungen vornehmen, die die korrekte Funktionsweise von Microsoft Defender for Endpoint stören würden. Während des Fehlersuchprozesses werden alle Aktivitäten weiterhin überwacht.

Um ein Gerät in den Fehlersuchmodus zu versetzen, muss ein Administrator die Geräteseite über das Portal öffnen und auf „**Fehlersuchmodus einschalten**“ in den verfügbaren Aktionen klicken. Nach der Aktivierung kann es bis zu fünfzehn (15) Minuten dauern, bis der Modus auch auf dem Gerät wirksam ist. Der Fehlersuchmodus bleibt aktiv, bis ein Administrator ihn ausschaltet oder ein Zeitraum von drei (3) Stunden abläuft. Danach wird der Modus automatisch deaktiviert.

Weitere Informationen zur Verwendung der Fehlersuche und zu den Voraussetzungen, die erfüllt sein müssen, damit der Fehlersuchmodus funktioniert, sind [\[hier\]{.underline}](#) dokumentiert.

Offboarding

Eine oft übersehene Aufgabe ist das Offboarding von Geräten, die nicht mehr in Gebrauch sind. Obwohl es kein großes Problem darstellt, wenn Geräte nicht ausgebunden werden, machen sie den Gerätebestand unübersichtlich, da sie nach sieben Tagen als „Inaktive Geräte“ angezeigt werden. Sie bleiben auf dieser Liste auf unbestimmte Zeit, bis sie manuell entfernt werden.

Das Offboarding von Windows-10-Geräten ist recht einfach. Leider gibt es kein spezielles Offboarding-Profil. Stattdessen musst du ein Skript auf dem Gerät ausführen, das das Offboarding durchführt. Dieses Skript kann beliebig verteilt und ausgeführt werden – manuell, mit Microsoft Endpoint Manager, über Gruppenrichtlinien oder ein anderes Drittanbieter-Tool, das die Aufgabe übernehmen kann. Dasselbe gilt für andere Betriebssysteme wie macOS oder Linux.

Die verschiedenen Skripte kannst du aus dem Microsoft 365 Security Center herunterladen, indem du zu **Einstellungen > Endpunkte > Offboarding** navigierst. Dort wählst du das gewünschte Betriebssystem aus dem Dropdown-Menü und folgst den beschriebenen Schritten. Um zum Beispiel ein macOS-Gerät auszubinden, musst du den Agent deinstallieren und ein Python-Skript ausführen:

^ Offboard macOS devices through Microsoft Defender for Endpoint

Uninstall the agent and offboard a device

Discontinue Microsoft Defender for Endpoint monitoring on a given device by uninstalling the agent and applying a configuration change to it. Download the following offboarding configuration package available for a range of deployment tools.

For security reasons, the offboarding package will expire within 30 days of its creation. The expiry date is embedded in the created package name: `WindowsDefenderATPOffboardingPackage_valid_until_YYYY-MM-DD.zip` (where YYYY-MM-DD is the expiry date of the package).

Expired offboarding packages sent to a device will fail to offboard the device.

Deployment method

Local Script (for up to 10 devices)



You can configure a single device by running a script locally.

Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other deployment options above.

Before downloading the packages, review the [instructions](#).

 Download package

Abbildung 7-25: Überprüfen der Offboarding-Informationen für macOS

Windows-Geräte, die über den Microsoft Monitoring Agent eingebunden wurden, erfordern, dass du entweder den Monitoring Agent deinstallierst oder die relevante Konfiguration entfernst, damit er keine Daten mehr an den Cloud-Dienst sendet.

In seltenen Fällen hast du möglicherweise keinen Zugriff mehr auf das ursprüngliche Gerät – zum Beispiel, weil es verloren ging, gestohlen wurde oder bereits mit einem anderen Namen oder Betriebssystem neu installiert wurde. In solchen Fällen bleiben Geräte oft zu lange im Geräteliste und du möchtest sie manuell ausbinden. Dazu musst du ein Skript ausführen, das die [Microsoft Defender for Endpoint API](#) aufruft, um das Gerät auf diesem Weg auszubinden. Beachte, dass dies nur für Windows 10 und Windows Server 2019 funktioniert.

Weg aber nicht weg: Auch nach dem Offboarding bleiben Geräte noch eine Weile erhalten. Dies liegt daran, dass zugehörigen Daten 180 Tage lang verfügbar bleiben - auch für ausgebundene Geräte. Diese Informationen könnten für eine spätere Untersuchung noch wichtig sein. Nach Ablauf der 180 Tage gibt es keine weiteren Aktivitätsinformationen mehr, und das Gerät verschwindet aus der Geräteliste. Bis dahin behalten ausgebundene Geräte den Status *Inaktiv*. Eine Möglichkeit diese Geräte besser zu verwalten, besteht darin, ihnen ein bestimmtes Tag zuzuweisen oder sie in einer Geräteliste zusammenzufassen - beispielsweise basierend auf diesem Tag.

Secure Score

Secure Score, ausführlicher in Kapitel 9 besprochen, kann Informationen von Microsoft Defender for Endpoint abrufen und erhält dadurch Einblicke in die Sicherheitslage des

Gerätebestands. Dadurch wird die Berechnung und Verfolgung deines Gerät-Scores ermöglicht, wie unten dargestellt:

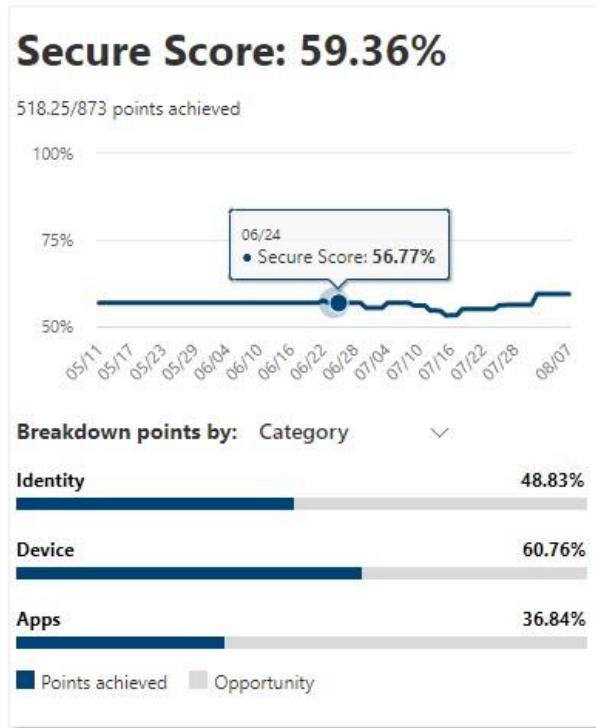


Abbildung 7-26: Der Geräte-Score in Microsoft Secure Score basiert auf Telemetrie von Microsoft Defender for Endpoint.

Um die Integration mit Microsoft Secure Score zu aktivieren oder zu deaktivieren, navigiere zu **Einstellungen > Endpunkte > Erweiterte Funktionen**. Suche **Microsoft Secure Score** in der Liste und schalte die Funktion entweder ein oder aus.

Next-Gen Protection

Eine der Schutzfunktionen von Microsoft Defender for Endpoint ist das Antivirus, auch bekannt als Microsoft Defender. Du hast zweifellos schon von Microsoft Defender gehört – früher war dies der Name des integrierten Antivirus in Windows. Als es zum ersten Mal vor vielen Jahren eingeführt wurde, hatte es keinen guten Ruf und schnitt auch bei den meisten Antivirus-Tests nicht gut ab. In den letzten Jahren ist Microsofts eingebautes Antivirus jedoch zu einer erstklassigen Lösung geworden, die oft besser abschneidet als andere kommerzielle Lösungen.

Das Antivirus liefert modernsten Schutz auf dem Gerät selbst und tut dies auf verschiedene Weise:

- **Cloudbasierter Schutz**, der die Leistung des Cloud-Dienstes nutzt, um bösartige Dateien und Aktivitäten zu erkennen und zu blockieren.

- **Echtzeit-Antivirusschutz**, der als Kernfunktionalität des Antivirus angesehen werden kann: Erkennung und Blockierung bösartiger Dateien und Prozesse. Dies geschieht auf verschiedene Weise, einschließlich Datei- und Prozessverhaltensüberwachung.
- **Immer aktueller Schutz**, der durch dedizierte Updates empfangen wird, die Erkennungsfähigkeiten für die neuesten Bedrohungen enthalten, die auf verschiedene Weise erkannt werden: manuelle und automatische Bigdata-Analyse, maschinelles Lernen und eingehende Bedrohungsforschung durch Microsoft.

Daher ist es keine Überraschung zu erfahren, dass es ein integraler Bestandteil von Microsoft Defender for Endpoint ist und die erste Verteidigungslinie auf dem Gerät selbst bereitstellt. Der Next-Gen-Schutzsensor ist neben seinen Schutzeigenschaften auch dafür verantwortlich, Informationen an den Cloud-Dienst zu sammeln und zu senden. Dies ermöglicht es ihm, Funktionen wie den cloudbasierten Schutz zu nutzen, der später besprochen wird.

Cloudbasierter Schutz

Bedrohungen entwickeln sich blitzschnell, was bedeutet, dass zu dem Zeitpunkt, wenn eine neue Bedrohung erkannt wurde, bereits mehrere andere aufgetaucht sind. Um mit diesen Bedrohungen Schritt halten zu können, sind nicht nur häufige Updates wichtig, sondern auch eine nahtlose Zusammenarbeit zwischen dem Client und der Cloud-Plattform. Letztere ist mit einer Vielzahl anderer Dienste und Systeme verbunden, analysiert kontinuierlich neue Informationen und hat unendlich mehr Rechenleistung als das, was auf dem Gerät selbst verfügbar ist.

Die cloudbasierten Schutzfunktionen, auch als Microsoft Advanced Protection Service (MAPS) bezeichnet, existieren, um die Schutzfähigkeiten des Clients zu verbessern, indem sie ihm ermöglichen, auf das kollektive Wissen der Cloud zuzugreifen. Was bedeutet das? Der Cloud-Dienst ist mit verschiedenen Systemen und allen Kundeninstanzen weltweit verbunden. Dadurch hat er Zugriff auf eine unglaubliche Menge an Informationen, die er kontinuierlich analysiert. Sobald eine potenzielle Bedrohung in der Umgebung eines Kunden erkannt wurde, profitieren alle anderen Instanzen von dieser Erkennung, da sie nun auch sofortigen Zugriff auf diese Information haben. So dauert es nur Momente, bis eine neue Bedrohung auf allen verbundenen Geräten erkannt und blockiert wird. Man könnte sagen: eine kollektive Intelligenz für mehr Sicherheit.

Blockierung beim ersten Auftreten

Wenn Microsoft Defender Antivirus auf eine Datei stößt, die ihm noch nicht begegnet ist und deren Status daher unklar ist, fragt es den Cloud-Dienst ab, um zu prüfen, ob dieser die Datei bereits kennt. Dafür verwendet es den eindeutigen Hash-Wert der Datei.

Wenn der Cloud-Dienst der Datei noch nicht begegnet ist, wird das Antivirus die Datei sperren und eine Kopie davon an die Plattform hochladen, die dann verschiedene Techniken wie

Heuristik, maschinelles Lernen und automatisierte Analyse (Sandboxing) verwendet, um festzustellen, ob die Datei bösartig ist. Sobald ein Urteil über die Datei gefällt wurde, wird der Cloud-Dienst entweder das Öffnen der Datei erlauben oder Defender Antivirus anweisen, die Datei zu blockieren.

Nicht alle Dateien werden überprüft. Die Blockierung beim ersten Auftreten wird nur für ausführbare und nicht-portable ausführbare Dateien verwendet, die aus dem Internet heruntergeladen werden.

Potenziell unerwünschte Anwendungen (PUA)

Neben offensichtlich bösartiger Software gibt es eine ganze Welt von unerwünschten Anwendungen, die in einer Grauzone leben, aber dennoch unerwünscht sind. Dazu gehören zum Beispiel:

- **Adware**, das ist Software, die Werbung, Werbeaktionen und andere unerwünschte Nachrichten innerhalb anderer Anwendungen anzeigt, oder diese in Webseiten einfügt, die du besuchst.
- **Bloatware** ist Software, die automatisch mit anderen Softwarestücken installiert wird, aber nicht unbedingt von derselben Firma stammt oder auch nur mit der Anwendung zusammenhängt, die du gerade installiert hast.

Obwohl nicht per se schädlich, können diese Arten von Anwendungen nervig sein, Systemressourcen verbrauchen und möglicherweise Schwachstellen einführen, die sonst nicht existieren würden. Durch *Potenziell unerwünschte Anwendungen* kann Defender Antivirus prüfen, ob eine Anwendung (ausführbare Datei) als potenziell unerwünscht aufgeführt ist. Wenn ja, wird es verhindern, dass die Anwendung ausgeführt wird.

Die PUA-Liste, die verwendet wird, um zu bestimmen, ob eine Anwendung unerwünscht ist, ist willkürlich und wird von Microsoft verwaltet. Du kannst nicht manuell Anwendungen zu dieser Liste hinzufügen oder von ihr entfernen. Wenn du auf eine Anwendung stößt, die nicht blockiert werden sollte, gibt es zwei Dinge für dich zu tun:

1. Füge einen Ausschluss für die Datei in der Antivirus-Richtlinie hinzu. Dies wird später in diesem Kapitel erklärt.
2. Melde den False Positive an Microsoft.

Audit-Modus: Wenn du dir nicht sicher bist, welche Auswirkungen das Einschalten dieser Funktion haben könnte, kannst du sie zunächst im Audit-Modus testen. Dabei werden

potenziell blockierte Anwendungen protokolliert. Beachte, dass die Protokollierungs-informationen nicht im Microsoft 365 Security Center aufgezeichnet werden und lokal vom Gerät abgerufen werden müssen.

Microsoft Defender SmartScreen

In vielerlei Hinsicht ist Microsoft Defender for Endpoint die erste Verteidigungslinie gegen verschiedene Bedrohungen. Diese Bedrohungen erfordern oft, dass du eine bestimmte Aktion ausführst, bevor sie sich materialisieren können. Leider werden viele Benutzer getäuscht, weil sie fälschlicherweise glauben, eine Website sei vertrauenswürdig oder eine Anwendung harmlos. Phishing ist längst nicht mehr nur ein Thema für E-Mails!

Derzeit funktioniert SmartScreen nur mit Microsoft Edge. Er wurde entwickelt, um dich vor Bedrohungen wie Phishing, durch Websites gelieferter Malware und dem Herunterladen von (potenziell) schädlichen Dateien zu schützen. Dies geschieht auf verschiedene Weisen:

- Webseiten werden auf verdächtiges Verhalten analysiert. Wenn eine Seite als verdächtig eingestuft wird, zeigt SmartScreen dir eine Warnung an.
- Besuchte Websites werden mit einer Liste gemeldeter Phishing-Websites abgeglichen. Bei Übereinstimmung erhältst du eine Warnung, dass die aufgerufene Seite möglicherweise gefährlich ist.
- Wenn du eine Datei herunterlädst, prüft SmartScreen den Hash dieser Datei Gegen eine Liste bekannter bösartiger Dateien. Wird eine Übereinstimmung gefunden, bekommst du eine Warnung, die auf ein potenzielles Risiko hinweist.
- Downloads werden zusätzlich mit einer Liste bekannter und häufig heruntergeladener Dateien verglichen. Fehlt eine Datei auf dieser Liste, wirst du ebenfalls gewarnt und zur Vorsicht aufgefordert.

Die letzten beiden Optionen richten sich nicht ausschließlich gegen bösartige Software. Microsoft Defender SmartScreen arbeitet auch eng mit potenziell unerwünschten Anwendungen zusammen und generiert eine Warnung, wenn eine App als potenziell unerwünscht gilt. Einige typische Warnungen, denen du begegnen könntest, sind:



Abbildung 7-27: Edge Chromium zeigt eine Warnung für einen potenziell gefährlichen Download

Benutzererfahrung: Anstatt dir hier alle möglichen Warnbildschirme von SmartScreen zu zeigen, kannst du dir diese auf der [folgende Website](#) ansehen. Dort kannst du verschiedene Szenarien testen und die Benutzererfahrung selbst nachvollziehen.

SmartScreen überschreiben

In manchen Fällen möchtest du SmartScreens Entscheidung möglicherweise überschreiben, wenn du glaubst, dass das Urteil falsch ist. Je nach Konfiguration kannst du dazu folgende Aktionen ausführen:

Wenn es sich um einen Download handelt, klickst du – wie in Abbildung 7-27 gezeigt – auf die Auslassungspunkte und wählst **Behalten** aus. Möglicherweise musst du zusätzlich eine Sicherheitswarnung bestätigen:

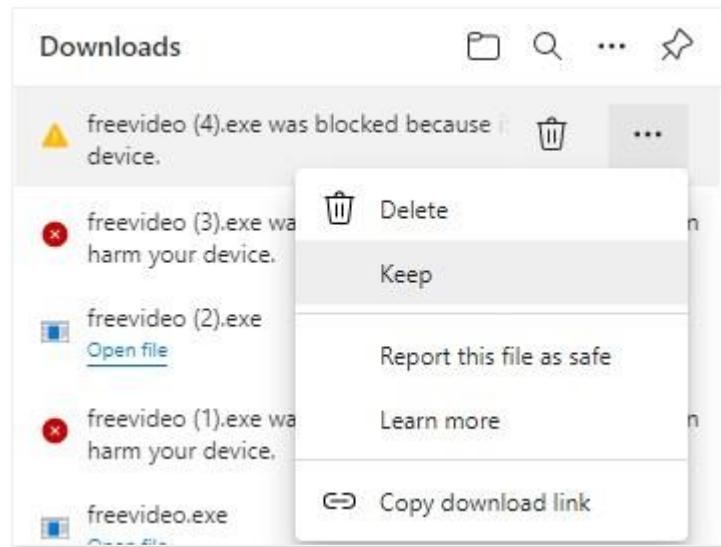


Abbildung 7-28: Überschreiben von SmartScreens Urteil in Microsoft Edge.

Wenn du versuchst, eine blockierte Anwendung auszuführen, klickst du zunächst auf **Weitere Informationen** und dann auf **Trotzdem ausführen**.



Abbildung 7-29: Überschreiben des SmartScreen-Popup-Fensters.

Alternativ kannst du auch mit der rechten Maustaste auf die Datei klicken, bevor du sie öffnest, und **Eigenschaften** auswählen. Am unteren Rand des Eigenschaftenfensters kannst du das Kontrollkästchen neben **Entsperrern** aktivieren. Danach wird die Datei freigegeben (siehe Abbildung 7-30). Beim nächsten Öffnen erscheint dann keine Warnung mehr. Beide Methoden führen letztlich zum gleichen Ergebnis.

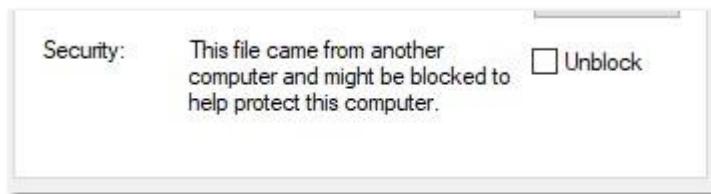


Abbildung 7-30: Überschreiben von SmartScreens Urteil im Windows Explorer.

Next-Gen-Schutz konfigurieren

Da der Next-Gen-Schutz über Microsoft Defender Antivirus bereitgestellt wird, ist es wenig überraschend, dass du diese Funktionen über die Antivirenrichtlinien steuerst. Es gibt drei Arten von Policies:

- Eine **Antivirenpolicy**, mit der du Funktionen aktivierst, deaktivierst oder konfigurierst.
- Eine **Benutzererfahrungspolicy**, die bestimmt, welchen Zugriff du auf das Defender Security Center hast und wie Warnungen dargestellt werden.
- Eine **Ausschlusspolicy**, über die du Ausnahmen für Defender Antivirus definieren kannst.

Diese Policies kannst du im [Microsoft Endpoint Manager Portal](#) konfigurieren, indem du zu **Endpoint Security > Antivirus** navigierst. Klicke dann auf **Policy erstellen**, um den Assistenten zu starten.

Eine Antivirenpolicy konfigurieren

Wähle im ersten Schritt **Windows 10 und höher** als Plattform und **Microsoft Defender Antivirus** als Profiltyp aus und klicke auf **Erstellen**. Auf der Registerkarte **Grundlagen** gibst du einen Namen und eine Beschreibung für die Policy ein und klickst anschließend auf **Weiter**.

Die Registerkarte **Konfigurationseinstellungen** enthält verschiedene Abschnitte, die im Folgenden beschrieben werden.

Cloud-Schutz

In diesem Abschnitt kannst du die meisten cloudbasierten Schutzfunktionen konfigurieren.

- **Cloud-bereitgestellten Schutz aktivieren** steuert, ob die Funktion ein- oder ausgeschaltet wird. Wenn du dies nicht konfigurierst, ist sie standardmäßig aktiviert.
- **Cloud-bereitgestellte Schutzebene** ermöglicht dir die Auswahl zwischen verschiedenen Einstellungen:
 - Hoch: Bietet eine ausgewogene aber starke Schutzebene. Es werden aggressiv unbekannte Dateien blockiert, während die Systemleistung ausgewogen bleibt.
 - Hoch Plus: Ein etwas aggressiverer Ansatz als *Hoch*. Hierbei werden zusätzliche Überprüfungen durchgeführt, wenn eine unbekannte Datei gefunden wird.
 - Null-Toleranz: Blockiert alle unbekannten ausführbaren Dateien.
- **Defender Cloud Extended Timeout** definiert die Anzahl der Sekunden, die Defender Antivirus eine Datei blockieren kann, während sie über den Cloud-Service auf Schadcode überprüft wird. Der von dir eingegebene Wert wird zum Standard-Timeout von 10 Sekunden hinzugefügt.



Abbildung 7-31: Eine Beispielkonfiguration für cloudbasierten Schutz.

Microsoft Defender Antivirus Ausschlüsse

Wie der Name schon sagt, kannst du in diesem Abschnitt Ausschlüsse für Defender Antivirus hinzufügen. Wenn du auch eine separate Ausschlusspolicy erstellst, werden alle Ausschlüsse aus beiden Richtlinien auf die Geräte angewendet.

- **Lokale Admin-Zusammenführung deaktivieren:** Diese Einstellung steuert, ob local definierte Ausschlüsse mit der zentralen Ausschlussliste zusammengeführt werden sollen. Wenn auf **Nein** gesetzt, werden Ausschlüsse zusammengeführt. **Ja** bedeutet, dass nur Ausschlüsse aus den zentralen Policies beibehalten werden - lokale Ausschlüsse werden dann ignoriert.
- **Defender-Prozesse zum Ausschließen:** Diese Einstellung wird verwendet, um eine Liste von Prozessen zu erstellen, die von Defender Antivirus ignoriert werden sollen.
- **Dateierweiterungen von Scans und Echtzeitschutz ausschließen:** Diese Einstellung wird verwendet, um festzulegen, ob bestimmte Dateierweiterungen vom Scanprozess ausgeschlossen werden sollen.
- **Defender-Dateien und -Ordner zum Ausschließen:** Diese Einstellung steuert, welche Dateien und Ordner von Defender Antivirus ignoriert werden sollen.

Sei vorsichtig! Halte Ausschlüsse immer auf einem Minimum und vermeide sie, wenn möglich. Besonders Ordnerausschlüsse können böswilligen Akteuren einen Weg in deine Umgebung bieten, da sie diese Speicherorte missbrauchen könnten, um Schadsoftware zu platzieren oder schädliche Prozesse auszuführen.

Echtzeitschutz

Echtzeitschutzeinstellungen beziehen sich auf die Kernfunktionalität des Antivirusscanners, einschließlich Scanverhalten, Netzwerkschutz und weiterer Schutzoptionen.

- **Echtzeitschutz einschalten** steuert, ob Dateien gescannt werden, bevor auf sie zugegriffen wird oder sie ausgeführt werden.
- **Zugriffsenschutz aktivieren** sorgt dafür, dass Dateien sofort beim Zugriff überprüft werden.
- **Eingehende und ausgehende Dateien überwachen** kontrolliert den Netzwerkverkehr und prüft Dateien, die gesendet oder empfangen werden. Dies betrifft insbesondere Server, wie z.B. Dateiserver, bei denen du unter Umständen eine Richtung bevorzugen möchtest. Diese Auswirkungen sind jedoch gering, und es wird empfohlen, beide Richtungen zu überwachen.
- **Verhaltensüberwachung einschalten** sorgt dafür, dass die Antivirus-Engine Prozess-, Datei- und Registrierungsänderungen sowie andere Ereignisse auf verdächtige Aktivitäten hin überwacht.
- **Eindringsschutz einschalten** steuert, ob diese Funktion aktiviert oder deaktiviert ist.
- **Netzwerkschutz aktivieren** stellt sicher, dass Funktionen wie Web Threat Detection oder Content Filtering korrekt arbeiten. Wenn deaktiviert, funktionieren diese abhängigen Funktionen nicht.
- **Alle heruntergeladenen Dateien und Anhänge scannen** stellt sicher, dass alle Dateien nach dem Herunterladen automatisch gescannt werden - zusätzlich zu den Maßnahmen, die Defender SmartScreen bereits durchführt.
- **Skripte scannen, die in Microsoft Browsern verwendet werden**, sorgt dafür, dass Skripte (z.B. JavaScript) vor der clientseitigen Ausführung geprüft werden.
- **Netzwerkdateien scanne** ermöglicht das Scannen von Inhalten auf verbundene Netzwerklauferwerken. In Unternehmensnetzwerken ist dies unter Umständen nicht erwünscht, kann aber nützlich sein, wenn Benutzer Netzwerklauferwerke auch außerhalb des Unternehmens, z.B. zu Hause, verwenden dürfen.
- **E-Mails scannen** stellt sicher, dass alle Dateien geprüft werden, die von verschiedenen E-Mail-Clients zur Speicherung von Nachrichten verwendet werden. Beispiele sind PST-, DBX- und andere Dateitypen.

Die folgende Abbildung ist nur ein Beispiel dafür, wie die Echtzeitschutzeinstellungen konfiguriert werden können. Sie zeigt jedoch eine Konfiguration, die ich den meisten Kunden empfehle, da sie ein hohes Schutzniveau bietet.

Real-time protection

Turn on real-time protection ⓘ	Yes
Enable on access protection ⓘ	Yes
Monitoring for incoming and outgoing files ⓘ	Monitor all files
Turn on behavior monitoring ⓘ	Yes
Turn on intrusion prevention ⓘ	Yes
Enable network protection ⓘ	Enable
Scan all downloaded files and attachments ⓘ	Yes
Scan scripts that are used in Microsoft browsers ⓘ	Yes
Scan network files ⓘ	Yes
Scan emails ⓘ	Yes

Abbildung 7-32: Eine Beispielkonfiguration für die Echtzeitschutzeinstellungen von Defender Antivirus.

Behebung

In diesem Abschnitt konfigurierst du verschiedene Einstellungen, die festlegen, wie Defender Antivirus auf erkannte Bedrohungen reagiert.

- **Anzahl der Tage, die Malware in Quarantäne gehalten wird** bestimmt, wie lange du infizierte Dateien in Quarantäne behalten möchtest. Typischerweise sind 30 Tage ein guter Ausgangspunkt.
- **Probenübermittlung - Zustimmung** steuert, ob ein Benutzer manuell bestätigen muss, bevor eine verdächtige Datei zur Analyse an den Cloud-Service gesendet wird. Idealerweise ist die Einstellung so konfiguriert, dass alle Proben automatisch gesendet werden. Es kann jedoch regulatorische Anforderungen geben, die eine Zustimmung erforderlich machen. In solchen Fällen solltest du die Einstellung auf deaktiviert (**Keine**) oder **Immer nachfragen** setzen.
- **Aktion für PUA** bestimmt, wie Defender Antivirus mit einer Anwendung umgeht, die sich auf der PUA-Liste befindet. Wenn idealfall sollten diese blockiert werden. Wenn du die Funktion neu einführt, kann es sinnvoll sein, sie zunächst im Überwachungsmodus (Audit) zu aktivieren, um Auswirkungen vorab zu analysieren.

- **Aktionen für erkannte Bedrohungen** ermöglichen dir, je nach Bedrohungsgrad unterschiedliche Maßnahmen festzulegen. Wenn du keine abweichenden Aktionen konfigurieren möchtest – zumal dies nur für Windows 10 Endpunkte gilt – empfiehlt es sich, die Standardeinstellungen beizubehalten

Die folgende Abbildung zeigt die empfohlenen Einstellungen für die verschiedenen Reaktionsoptionen:

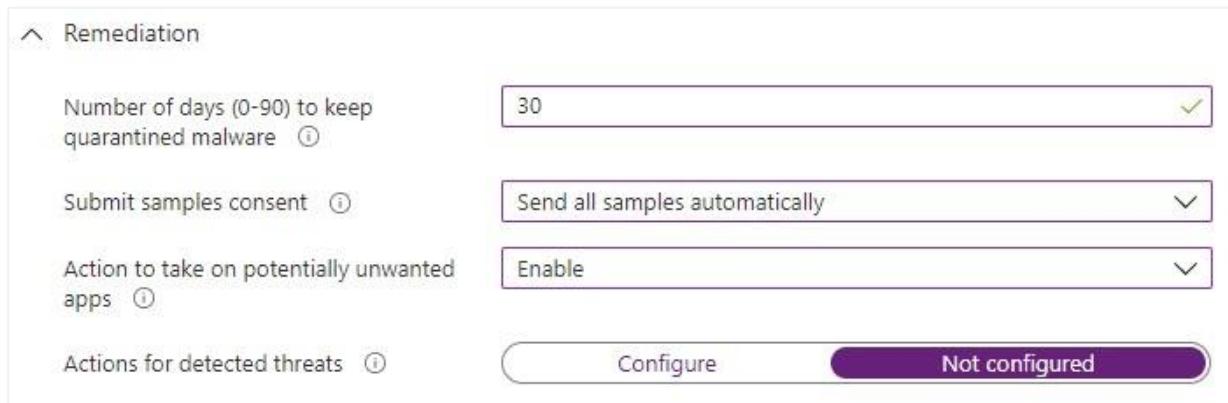


Abbildung 7-33: Eine Beispielkonfiguration für die Behebungseinstellungen von Defender Antivirus.

Scan

In diesem Abschnitt definierst du Einstellungen bezüglich der automatischen und bedarfsgesteuerten Scans von Defender Antivirus. Die folgende Abbildung zeigt die empfohlenen Einstellungen für eine ausgewogene Konfiguration zwischen Schutz und Leistung.

Scan

Scan archive files ⓘ	Yes
Use low CPU priority for scheduled scans ⓘ	Yes
Disable catch-up full scan ⓘ	No
Disable catch-up quick Scan ⓘ	No
CPU usage limit per scan ⓘ	25
Scan mapped network drives during full scan ⓘ	No
Run daily quick scan at ⓘ	11 AM
Scan type ⓘ	Quick scan
Day of week to run a scheduled scan ⓘ	Wednesday
Time of day to run a scheduled scan ⓘ	12 PM
Check for signature updates before running scan ⓘ	Yes

Abbildung 7-34: Eine Beispielkonfiguration für die geplanten Scan-Einstellungen von Defender Antivirus.

- **Archivdateien scannen** stellt sicher, dass Archive (wie ZIP-Dateien) und deren Inhalte während eines Scans einbezogen werden.
- **Niedrige CPU-Priorität verwenden** stellt sicher, dass die Auswirkungen auf Benutzer während eines Scans minimal gehalten werden.
- **Nachholenden Voll-/Schnellscan deaktivieren** definiert, ob Defender Antivirus einen verpassten Scan nachholen wird, zum Beispiel wenn das Gerät offline war. Wenn dies auf *Nein* gesetzt ist, wird ein Scan initiiert, sobald zwei aufeinanderfolgende Scan-Fenster verpasst wurden und das Gerät wieder online ist. Diese Einstellung gilt nur, wenn ein geplanter Scan konfiguriert ist - andernfalls wird es keine Nachholscans geben.
- **CPU-Nutzungslimit pro Scan** definiert, wie viel CPU-Leistung (in Prozent) Defender Antivirus maximal nutzen darf. Obwohl 50% der Standard ist, bin ich gerne vorsichtig bei Benutzerauswirkungen und setze dies auf 25%. Auf der anderen Seite kann dies dazu führen, dass Scans möglicherweise länger dauern.
- **Zugeordnete Netzwerklaufwerke während Vollscan scannen** ist typischerweise nicht notwendig, wenn der Zugriffscanner und bidirektionales Scannen von Dateien aktiviert ist und du einen VirensScanner auf deinen Dateiservers hast. Andererseits kann dies in Szenarien nützlich sein, in denen ein Gerät Laufwerke außerhalb des Unternehmensnetzwerks zuordnen darf, wie zu Hause.

- **Täglichen Schnellscan ausführen um** legt fest, zu welcher Uhrzeit ein täglicher Schnellscan ausgeführt werden soll.
- **Scan-Typ** definiert welcher geplante Scan ausgeführt werden soll. Da bereits ein täglicher Schnellscan konfiguriert ist, wird empfohlen, einen wöchentlichen Vollscan des Geräts durchzuführen.
- **Wochentag für geplanten Scan** bestimmt, an welchem Tag der geplante Scan ausgeführt werden soll.
- **Tageszeit für geplanten Scan** legt fest, zu welcher Uhrzeit der geplante Scan erfolgen soll.
- **Vor Scan nach Signaturupdates suchen** steuert, ob vor der Ausführung der geplanten Scans ein Signaturupdate versucht werden soll. Dies gilt nicht für bedarfsgesteuerte Scans über die Benutzeroberfläche des Clients.

Updates

In diesem Abschnitt definierst du, wie Updates von Defender Antivirus abgerufen werden. Dies betrifft Signatur- und Engine-Updates.

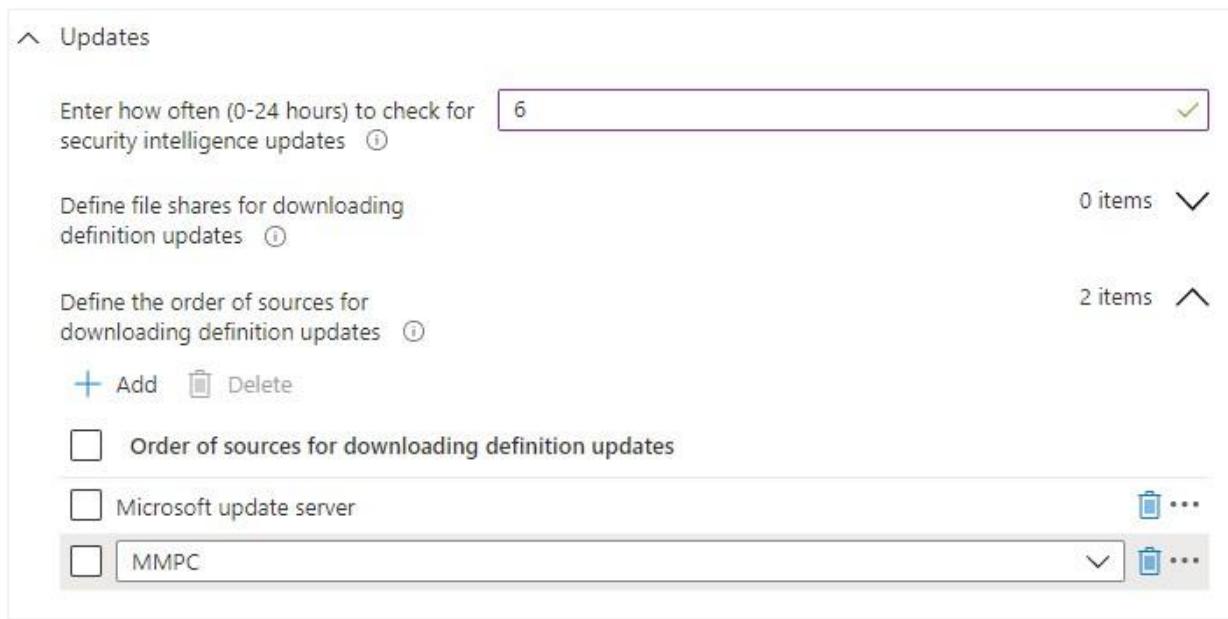


Abbildung 7-35: Eine Beispielkonfiguration für die Update-Einstellungen von Defender Antivirus.

In der obigen Abbildung haben wir Updates so konfiguriert, dass sie direkt vom Microsoft-Update-Server (Windows Update) abgerufen werden. Wenn das fehlschlägt, wird der Client auf das Microsoft Malware Protection Center (MMPC) zurückgreifen, welches der Verwaltungskanal für Defender Antivirus ist.

Je nachdem, wie Geräte in deiner Umgebung verwaltet werden, möchtest du möglicherweise alternative Updatequellen konfigurieren. Mögliche Alternativen sind:

- **Interner Definitionsupdateserver**, der sich auf einen internen WSUS-Server bezieht, falls einer verfügbar ist.
- **Dateifreigaben** funktioniert in Verbindung mit der Einstellung *Dateifreigaben für das Herunterladen von Definitionsupdates definieren* und weist einen Client an, Definitionsupdates von (einer) vordefinierten Dateifreigabe(n) abzurufen. Du würdest diese Einstellung normalerweise nicht verwenden, es sei denn, du hast Clients, die nicht mit dem Internet verbunden sind und keinen Zugriff auf einen internen Update-Server haben. Dies könnte in einer DMZ oder einer hochgesicherten Zone der Fall sein.

Benutzererfahrung

In diesem letzten Abschnitt steuerst du, ob ein Benutzer Zugriff auf die Microsoft-Defender-App in Windows hat. Die Tatsache, dass diese Einstellung in dieser Policy verfügbar ist, ist etwas seltsam, da es eine eigene Policy für die Benutzererfahrung gibt, die wir als Nächstes besprechen werden. Wenn deaktiviert, ist der Zugriff auf die Microsoft-Defender-Benutzeroberfläche deaktiviert und Benachrichtigungen werden unterdrückt; betrachte es als einen stillen Modus für Defender Antivirus.

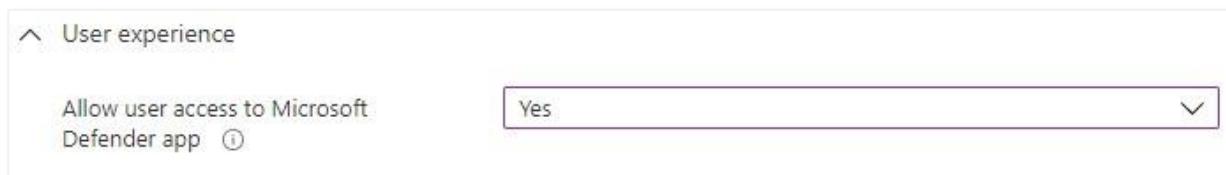


Abbildung 7-36: Eine Beispielkonfiguration für die Benutzererfahrungseinstellungen von Defender Antivirus.

Eine Windows Security Experience Policy konfigurieren

Wie bei der Antivirenpolicy wählst du bei der Erstellung eines neuen Profils „**Windows 10 und höher**“ als Plattform und „**Windows Security Experience**“ als Profiltyp aus und klickst dann auf **Erstellen**. Gib auf der Registerkarte *Grundlagen* einen Namen und eine Beschreibung für die Policy ein und klicke auf **Weiter**.

Anders als bei der Antivirenpolicy ist es schwierig, feste Empfehlungen für die meisten Einstellungen in dieser Policy zu geben, da dies von einer Umgebung zur anderen stark variieren kann. Das Einzige, was klar ist, ist, dass du *Manipulationsschutz aktivieren* solltest, da dies sicherstellt, dass ein lokaler Benutzer die Sicherheitskonfiguration von Defender auf dem lokalen Computer nicht manipulieren kann.

Die meisten Einstellungen steuern die Benutzererfahrung im Windows Security Center, wie in der folgenden Abbildung dargestellt.

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
No action needed.



Account protection
No action needed.



Firewall & network protection
No action needed.



App & browser control
No action needed.



Device security
View status and manage hardware security features



Device performance & health
No action needed.



Family options
Manage how your family uses their devices.

Abbildung 7-37: Windows Security Center Übersicht.

Welche Einstellungen du verwendest, hängt davon ab, welche Funktionen du aktiviert hast. Wenn du zum Beispiel keinen Kontoschutz (wie Windows Hello) konfiguriert hast, dann kann es sinnvoll sein, den Zugriff auf Kontoschutz in der Policy zu deaktivieren. Das Gleiche gilt für die anderen Funktionen.

Benachrichtigungen blockieren: Manchmal treffe ich auf Organisationen, die alle Benachrichtigungen von Microsoft Defender blockieren möchten, weil sie den Benutzer nicht stören wollen. Auch wenn ich die Überlegung verstehen kann, halte ich es immer noch für eine schlechte Idee. Aus Sicht der Benutzersensibilisierung bieten Benachrichtigungen - besonders wenn etwas Schädliches erkannt wird - einen großen Wert und eine Lernmöglichkeit.

Ausschlüsse verwalten

Ausschlüsse für Defender Antivirus werden entweder über die Antivirenpolicy oder über eine Ausschlusspolicy verwaltet. Die Regel hier ist einfach: Ausschlüsse, die breit für alle Geräte gelten sollen, die die Antivirenpolicy erhalten, gehören in diese Policy. Ausschlüsse, die nur für eine Teilmenge von Geräten gelten sollen, solltest du in einer separaten Ausschlusspolicy definieren, die zusätzlich zur Antivirenpolicy angewendet werden kann.

Nehmen wir zum Beispiel an, du hast einen Ordner „C:\App1“ auf jedem Windows-Gerät in deiner Umgebung. Da die Anwendung nicht richtig funktioniert, wenn die Datei von Defender gescannt wird, musst du sie vom Scannen ausschließen. Eine Teilmenge deiner Geräte hat auch eine andere App, „App2“, die das gleiche Problem hat, aber diese App läuft aus einem Ordner „C:\App2“.

Obwohl du sowohl C:\App1 als auch C:\App2 in die Ausschlussliste der Antivirenpolicy aufnehmen kannst, die auf alle deine Geräte angewendet wird, würde das bedeuten, dass du nicht existierende Ordner auf einigen Geräten ausschließt – was ein Angreifer ausnutzen könnte, um bösartige Dateien vor Defender Antivirus zu verstecken. Stattdessen ist es besser, C:\App1 von der Antivirenpolicy auszuschließen, während du eine neue Ausschlusspolicy erstellst, die nur C:\App2 enthält und nur auf die Gruppe von Geräten angewendet wird, die auch App2 installiert haben.

Kumulativ: Ausschlüsse werden kumulativ angewendet, aber nur wenn du sie über separate Ausschlusspolicies anwendest. Wenn du mehrere solcher Policies auf mehrere Geräte anwendest, werden alle Ausschlüsse im Geltungsbereich eines Geräts angewendet.

Vorsicht bei Platzhaltern: Versuche immer, Ausschlüsse so spezifisch wie möglich zu erstellen. Manchmal ist das allerdings nicht praktikabel, da die Liste der auszuschließenden Elemente zu umfangreich werden könnte. In solchen Fällen kannst du mit Platzhaltern arbeiten. Platzhalter, wie [hier](#) erläutert, werden von Endpoint Manager etwas bizarr ausgewertet. Zum Beispiel die Verwendung eines Sternchens, um eine einzelne Ordnerebene zu ersetzen, und nicht unbedingt Unterordner. Wenn du zum Beispiel C:\Folder1\Folder1.2\Folder1.2.1\data und C:\Folder1\Folder1.2\Folder1.2.2\data ausschließen möchtest, solltest du C:\Folder1*|*\data anstelle von C:\Folder1*\data verwenden.

Leistungsprobleme beheben

Manchmal beschweren sich Systemeigentümer, dass ihr System nach der Bereitstellung von Microsoft Defender for Endpoint langsamer läuft. Wenn das passiert, ist es wichtig, subjektive Eindrücke beiseitezulassen und die Ursache des Leistungsabfalls zu identifizieren. Microsoft stellt dafür den [Microsoft Defender Antivirus Performance Analyzer](#) zur Verfügung – eine Reihe von PowerShell-Befehlen, die ein Administrator ausführen kann. Führe zunächst den folgenden Befehl aus, um die Prozesse zu erfassen, die durch Microsoft Defender AV beeinflusst werden:

```
New-MpPerformanceRecording -RecordTo <path to .etl file>
```

Führe anschließend die Anwendungen aus, die angeblich unter Leistungseinbußen leiden, und prüfe, ob du das Problem reproduzieren kannst. Falls du das Problem nicht sofort reproduzieren kannst oder es sich um eine allgemeine Verlangsamung handelt, lasse das

System eine (kurze) Weile laufen. Sobald du sicher bist, dass du das Verhalten erfasst hast, drücke **STRG+C**, um die Aufzeichnung zu beenden.

Der zweite Schritt besteht darin, die Aufzeichnung mit dem folgenden Befehl zu analysieren:

```
Get-MpPerformanceReport -Path <path to .etl file>
```

Um irrelevante Informationen zu vermeiden, kannst du zusätzliche Parameter verwenden, um die Ergebnisse zu filtern. Mit dem folgenden Befehl erhältst du zum Beispiel die Top-10-Liste der Prozesse, die die Leistung beeinflussen:

```
Get-MpPerformanceReport -Path <path to .etl file> -TopProcesses 10
```

Für zusätzliche Filterparameter, schaue dir die [Dokumentation](#) an.

Ein Anfang: Leider kann die Ursachenanalyse bei Performanceproblemen zeitaufwendig sein. Auch wenn du gute Ansätze verfolgst, liefert der Performance Analyzer möglicherweise nicht die erhofften Ergebnisse oder ist nicht aussagekräftig genug. Unterschätze daher nicht den Wert anderer Tools wie ProcMon, perfmon und weitere Diagnosetools!

Netzwerk- & Webschutz

Im vorherigen Abschnitt haben wir den Netzwerkschutz in den Echtzeitschutzeinstellungen der Antiviren-Policy aktiviert. Wir haben jedoch das Konzept des Netzwerkschutzes und wie er sich auf andere Funktionen wie den Webschutz auswirkt, noch nicht erklärt.

Der Webschutz fasst Web Threat Protection, Web Content Filtering und zu einem gewissen Grad auch benutzerdefinierte Indikatoren zusammen, um einen umfassenden Satz von Funktionen zum Schutz des Webverkehrs bereitzustellen. Der Webschutz ist vollständig in Microsoft Windows integriert, genauer gesagt in Microsoft Edge. Nicht jeder verwendet jedoch Microsoft Edge zum Surfen im Internet. Um den vom Webschutz gebotenen Schutz auf Browser von Drittanbietern auszuweiten, nutzt der Webschutz im Hintergrund den Netzwerkschutz, um sicherzustellen, dass die gleiche Funktionalität auch in anderen Browsern wie z. B. Chrome oder Firefox verfügbar ist.

Während der Webschutz nativ in Microsoft Edge integriert ist, überwacht der Netzwerkschutz die Netzwerkkonnektivität auf Betriebssystemebene (winhttp) und gilt damit für alle anderen Anwendungen und Browser von Drittanbietern, die die Funktionalität des Betriebssystems selbst nutzen. Es ist der Mechanismus, mit dem Funktionen wie der Webschutz Bedrohungen erkennen und blockieren können, die typischerweise im Internet zu finden sind.

- Er blockiert Anwendungen den Zugriff auf Hosts und Websites, die als bösartig markiert wurden, wie Phishing-Wesites oder Seiten, die schädliche Inhalte wie Exploits oder

andere Malware hosten. Es ist eine Erweiterung von SmartScreen und blockiert jeden HTTP(s)-Verkehr zu Quellen mit niedriger Reputation. Beachte, dass nur Verbindungen basierend auf dem Domain- oder Hostnamen blockiert.

- Er unterstützt die Webschutzfunktionen, indem er sie auf die Betriebssystemebene erweitert und somit auf andere unterstützte Browser und Anwendungen ausdehnt.
- Er bietet Einblicke in und die Möglichkeit zum Blockieren von benutzerdefinierten Kompromittierungsindikatoren (IOCs), die später in diesem Kapitel ebenfalls besprochen werden.
- Er hilft beim Erkennen und Blockieren von Command-and-Control (C2) Kommunikation, die häufig während Angriffen beobachtet wird und für verschiedene Aktionen verwendet wird - wie das Stehlen von Daten und/oder das Ausgeben neuer Befehle an die persistente Malware, die in der Umgebung aktiv ist. Durch solche Kommunikation können Angreifer verschiedene Aufgaben ausführen, wie das Bereitstellen neuer Malware, das Durchführen zusätzlicher Aufklärung innerhalb der Umgebung oder das Starten eines umfassenden Ransomware-Angriffs und so weiter.

Linux & macOS in Vorschau: Netzwerkschutzfunktionen für Linux und macOS sind derzeit in der Vorschau. Um dies zu nutzen, müssen deine Geräte einem Vorschaukanal der Software zugewiesen sein. Je nachdem, wie du Microsoft Defender for Endpoint bereitgestellt hast, kannst du den Release-Kanal entweder manuell oder über dein bevorzugtes Verwaltungstool umschalten. In seiner ersten Version wird der Netzwerkschutz für diese Betriebssysteme Web Threat Protection, Web Content Filtering und benutzerdefinierte IP/URL-Indikatoren unterstützen und den Zugriff auf verdächtige oder gefilterte Websites blockieren.

Netzwerkschutz Voraussetzungen

In vorherigen Abschnitten haben wir gezeigt, wie du den Netzwerkschutz über die Antiviren-Policy aktivierst. Während das in der Tat der Weg ist, die Funktion zu aktivieren, beachte die folgenden Voraussetzungen, bevor Funktionen wie die Erkennung von C2-Kommunikation verfügbar sind:

1. Das Gerät muss Windows 10, Windows 11, Windows Server 1803 oder Windows Server 2019 ausführen.
2. Microsoft Defender Antivirus muss Echtzeit- und cloudbasierten Schutz aktiviert haben und *aktiv* sein. Der passive Modus wird nicht unterstützt.
3. Die Defender Engine-Version muss mindestens 1.1.17300.4 sein. Wenn du ein aktuelles Betriebssystem hast, sollte dies auf jeden Fall der Fall sein.

SmartScreen

Webschutz und Netzwerkschutz werden beide vom SmartScreen-Service angetrieben, der dafür verantwortlich ist zu bewerten, ob eine Website oder ein Host potenziell schädlich ist oder nicht.

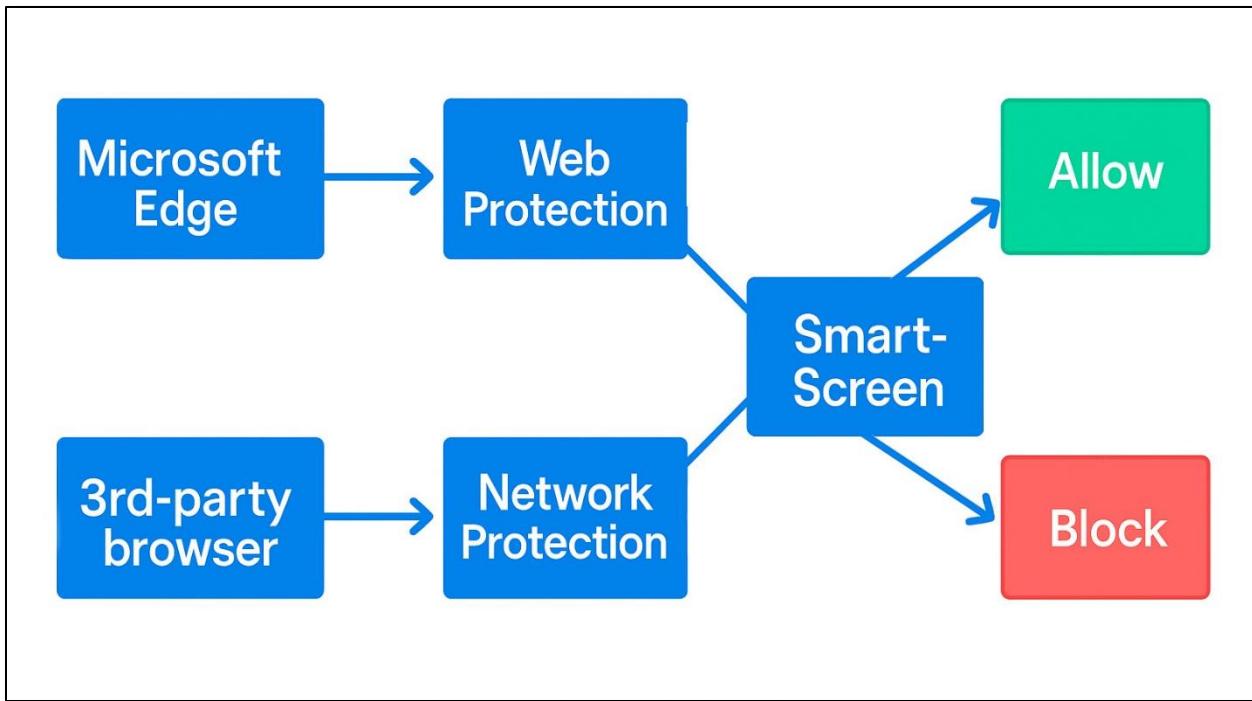


Abbildung 7-38: Beziehung zwischen Webschutz, Netzwerkschutz und SmartScreen.

Web Threat Protection

Web Threat Protection nutzt den Netzwerkschutz, um seinen Schutz gegen verschiedene Webbedrohungen bereitzustellen. Es integriert sich mit Microsoft Edge und Browsern von Drittanbietern wie Chrome oder Firefox und hindert Benutzer daran, auf schädliche Websites zuzugreifen – ganz ohne den Einsatz eines sicheren Web-Gateways (Proxys). Dadurch kann es Schutz für Geräte garantieren, unabhängig von ihrem Netzwerkstandort.

Um Web Threat Protection zu konfigurieren, öffne das Endpoint Manager Admin Center und navigiere zu **Endpoint Security > Attack surface reduction**. Klicke von dort aus auf **Policy erstellen**. Wähle **Windows 10 und höher** als Plattform und **Webschutz (Microsoft Edge Legacy)** als Profiltyp.

Konfiguriere als Nächstes die Einstellungen wie in der folgenden Abbildung dargestellt.

Web Protection (Microsoft Edge Legacy)

Enable network protection ⓘ	Enable
Require SmartScreen for Microsoft Edge Legacy ⓘ	Yes Not configured
Block malicious site access ⓘ	Yes Not configured
Block unverified file download ⓘ	Yes Not configured

Abbildung 7-39: Konfigurieren des Webschutzes

Web Content Filtering

Wie der Name schon sagt, ermöglicht diese Funktion Administratoren, den Zugriff auf Websites basierend auf ihrem Inhalt zu kontrollieren. Wenn eine Website blockiert wird, sehen Benutzer eine entsprechende Warnung im Browser. Websites, die nicht vom Inhaltsfilter markiert sind, können ohne Unterbrechung geöffnet werden – wobei jedes Element auf der Webseite, das Aufrufe an Seiten in einer blockierten Kategorie macht, möglicherweise dennoch blockiert wird. Ein Beispiel dafür ist in der folgenden Abbildung dargestellt:

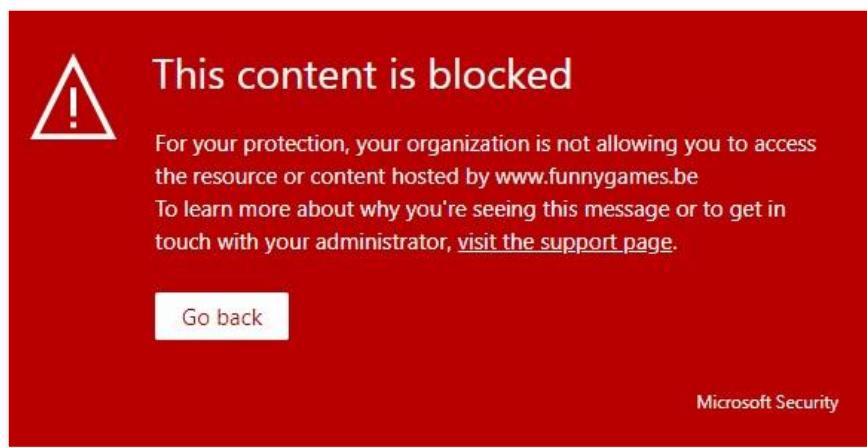


Abbildung 7-40: SmartScreen-Urteil im Windows Explorer überschreiben.

Zum Zeitpunkt der Erstellung ist Web Content Filtering auf den meisten gängigen Browsern verfügbar, einschließlich Microsoft Edge, Chrome, Firefox, Brave und Opera.

Geduld: Wenn du den Content Filter aktivierst oder Änderungen an einer Policy vornimmst, kann es eine kurze Weile dauern, bis deine Endpunkte die aktualisierte Konfiguration erhalten.

In der Regel dauert das nur ein paar Minuten. In meiner Erfahrung war dies innerhalb von zehn bis fünfzehn Minuten nach dem Vornehmen der Änderungen.

Web Content Filtering konfigurieren

Anders als die meisten anderen Policies wird Web Content Filtering nicht über Microsoft Intune verwaltet. Stattdessen werden die Policies über das **Microsoft 365 Security Center > Einstellungen > Endpoints > Web content filtering** erstellt. Klicke auf dieser Seite auf **Element hinzufügen**, um eine neue Policy zu erstellen:

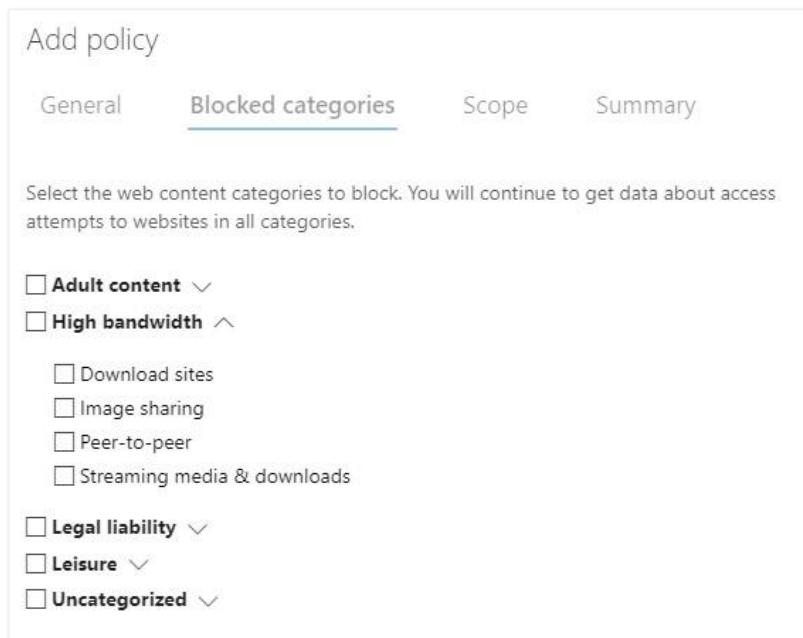


Abbildung 7-41: Eine Web Content Filtering Policy konfigurieren.

Die Seite **Blockierte Kategorien** ist der Ort, an dem du konfigurierst, welche Kategorien oder Unterkategorien blockiert werden sollen. Verfügbare Kategorien sind:

- **Erwachseneninhalt** - umfasst alle Arten von Erwachseneninhalten, von Gewalt bis über Nacktheit bis hin zu sexuell expliziten Inhalten wie Pornografie.
- **Hohe Bandbreite** - gruppiert Download- und Filesharing-Websites, Streaming-Medien und andere ähnliche Plattformen gruppiert.
- **Rechtliche Haftung** - betrifft Websites, die Inhalte hosten könnten, die je nach Land oder Region als rechtswidrig gelten. Diese Kategorie umfasst Websites über Hacking, Hassrede, Betrug, illegale Waren und Drogen sowie andere potenziell kriminelle Aktivitäten.
- **Freizeit** - umfasst Spiele, professionelle und soziale Netzwerke, webbasierte E-Mail-Plattformen usw.
- **Nicht kategorisiert** - bezieht sich auf neu registrierte Domains und geparkte Domains.

Interessant: Die Kategorie *Nicht kategorisiert* ist besonders interessant, da sie die Unterkategorien *Neu registrierte Domains* und *Geparkte Domains* enthält. Neu registrierte Domains können nützlich sein, um Domainnamen zu blockieren, die während eines gezielten Angriffs registriert werden. Es ist nicht ungewöhnlich, dass böswillige Akteure einen neuen Domainnamen registrieren, um einen Angriff auf eine Organisation durchzuführen - zum Beispiel indem sie eine Domain registrieren, die so aussieht, als gehöre sie zur Organisation oder einer anderen bekannten Domain sehr ähnlich ist. Ein solches Beispiel, das wir beobachtet haben, ist ein Angreifer, der "Eventbrlte" als seinen Domainnamen verwendete, anstelle der legitimen "Eventbrite" Domain.

Ausnahmen verwalten

Web Content Filtering Policies werden entweder auf alle Geräte oder pro Gerätegruppe angewendet. Leider erlaubt die Policy nicht, einzelne URLs zur Liste der zu blockierenden Domains hinzuzufügen, noch kannst du Ausnahmen innerhalb der Policy selbst definieren. Der einzige Weg, bestimmte Domains und URLs zu blockieren oder freizugeben, ist, sie als erlaubten Indikator hinzuzufügen. Dies überschreibt die in jeder anderen Policy definierte Aktion, etwa eine Web Content Filtering Policy.

Kompromittierungsindikatoren und wie du sie erstellst, werden später in diesem Kapitel ausführlicher behandelt.

C2-Kommunikation erkennen

Mit aktiviertem Netzwerkschutz kann Microsoft Defender for Endpoint verschiedene Arten von böswilliger Kommunikation erkennen – einschließlich Command-and-Control-Kommunikation. Beachte jedoch, dass du dich nicht ausschließlich auf Microsoft Defender for Endpoint für diese Art von Kommunikation verlassen solltest. Das Erkennen von C2-Kommunikation ist extrem schwierig, und es gibt keine Garantie, dass Defender for Endpoint alle C2-Kommunikationen erkennen wird.

Wenn es jedoch gelingt, wirst du einen Vorfall bemerken, der im Microsoft 365 Defender Admin Center ausgelöst wird – wie in der folgenden Abbildung dargestellt.

Incidents > Command and Control behavior was blocked on one endpoint

Command and Control behavior wa...

Manage incident Ask Defender Experts Comments and history

Attack story Alerts (1) Devices (1) Users (1) Mailboxes (0) Apps (0) Investigations (0) Evidence and Response (1) Summary

Alerts < >

1/1 Active alerts Unpin all Show all Incident graph Layout Group similar nodes

Jan 2, 2023 9:22 AM • New
Command and Control behavior was blocked

"powershell.exe"

MichaelVanHorenbeek

Command and Control behavior was blocked on one endpoint
Low Active

Manage incident

Incident details

Assigned to	Incident ID
Unassigned	
Classification	Categories
Not set	Command and control
First activity	Last activity
Jan 2, 2023 9:22:25 AM	Jan 2, 2023 9:22:25 AM

Abbildung 7-42: C2-Kommunikation mit Microsoft Defender for Endpoint untersuchen

Zeek und Microsoft Defender for Endpoint

Microsoft Defender for Endpoint ist eine Endpoint Detection and Response (EDR) Lösung, während Network Detection and Response (NDR) Lösungen Netzwerksignale nutzen, um ähnliche Funktionalität anzubieten. Zeek ist eine weit verbreitete Open-Source-Netzwerksicherheitsüberwachungslösung, die Informationen aus Netzwerk-Packet-Captures erfasst und analysiert, um verdächtiges oder böswilliges Verhalten zu erkennen.

Um die Netzwerkschutzfähigkeiten in Microsoft Defender for Endpoint zu verbessern, hat Microsoft Zeek in seinen Agenten integriert. Diese Integration erfasst zusätzliche Netzwerkverkehrsinformationen, die zur Analyse an Microsofts Cloud gesendet werden. Dadurch wird eine verbesserte Erkennung von Angriffstechniken und Mustern wie Command-and-Control-Kommunikation, PrintNightmare-Ausnutzung, Passwort-Spray-Angriffen und mehr ermöglicht.

Während sich diese Funktion noch in den Anfängen befindet, werden zukünftige Vorteile erwartet – einschließlich der Möglichkeit, dass Advanced Hunting die erfassten Informationen anzeigt. Organisationen können auch eigene Erkennungen mit den offengelegten Informationen aufbauen, ohne Zeek in ihrer Umgebung bereitstellen zu müssen.

Attack Surface Reduction

In Kapitel 1 haben wir erwähnt, dass eine umfassende und effektive Sicherheitsstrategie aus vielen Schichten besteht und sich auf verschiedene Aktivitäten konzentriert – wobei Defender for Endpoint hilft, eine Vielzahl von Bedrohungen zu identifizieren, zu schützen, zu erkennen und darauf zu reagieren, denen du begegnen könntest. Bisher haben wir bereits besprochen, wie Defender Antivirus hilft, deine Assets zu schützen, und wie die EDR-Fähigkeiten es dir ermöglichen, Bedrohungen zu erkennen, die aktiv sein könnten.

Ein weiterer wichtiger Aspekt der Cybersicherheit ist das Prinzip der Attack Surface Reduction – wobei du versuchst, die Exposition deiner Systeme so weit wie möglich zu begrenzen, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu verringern. Als solches ist die Reduzierung der Angriffsfläche viel mehr als nur, einen Antivirus zu aktivieren. Es geht darum, sicherzustellen, dass böswillige Aktivitäten nicht ausgeführt werden können, dass Geräte mit den neuesten Sicherheitsupdates ausgestattet sind, dass nur die Aktionen möglich sind, die wirklich erforderlich sind – und so weiter.

Innerhalb von Microsoft Defender for Endpoint besteht Attack Surface Reduction aus mehreren Funktionen, die genau das tun: die Angriffsfläche eines Geräts auf verschiedenen Ebenen reduzieren. In den folgenden Abschnitten wirst du etwas tiefer in jede dieser Funktionen eintauchen.

Ein wenig verwirrend: Manchmal frage ich mich, wie und warum einige Produkte- oder Funktionsnamen gewählt werden. Nimm zum Beispiel *Attack Surface Reduction*. Es ist nicht nur ein Kernprinzip in der Cybersicherheit, sondern auch eine Funktion innerhalb von Microsoft Defender – nämlich die *Attack Surface Reduction Rules*, die ebenfalls darauf abzielen, die Angriffsfläche zu reduzieren. Aber das auch andere Funktionen wie Application Control verfolgen dasselbe Ziel. Obwohl das nicht unbedingt ein Problem ist, kann es etwas verwirrend sein, wenn du dich mit anderen Leuten über die Funktionen unterhältst.

Attack Surface Reduction Rules

Die ersten und wahrscheinlich am einfachsten zu implementierenden Funktionen sind die Attack Surface Reduction Rules. Diese Regeln zielen darauf ab, spezifische Aktivitäten zu verhindern, die häufig bei verschiedenen Arten von Angriffen verwendet werden – zum Beispiel, wenn eine Anwendung versucht, den LSASS-Prozess zu dumpen, Microsoft Office-Anwendungen versuchen, einen anderen Prozess zu starten, oder ein Skript versucht, eine andere Anwendung (ausführbare Datei) zu starten.

Attack Surface Reduction Rules sind nur für Geräte verfügbar, die Windows 10 oder Windows Server 2019 (einschließlich der Semi-Annual Channel-Version) ausführen. Um sie zu verwenden, brauchst du auch nicht zwingend eine Windows E5- oder Defender-for-Endpoint-Lizenz, da sie

eine Kernfunktion von Windows sind. Mit der E5- oder Defender-Lizenz erhältst du jedoch zusätzliche Berichtsfunktionen, die – wie du noch lernen wirst – während der Bereitstellung nützlich sein können.

Kein Allheilmittel: Das Versprechen von Attack Surface Reduction Rules ist großartig: typische böswillige Aktivitäten von vornherein zu verhindern. Wie du noch sehen wirst, gibt es dabei allerdings einige Vorbehalte. Erstens existieren viele schlecht geschriebene Anwendungen, die du möglicherweise von der einen oder anderen Regel ausschließen musst. Ausschlüsse zu erstellen bedeutet aber immer auch, neue Angriffsflächen zu schaffen. Zweitens scheint Microsoft einige interne Ausschlüsse eingebaut hat, die - wenn richtig ausgenutzt - bestimmte ASR-Regeln umgehen könnten. Für weitere Informationen, schaue [hier](#).

Derzeit gibt es etwa siebzehn verschiedene Attack Surface Reduction Rules, die du aktivieren kannst. Die folgende Tabelle bietet dir einen Überblick über alle. Controlled Folder Access ist in dieser Tabelle nicht enthalten, da er später in einem eigenen Abschnitt behandelt wird.

Name	Zweck
Missbrauch ausgenutzter, verwundbarer signierter Treiber blockieren	Verhindert, dass eine Anwendung einen verwundbaren Treiber auf die Festplatte schreibt. Treiber haben in der Regel hohe Privilegien bis hin zum Kernel und können so erheblichen Schaden anrichten (z. B. PrintNightmare).
Adobe Reader daran hindern, Tochterprozesse zu erstellen	Verhindert, dass Adobe Acrobat Reader beim Öffnen einer manipulierten PDF-Datei neue Prozesse startet.
Alle Office-Anwendungen daran hindern, Tochterprozesse zu erstellen	Verhindert, dass Office-Anwendungen (Word, Excel, PowerPoint, OneNote, Access) durch Makros oder andere Techniken neue Prozesse starten.
Credential-Stealing aus LSASS blockieren	LSASS (Local Security Authority Subsystem) authentifiziert Anmeldungen. Diese Regel verhindert das Auslesen von Anmeldeinformationen aus dem Prozess, wenn Credential Guard nicht verfügbar ist.
Ausführen von ausführbarem Inhalt aus E-Mail-Clients/webmail blockieren	Verhindert, dass Anwendungen oder Skripte direkt aus einer E-Mail (Outlook oder Outlook Web) gestartet werden.
Ausführen von ausführbaren Dateien verhindern, sofern nicht vertraulich	Verhindert das Ausführen seltener Programme, die bestimmte Kriterien (Verbreitung > 1000 Geräte, älter als 24 Stunden, vertrauenswürdige Speicherorte) nicht erfüllen.
Ausführung potenziell obfuscierter Skripts blockieren	Stoppt Skripte mit verschleiertem Code (JavaScript, VBScript, PowerShell, Office-Makros).

Name	Zweck
JavaScript/VBScript am Starten heruntergeladener Executables hindern	Verhindert, dass über Skripte vorinstallierter JavaScript/VBScript schädlicher Code nachgeladen und ausgeführt wird.
Office-Anwendungen am Erstellen ausführbarer Dateien hindern	Verhindert, dass Makros oder andere Office-Komponenten ausführbare Dateien auf der Festplatte ablegen (Persistenz-Technik).
Office-Anwendungen am Injizieren von Code in andere Prozesse hindern	Verhindert, dass Office-Makros Code in fremde Prozesse injizieren, eine häufige Angriffstechnik.
Outlook am Erstellen von Tochterprozessen hindern	Blockiert in Outlook den Start unbekannter Kindprozesse (z. B. schädliche Anhänge). Hinweis: Policy Tips in Outlook funktionieren dann nicht mehr.
Persistenz via WMI-Ereignisabonnements blockieren	Verhindert, dass Code über WMI-Events persistent auf dem Gerät bleibt (z. B. fileless Malware).
Prozesserzeugung durch PSExec/WMI-Kommandos blockieren	Verhindert das Starten von Prozessen über PSExec oder WMI. (Legitime Nutzung durch Configuration Manager möglich.)
Untrusted/unsigned Prozesse von USB blockieren	Verhindert das Ausführen nicht signierter oder nicht vertrauenswürdiger Programme von USB-Sticks oder SD-Karten.
Win32-API-Aufrufe aus Office-Makros blockieren	Verhindert, dass Makros Win32-APIs aufrufen (Fileless-Technik), um schädlichen Code im Speicher auszuführen.
Erweiterten Ransomware-Schutz verwenden	Fügt über Defender hinaus eine zusätzliche Analyse-Ebene hinzu und blockiert verdächtige Dateien. Vorher als sicher eingestufte, signierte oder weit verbreitete Dateien werden nicht blockiert.

Tabelle 7-2: Übersicht der Attack Surface Reduction Rules

Bereitstellen von ASR Rules

Angesichts der Vielzahl an Methoden, die Angreifer verwenden können, um ein Gerät zu kompromittieren, ist es nur logisch, dass du jede Regel aktivieren möchtest, um es einem Angreifer so schwer wie möglich zu machen. Leider ist das nicht immer möglich, da auch gutartige und legitime Anwendungen die oben genannten Aktivitäten nutzen können, um ordnungsgemäß zu funktionieren. Ein gängiges Beispiel zur Veranschaulichung: Microsoft

Configuration Manager nutzt WMI, um Remote-Geräte zu verwalten. Die Regel „Prozesserstellungen blockieren, die von PSEXEC und WMI-Befehlen ausgehen“ würde, wenn aktiviert, den Configuration Manager Client stören und daran hindern, korrekt zu funktionieren. Wenn du also Deine Umgebung über Configuration Manager verwaltetest, kannst du diese Regel nicht im Blockierungsmodus aktivieren und musst nach Alternativen suchen.

Letztendlich kann es viele legitime Gründe geben, warum eine Anwendung eine Aktivität durchführt, die verdächtig erscheint, es aber nicht ist. Daher ist es keine gute Idee, von Anfang an jede Attack Surface Reduction Rule im Blockierungsmodus zu konfigurieren. Stattdessen wird empfohlen, alle Regeln – wenn möglich – zunächst im Überwachungsmodus zu konfigurieren und die Berichtsfunktionen zu nutzen, um die Auswirkungen jeder Regel auf deine Umgebung zu bewerten. Sobald du das Gefühl hast, dass eine Regel wenig bis gar keinen Einfluss hat, zum Beispiel weil du die notwendigen Ausschlüsse konfiguriert hast, kannst du sie so konfigurieren, dass die entsprechenden Aktivitäten blockiert werden.

Es gibt immer Ausnahmen: Obwohl die Empfehlung ist, mit Vorsicht vorzugehen, existieren auch hier klare Fälle, in denen sofortiges Blockieren sinnvoll ist. Zum Beispiel gibt es keine guten Gründe, warum eine Office-Anwendung Code in einen anderen Prozess injizieren sollte. Daher ist es durchaus sinnvoll, diese Regel von Anfang an im Blockierungsmodus zu konfigurieren. Aber man kann nie zu sicher sein. Es liegt also an dir zu entscheiden, ob du sie von Anfang an blockieren möchtest oder sie zuerst im Überwachungsmodus konfigurierst...

Attack Surface Reduction Rules haben eine eigene Richtlinie (Profiltyp), die über Microsoft Endpoint Manager konfiguriert wird. Obwohl du auch Gruppenrichtlinien, Configuration Manager und PowerShell verwenden kannst, um die Regeln bereitzustellen und zu konfigurieren, werden diese Optionen hier nicht behandelt.

Eine ASR Rule Richtlinie erstellen

Öffne das Microsoft Endpoint Manager Portal und navigiere zu **Endpunktssicherheit > Attack Surface Reduction**. Klicke dann auf „**Richtlinie erstellen**“. Wähle „**Windows 10 und höher**“ als Plattform und „**Attack Surface Reduction Rules**“ als Profiltyp aus. Nach der Eingabe eines Namens und einer Beschreibung gehst du weiter zu den **Konfigurationseinstellungen**, wo Du die verschiedenen Regeln konfigurieren kannst.

Je nach Regel stehen folgende Optionen zur Verfügung. Beachte, dass nicht alle Regeln jede dieser Aktionen unterstützen:

- **Blockieren:** Blockiert die Aktivität, wenn sie erkannt wird.
- **Überwachungsmodus:** Fügt einen Eintrag zu den Windows-Ereignisprotokollen hinzu und erscheint in den Berichten in Defender for Endpoint.
- **Deaktivieren:** Deaktiviert die Regel. Übereinstimmende Aktivitäten sind ohne spezifische Protokollierung erlaubt.

- **Warnen:** Eine Hybrid-Option zwischen Blockieren und Überwachen. Immer wenn eine Aktivität blockiert wird, erhält der Benutzer eine entsprechende Benachrichtigung. Er kann dann auch wählen, die Blockierung zu umgehen und die Aktivität dennoch zuzulassen. Diese wird dann für 24 Stunden freigegeben. Diese Option ist ideal, wenn du eine Funktion schnell ausrollen möchtest, aber Benutzer nicht unbedingt bei ihrer Arbeit einschränken möchtest.

Attack Surface Reduction Rules

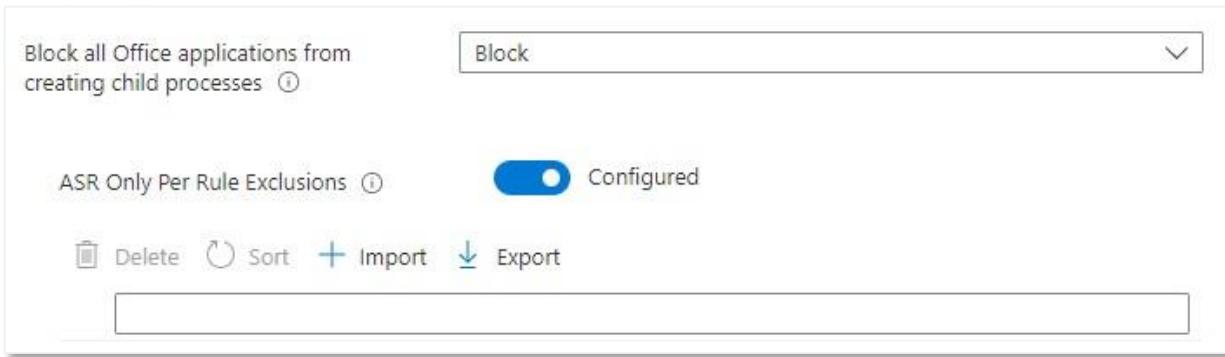
Block persistence through WMI event subscription	Not configured
Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ	Not configured
Block Adobe Reader from creating child processes ⓘ	User defined
Block Office applications from injecting code into other processes ⓘ	Enable
Block Office applications from creating executable content ⓘ	Audit mode
	Warn
	Not configured

Abbildung 7-43: Konfigurieren der Regeln zur Reduzierung der Angriffsfläche

Verwalten von Ausnahmen/Ausschlüssen

Ende 2022 hat Microsoft die Möglichkeit eingeführt, Ausschlüsse pro Attack Surface Reduction Rule zu konfigurieren. Zuvor war es nur möglich, Ausschlüsse global festzulegen. Wie du dir vorstellen kannst, war das keine besonders wünschenswerte Situation – denn ein Prozess, der von einer Regel ausgeschlossen wird, sollte nicht automatisch auch bei anderen ausgeschlossen sein.

Um einen Ausschluss pro Regel zu konfigurieren, führe die folgenden Schritte aus: Navigiere im Endpoint Manager Admin Center zu **Endpunktsicherheit**, öffne die Richtlinie für Attack Surface Reduction Rules und bearbeite die Konfigurationseinstellungen. Dort siehst du für jede Regel die Option „**ASR Only per Rule Exclusions**“.

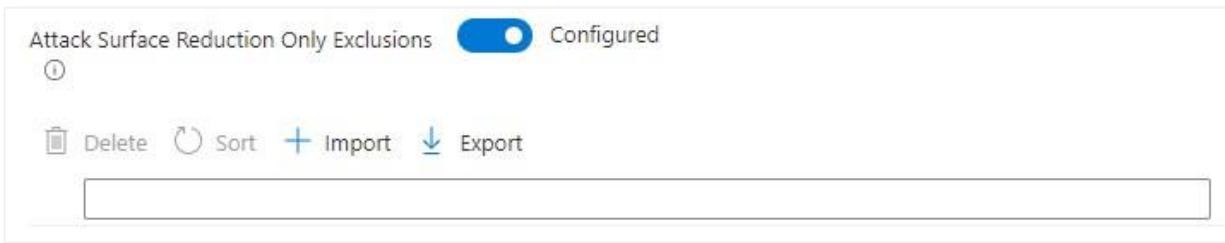


The screenshot shows the configuration of an Attack Surface Reduction (ASR) rule exclusion. At the top, there is a dropdown menu set to "Block". Below it, a toggle switch is labeled "Configured". A section titled "ASR Only Per Rule Exclusions" contains a note with a help icon. At the bottom, there are buttons for "Delete", "Sort", "Import", and "Export".

Abbildung 7-44: Konfigurieren eines Ausschlusses pro Attack Surface Reduction Rule

Einträge in der Ausschlussliste können Wildcards enthalten. Wichtig ist, dass diese Wildcards auf die gleiche Weise verarbeitet werden wie bei der Antiviren-Richtlinie. Weitere Informationen dazu findest du in den vorherigen Abschnitten.

Wenn du möchtest, hast du auch die Möglichkeit, einen globalen Ausschluss zu konfigurieren. Dadurch wird sichergestellt, dass die Datei oder der Prozess, den du ausschließt, automatisch bei allen Regeln berücksichtigt wird. Um diesen Ausschluss zu konfigurieren, navigiere zum Ende der Einstellungen und suche nach der entsprechenden Option:



The screenshot shows the configuration of a global ASR rule exclusion. It features a dropdown menu set to "Configured", a toggle switch also set to "Configured", and a section titled "Attack Surface Reduction Only Exclusions". At the bottom, there are buttons for "Delete", "Sort", "Import", and "Export".

Abbildung 7-45: Konfigurieren eines globalen Ausschlusses für Attack Surface Reduction Rules

Ähnlich wie beim Konfigurieren eines regelspezifischen Ausschlusses fügst du die entsprechenden Elemente hinzu, die du ausschließen möchtest, und speicherst anschließend die Richtlinie.

Berichterstattung

Sobald du deine Attack Surface Reduction Rules konfiguriert hast – insbesondere im Überwachungsmodus – möchtest du nachvollziehen können, welche Aktivitäten blockiert worden wären, bevor du entscheidest, eine Regel im Blockierungsmodus zu aktivieren. Ohne Defender for Endpoint stehen dir dafür nur die Windows-Ereignisprotokolle zur Verfügung. Konkret gibt es drei Ereignisse, die dabei von Interesse sind:

- **Ereignis-ID 5007** wird protokolliert, wenn eine Änderung an der ASR-Konfiguration vorgenommen wird.
- **Ereignis-ID 11xx** wird protokolliert, wenn eine Aktivität blockiert oder überwacht wird. Die Ereignis-ID hängt von der ASR Rule selbst ab.

Defender for Endpoint macht die Berichterstattung zu ASR deutlich einfacher, da du die Ereignisprotokolle nicht selbst sammeln und manuell durchsuchen musst. Stattdessen kannst du die integrierten Berichte sowie das Threat and Vulnerability Management nutzen, um den Status deiner Umgebung im Blick zu behalten. Weitere Informationen zum Schwachstellen-Management findest du später in diesem Kapitel.

Um auf die Berichte zuzugreifen, öffne das Microsoft 365 Security Center und navigiere zu **Berichte > Attack Surface Reduction Rules**. Auf dieser Seite findest du verschiedene Informationen zu ASR.

Zunächst gibt es eine Übersicht darüber, wie häufig eine Regel in deiner Umgebung ausgelöst wurde. Dies ist in Abbildung 7-46 unten zu sehen. Die Grafik und die darunterliegenden Tabellen geben einen detaillierten Überblick darüber, welche Regeln übereinstimmende Aktivitäten erkannt haben, auf welchen Geräten dies geschah und welche Aktionen dabei durchgeführt wurden (Blockiert/Überwacht).

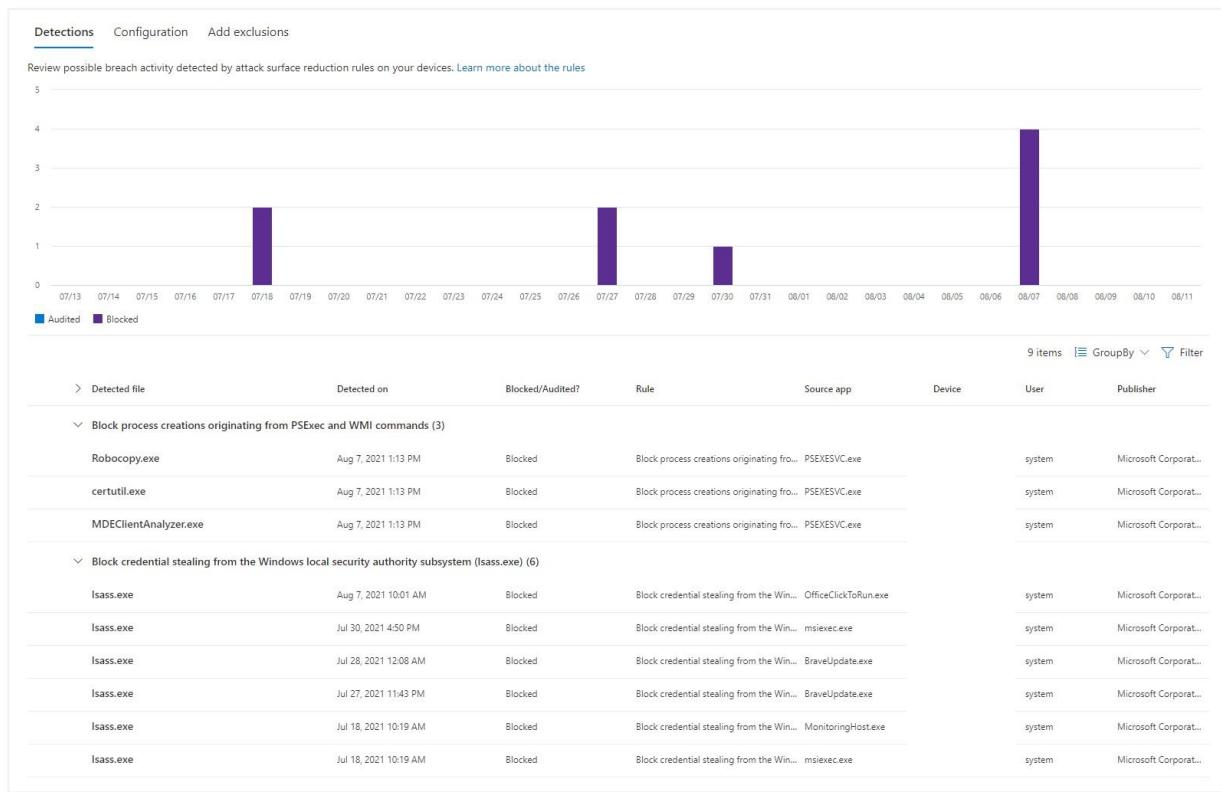


Abbildung 7-46: Überprüfung der Attack Surface Reduction Erkennungen.

Wenn du von den **Erkennungen** zur Registerkarte **Konfiguration** wechselst, siehst du eine Übersicht über die Geräte in deiner Umgebung sowie weitere Informationen darüber, wie viele Regeln konfiguriert wurden, wie sie konfiguriert sind oder ob sie deaktiviert wurden. Wenn du auf eines der Geräte klickst, erscheint auf der rechten Seite des Bildschirms eine Auswahl mit den Detailinformationen zu diesem Gerät. Beachte, dass im Bild nur eine Teilmenge der Regeln angezeigt wird:



The screenshot shows a table titled "Configuration details of attack surface reduction rules on this device". The table has two columns: "Rule" and "Status". There are seven rows of data:

Rule	Status
Block executable content from email client and webmail	Block
Block all Office applications from creating child processes	Block
Block Office applications from creating executable content	Block
Block Office applications from injecting code into other processes	Block
Block JavaScript or VBScript from launching downloaded executable cont...	Block
Block execution of potentially obfuscated scripts	Block
Block Win32 API calls from Office macro	Block
Block executable files from running unless they meet a prevalence, age, or...	Audit

Abbildung 7-47: Überprüfung der Konfiguration der Attack Surface Reduction Rule eines Geräts

Zusätzlich gibt es die Registerkarte **Ausschlüsse hinzufügen**, die dir eine Übersicht über Dateien und Prozesse bietet, die mit einer der Attack Surface Reduction Rules übereingestimmt haben, wie oft sie erkannt wurden und wie viele Geräte betroffen waren. Durch einen Klick auf den Dateinamen wird auf der rechten Seite des Bildschirms eine Detailansicht geöffnet. Dort findest du weitere Informationen sowie die Möglichkeit, den Pfad abzurufen, den du für einen Ausschluss dieser Datei oder dieses Prozesses konfigurieren solltest.

Zusätzlicher Datenpunkt: Beachte, dass die Informationen auf der Registerkarte **Ausschlüsse** nur ein Hinweis sind, den du in deine Überlegungen einbeziehen kannst. Es bedeutet nicht, dass du ihn einen Ausschluss konfigurieren musst, nur weil die Datei oder der Prozess auf dieser Seite erscheint. Ein gutes Beispiel dafür ist der Prozess lsass.exe. Die Regel, die den Zugriff auf diesen Prozess blockiert, erzeugt häufig viele Erkennungen, da auch legitime Anwendungen mit dem Prozess interagieren. Oft hat das Blockieren jedoch keine negativen Auswirkungen, sodass viele dieser Erkennungen ignoriert werden können.

Eine weitere Möglichkeit, Informationen über blockierte oder erkannte Aktivitäten abzurufen, sind die **Advanced-Hunting-Funktionen**, da alle Informationen zu ASR in der Tabelle **DeviceEvents** protokolliert werden. Wenn du zum Beispiel alle ASR-Aktivitäten der letzten fünf Tage anzeigen möchtest, verwendest du folgende Abfrage:

DeviceEvents

```
| where Timestamp > ago(5d)
| where ActionType startswith "asr"
```

Anstatt die Ergebnisse in einer Tabelle anzuzeigen, kannst du sie auch direkt aus der KQL-Abfrage heraus grafisch darstellen. Die folgende KQL verwendet die gleichen Informationen wie zuvor, gruppiert die Anzahl der Treffer jedoch pro **ActionType** und stellt sie in einem Kreisdiagramm dar:

DeviceEvents

```
| where Timestamp > ago(5d)
| where ActionType startswith "asr"
| summarize Action = count() by ActionType
| render piechart
```

Das Ergebnis würde ungefähr so aussehen:

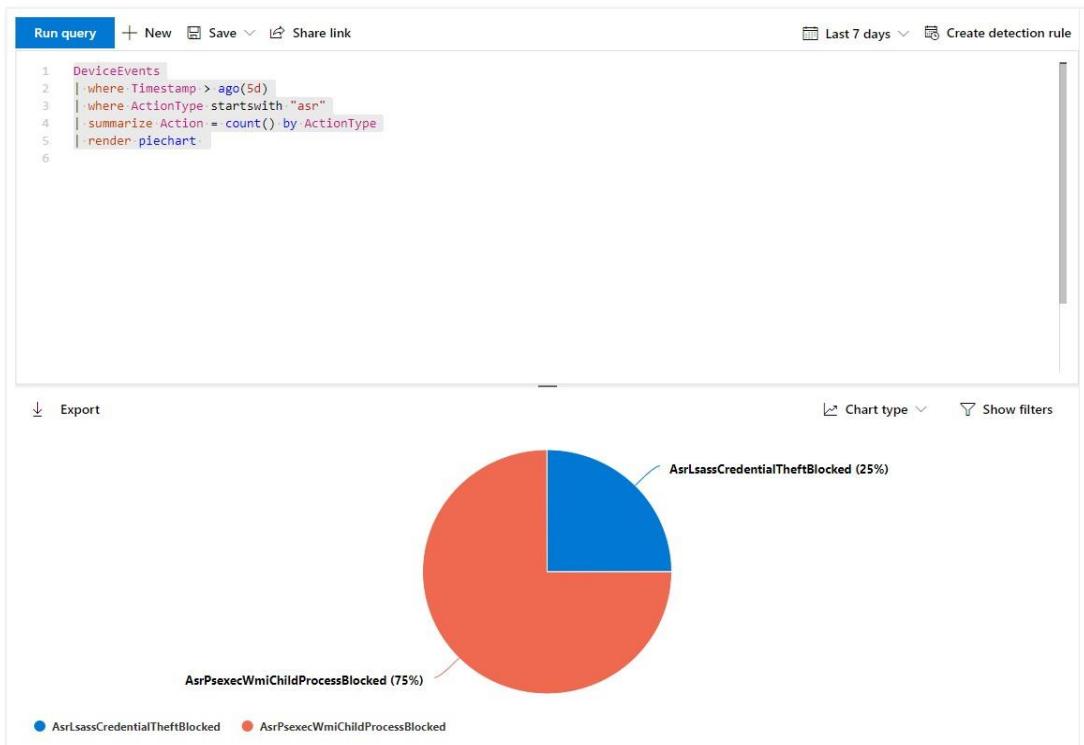


Abbildung 7-48: Überprüfung von ASR-Erkennungen durch eine Advanced-Hunting-Abfrage.

Anwendungsfall: Nutze die Advanced-Hunting-Funktionen für das, was sie wert sind. Das obige Beispiel war nur ein einfaches, um zu zeigen, dass die Informationen mit einer Abfrage zugänglich sind. Die gleichen Informationen findest du aber auch in den integrierten Berichten. Die Advanced-Hunting-Funktion eignet sich hervorragend, um tiefer in die Details von Erkennungen einzutauchen oder um ASR-Erkennungen mit anderen Informationen über das bzw. die Gerät(e) abzulegen.

Application Control

Application Control stellt sicher, dass nur zugelassene Anwendungen auf einem Gerät ausgeführt werden können. Auf diese Weise verhinderst du, dass unbekannte Anwendungen – wie Malware und anderer schädlicher Code – auf dem Gerät ausgeführt werden und Schaden anrichten können. Wie viele der Attack Surface Reduction-Funktionen ist auch Application Control nur für Windows 10 und Windows Server 2016 und höher verfügbar.

Application Control darf nicht mit AppLocker verwechselt werden. Obwohl beide Funktionen eine ähnliche Funktionalität bieten, ist Application Control neuer, anpassungsfähiger und der Weg in die Zukunft. Es gibt ein paar Dinge zu beachten, die wenig mit der Nützlichkeit von Application Control zu tun haben, sondern eher damit, wie es konfiguriert wird und welche Konsequenzen sich daraus ergeben:

- Die Konfiguration von Application Control kann schwierig sein. Obwohl du einfach eine Application Control-Richtlinie erstellen kannst, führt das nur einen Teil der Arbeit aus. Das Erstellen einer Liste zulässiger Anwendungen basierend auf Elementen wie dem Signaturzertifikat usw. erfordert (viel) mehr Arbeit als mit AppLocker-Richtlinien.
- Application Control wird nur unter Windows 10 unterstützt. Für ältere Betriebssysteme kannst du nur AppLocker verwenden.
- Die Aktivierung von Application Control unterbricht heute noch den Intune AutoPilot-Prozess.

Persönlich sehe ich Application Control noch nicht weit verbreitet. Die meisten Organisationen, die reif genug sind, um Application Control in irgendeiner Form zu nutzen, setzen immer noch auf AppLocker. Und bis zu einem gewissen Grad stimme ich dem zu. Mit einer recht einfachen AppLocker-Richtlinie kannst du die Sicherheitslage deiner Endpunkte bereits deutlich verbessern – was AppLocker zumindest vorerst zu einer sehr attraktiven Option im Vergleich zu Application Control macht.

Application Guard (App & Browser Isolation)

Application Guard bietet hardwarebasierte Isolation für Microsoft Edge und Microsoft Office (Apps for Enterprise). Immer wenn eine nicht vertrauenswürdige Seite besucht oder eine nicht vertrauenswürdige Datei geöffnet wird, wird die Anwendung in einem Hyper-V-Container

gestartet, der verhindert, dass diese Dateien und Websites über die Grenzen des Containers hinaus Schaden anrichten können. Da es sich um eine hardwaregestützte Funktion handelt, muss dein Gerät über die notwendige Hardware verfügen und die Voraussetzungen erfüllen, um sicherzustellen, dass Hyper-V darauf ausgeführt werden kann.

Die Unterstützung für Microsoft Edge und den älteren Internet Explorer ist standardmäßig vorhanden. Um mit diesen Browsern zu arbeiten, musst du nur eine Richtlinie erstellen und auf die entsprechenden Geräte anwenden. Andere Browser wie Chrome und Firefox können Application Guard ebenfalls nutzen, erfordern aber [etwas mehr Arbeit](#).

Application Guard aktivieren

Um Application Guard zu aktivieren, navigierst du zum Microsoft Endpoint Manager-Portal und klickst auf **Endpoint security > Attack surface reduction**. Klicke dann auf **Richtlinie erstellen** und wähle **Windows 10 und höher** als Plattform sowie **App- und Browser-Isolation** als Profil. Danach klickst du auf **Erstellen**.

Auf der Registerkarte **Konfigurationseinstellungen** kannst du wählen, ob du Application Guard mit den folgenden Optionen ein- oder ausschalten möchtest:

- **Aktiviert für Edge:** Aktiviert Application Guard nur für Microsoft Edge.
- **Aktiviert für isolierte Windows-Umgebung:** Aktiviert Application Guard nur für Microsoft Office.
- **Aktiviert für Edge UND isolierte Windows-Umgebungen:** Aktiviert Application Guard sowohl für Microsoft Edge als auch für Microsoft Office.

Sobald du einen der obigen Werte ausgewählt hast, werden weitere Optionen sichtbar, mit denen du zusätzliche Funktionen konfigurieren kannst – darunter die Möglichkeit, Protokolle für die Application Guard-Sitzungen zu erfassen, die Hardwarebeschleunigung zu aktivieren und Downloads auf das Host-Gerät zuzulassen (was die Grenzen des Containers aufheben würde).

Außerdem kannst du steuern, ob der Microsoft Edge-Browser lokal oder über das Netzwerk drucken darf, sowie das Drucken in die Dateiformate PDF oder XPS erlauben oder unterbinden.

Schließlich legst du über die **Windows-Netzwerkisolationsrichtlinie** fest, welche Ressourcen als Unternehmensressourcen gelten und welche nicht.

Windows network isolation policy ⓘ

	Configure	Not configured
IP ranges	0 items	▼
Cloud resources	0 items	▼
Network domains	0 items	▼
Proxy servers	0 items	▼
Internal proxy servers	0 items	▼
Neutral resources	0 items	▼
└ Disable Auto detection of other enterprise proxy servers ⓘ	Yes	Not configured
└ Disable Auto detection of other enterprise IP ranges ⓘ	Yes	Not configured

Abbildung 7-49: Definieren einer Windows-Netzwerkisolationsrichtlinie.

Admins können deaktivieren: Je nachdem, wie deine Richtlinien konfiguriert sind, können Benutzer möglicherweise nicht an den Application Guard-Richtlinien auf ihrem Gerät vornehmen – selbst dann nicht, wenn sie lokale Administratoren sind. Andererseits kann ein lokaler Administrator das Feature aus Windows deinstallieren und das Gerät neu starten, wodurch die Funktion (vorübergehend) deaktiviert wird.

Benutzererfahrung in Microsoft Edge

Wenn der Benutzer zum ersten Mal versucht, eine URL zu öffnen, die nicht als Unternehmensressource konfiguriert oder erkannt wird, wird ihm möglicherweise die folgende Meldung angezeigt, während im Hintergrund ein Hyper-V-Container erstellt wird:



Abbildung 7-50: Benachrichtigung, dass Windows Defender Application Guard startet.

Sobald der Container bereit ist, wird die Website in einem neuen Browserfenster geöffnet. Normalerweise gibt es wenig, was verrät, dass dies eine Instanz ist, die innerhalb des Hyper-V-Containers läuft – mit Ausnahme von ein paar Dingen:

- Neben der Adressleiste wird ein Symbol angezeigt, das darauf hinweist, dass der Browser im Application Guard-Modus ausgeführt wird (Abbildung 7-51).
- Der Browser öffnet sich, ohne dass ein Profil angemeldet ist.
- Erweiterungen, die in der regulären Browserinstanz aktiviert wurden, sind nicht installiert, vorhanden oder aktiviert.



Abbildung 7-51: Application Guard-Symbol neben der Adressleiste.

Abhängig von der Konfiguration deiner Application Guard-Richtlinie findest du möglicherweise auch andere Einschränkungen, wie zum Beispiel die Unmöglichkeit zu drucken, Informationen aus dem Browserfenster zu kopieren oder einzufügen usw.

Benutzerauswirkungen: Auf dem Papier ist Application Guard ein großartiges Feature mit vielen Sicherheitsvorteilen. Behalte jedoch immer die Auswirkungen im Hinterkopf, die es auf den Benutzer haben kann. Erstens gibt es viele URLs, Hosts, Domänen und IP-Adressen, die du als vertrauenswürdig kennzeichnen solltest - insbesondere alles, was mit Unternehmensressourcen zu tun hat. Allein für Office 365 müsstest du mehrere Domänennamen hinzufügen, einschließlich Wildcards, wie z.B. *.office.com, *.microsoft.com, <name>.sharepoint.com, <name-my>.sharepoint.com usw. Zweitens werden die Benutzer eine kurze Verzögerung bemerken, wenn sie URLs und Dateien öffnen, für die eine mit Application Guard-fähige Instanz geöffnet werden muss. Nicht zuletzt - und das ist durchaus relevant - erzeugt Application Guard in vielen Tests regelmäßig Fehlermeldungen, die einen Neustart erforderten, um behoben zu werden. Das bedeutet nicht, dass Application Guard nicht nützlich sein kann - aber du solltest alles gründlich testen, bevor du es für deine Benutzer aktivierst.

Controlled Folder Access

Controlled Folder Access ist ein zusätzlicher Schutz gegen Ransomware-Angriffe, da es erlaubt, eine Liste von Ordnerpfaden auf einem Gerät zu definieren, die zusätzlich gegen unbefugte Änderungen geschützt sind. Unter der Haube erlaubt das Feature nur vertrauenswürdigen (erlaubten) Anwendungen, in die angegebenen Ordnerpfade zu schreiben. Jeder andere Prozess, bei dem es sich um eine Ransomware-Datei handeln könnte, kann nicht schreiben – auch wenn er im Benutzerkontext ausgeführt wird, der normalerweise über die notwendigen Berechtigungen zum Schreiben und Ändern von Dateien verfügt.

Controlled Folder Access wird über die Attack Surface Reduction Rules-Richtlinie aktiviert. Suche insbesondere nach den folgenden Einstellungen:

- **Ordnerschutz aktivieren** - um das Feature ein- oder auszuschalten
- **Liste zusätzlicher Ordner, die geschützt werden müssen** - um eine Liste von Ordnerpfaden (zusätzlich zu den standardmäßig enthaltenen Ordnern) zu definieren, die von dem Schutz profitieren sollen. Typischerweise würdest du hier alle anderen Ordner einfügen, die Daten enthalten, die wichtig genug sind, um geschützt zu werden.
- **Liste der Apps, die Zugriff auf geschützte Ordner haben** – damit kannst du Ausnahmen steuern und festlegen, welche Anwendungen nicht daran gehindert werden, in die von dir in die angegebenen Ordner zu schreiben.

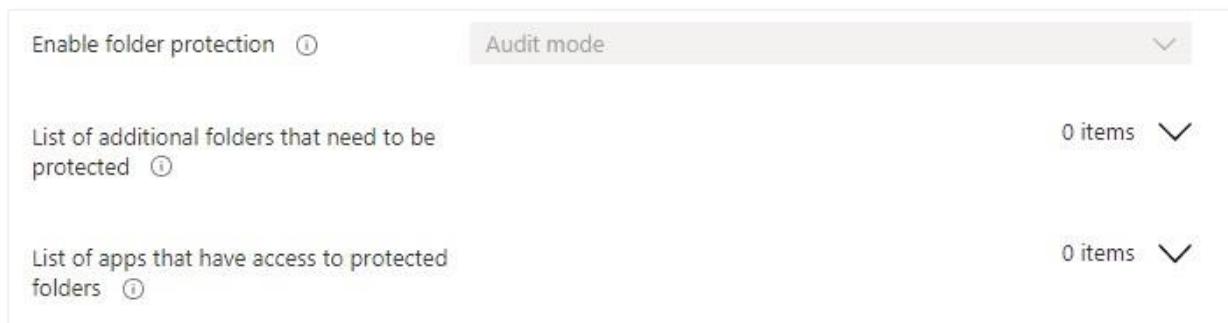


Abbildung 7-52: Überprüfen der Einstellungen für den kontrollierten Ordnerzugriff.

(Automatischer) Schutz: Du musst nicht alle Ordner selbst angeben. Wenn du das Feature aktivierst, werden die Systemordner von Windows zusammen mit einigen gängigen Ordnern unter C:\Users automatisch geschützt und müssen nicht in der Liste der zusätzlichen Ordner angegeben werden. Das Gleiche gilt für zugelassene Anwendungen. Apps, die in der Organisation weit verbreitet sind und nie wegen bösartiger Aktivitäten aufgefallen sind, werden automatisch zur Erlaubnisliste hinzugefügt und können Dateien in den geschützten Ordnerpfaden schreiben und ändern.

Berichte zum kontrollierten Ordnerzugriff

Immer wenn eine nicht vertrauenswürdige Anwendung versucht, in einen geschützten Ordner zu schreiben, erhält der Benutzer eine Benachrichtigung. Es wird jedoch keine Warnung im Security Center geben. Wie bei den anderen Attack Surface Reduction Rules werden die Ereignisse im Ereignisprotokoll protokolliert und sind über Advanced Hunting verfügbar. Um beispielsweise die Liste der blockierten und überwachten Aktivitäten der letzten fünf Tage abzurufen, verwende die folgende Abfrage:

```
DeviceEvents
| where Timestamp > ago(5d)
|     where ActionType in
```

('ControlledFolderAccessViolationAudited', 'ControlledFolderAccessViolationBlocked')

Exploit Protection

Wie die Attack Surface Reduction Rules zielt auch der Exploit-Schutz darauf ab, das Betriebssystem zu härten, indem er proaktiv häufige Techniken verhindert, die von bösartigem Code ausgeführt werden. Im Gegensatz zu den Attack Surface Reduction Rules geht er dabei tiefer ins Detail einer Aktivität und untersucht, wie eine Anwendung mit dem Betriebssystem interagiert. Genau wie alle anderen Attack Surface Reduction-Funktionen ist auch der Exploit-Schutz nur unter Windows 10 und Windows Server 2019 verfügbar. Auch er ist Teil des Windows-Betriebssystems und erfordert keine zusätzliche Lizenz. Defender for Endpoint ergänzt dieses Feature um zentrale Nachverfolgung, Berichterstattung und Integration in Untersuchungen.

Unter der Haube bietet der Exploit-Schutz eine Vielzahl von Gegenmaßnahmen, die entweder auf Anwendungs- oder Systemebene konfiguriert werden können. Die Gegenmaßnahmen werden jedoch immer pro Anwendung angewendet. Beispiele für einige Gegenmaßnahmen sind Arbitrary Code Guard (ACG), Export Address Filtering (EAF) Protection, Data Execution Prevention (DEP), Code Integrity Guard und viele andere.

Eine Übersicht über alle Gegenmaßnahmen, die im Exploit-Schutz verfügbar sind, und deren jeweiligen Zweck zu geben, würde das Buch unnötig aufblähen und nur wiederholen, was Microsoft bereits gut dokumentiert hat. Weitere Informationen zu den verschiedenen Fähigkeiten findest du [hier](#).

Nützlich, aber schwierig: Es besteht kein Zweifel an der Nützlichkeit und Wirksamkeit des Exploit-Schutzes. Andererseits gibt es, wenn eine Anwendung am Ausführen gehindert wird, kaum Informationen darüber, warum die Anwendung blockiert wurde – abgesehen von einem Eintrag in den Protokolldateien, der lediglich besagt, dass sie blockiert wurde und welche Einstellungen dafür verantwortlich waren. Das kann frustrierend sein, denn manchmal möchtest du verstehen, welcher Teil der Anwendung oder des Codes, den du ausführen willst, als potenziell bösartig gekennzeichnet wurde. Leider gibt es dafür keine direkte Abhilfe. Entwickler - falls sie daran interessiert sind, ihren Code zu aktualisieren - müssen möglicherweise mehrere Iterationen durchlaufen. Nur so lässt sich herausfinden, was im Code geändert werden muss, damit er nicht mehr vom Exploit-Schutz blockiert wird.

Exploit-Schutz aktivieren

Der einfachste Weg, den Exploit-Schutz zu aktivieren, besteht darin, ein Gerät in deiner Umgebung entweder über PowerShell oder das Windows Security Center zu konfigurieren und dann die relevante XML-Datei von diesem Gerät zu exportieren. Diese XML-Datei kann

anschließend in Microsoft Endpoint Manager verwendet werden, um eine Exploit-Schutz-Richtlinie zu erstellen. Beachte, dass du auch PowerShell, Configuration Manager, Gruppenrichtlinien oder jedes andere Tool verwenden kannst, das die XML-Datei verteilen und einen PowerShell-Befehl ausführen kann, um den Exploit-Schutz zu aktivieren.

Starte eine Exploit-Schutz-Richtlinie immer im Überwachungsmodus. Die im Exploit-Schutz enthaltenen Gegenmaßnahmen können sehr spezifisch sein und die Ausführung von Anwendungen auf einem Gerät beeinträchtigen. Sobald du die Auswirkungen einer neuen Richtlinie oder einer Richtlinienänderung bewertet hast, kannst du zum Blockierungsmodus übergehen.

Um ein Gerät lokal zu konfigurieren, öffne das Windows Security Center, klicke auf **App- & Browsersteuerung** und dann unten auf der Seite auf **Exploit-Schutz-Einstellungen**. Dadurch gelangst du zum entsprechenden Abschnitt, in dem du verschiedene Gegenmaßnahmen konfigurieren kannst, wie in Abbildung 7-53 dargestellt.

Wie du sehen wirst, gibt es zwei Registerkarten: **Systemeinstellungen** und **Programmeinstellungen**, auf denen du jeweils Standardeinstellungen konfigurieren kannst, die das Standardverhalten für alle Anwendungen auf dem System definieren, oder Gegenmaßnahmen pro Anwendung festlegst. Die Programmeinstellungen erben automatisch die auf Systemebene konfigurierten Einstellungen. Wenn keine Konfiguration vorhanden ist, wird die Standardeinstellung verwendet. Beachte, dass nicht alle Einstellungen auf Systemebene definiert werden können.

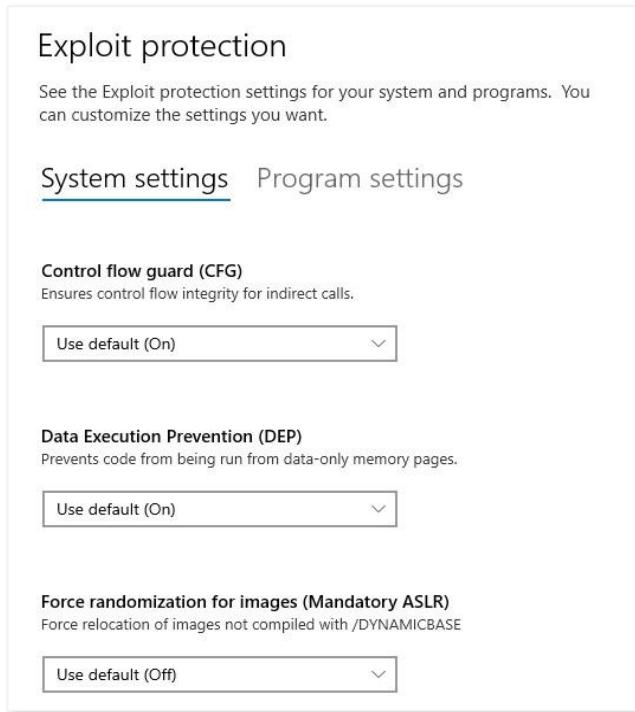


Abbildung 7-53: Konfigurieren des Exploit-Schutzes über das Windows Security Center.

Sobald du dein System nach deinen Wünschen konfiguriert hast, exportiere die XML-Datei des Exploit-Schutzes. Du kannst dies im Windows Security Center tun, indem du unten auf der Seite auf **Einstellungen exportieren** klickst. Alternativ kannst du dasselbe auch über PowerShell erledigen:

```
Get-ProcessMitigation -RegistryConfigFilePath c:\ExportedConfig.xml
```

Jetzt, da du die XML-Datei hast, lass uns die Richtlinie im Endpoint Manager-Portal erstellen. Navigiere zunächst zu **Endpunktsicherheit > Attack Surface Reduction** und klicke auf **Richtlinie erstellen**. Wähle **Windows 10 und höher** als Plattform und **Exploit-Schutz** als Profiltyp. Dann klickst du auf **Erstellen**.

Nachdem du einen Namen und eine Beschreibung für deine Richtlinie hinzugefügt hast, gehe zu den **Konfigurationseinstellungen**. Klicke auf **XML-Datei auswählen**, um nach der XML-Datei zu suchen, die du zuvor exportiert hast. Um zu verhindern, dass Benutzer an den Einstellungen des Exploit-Schutzes Änderungen vornehmen, aktiviere auch die Option **Benutzer daran hindern, die Benutzeroberfläche des Exploit Guard-Schutzes zu bearbeiten**.

Schließlich führst du die restlichen Schritte im Assistenten aus und weist die Richtlinie den Geräten zu, für die du den Exploit-Schutz aktivieren möchtest.

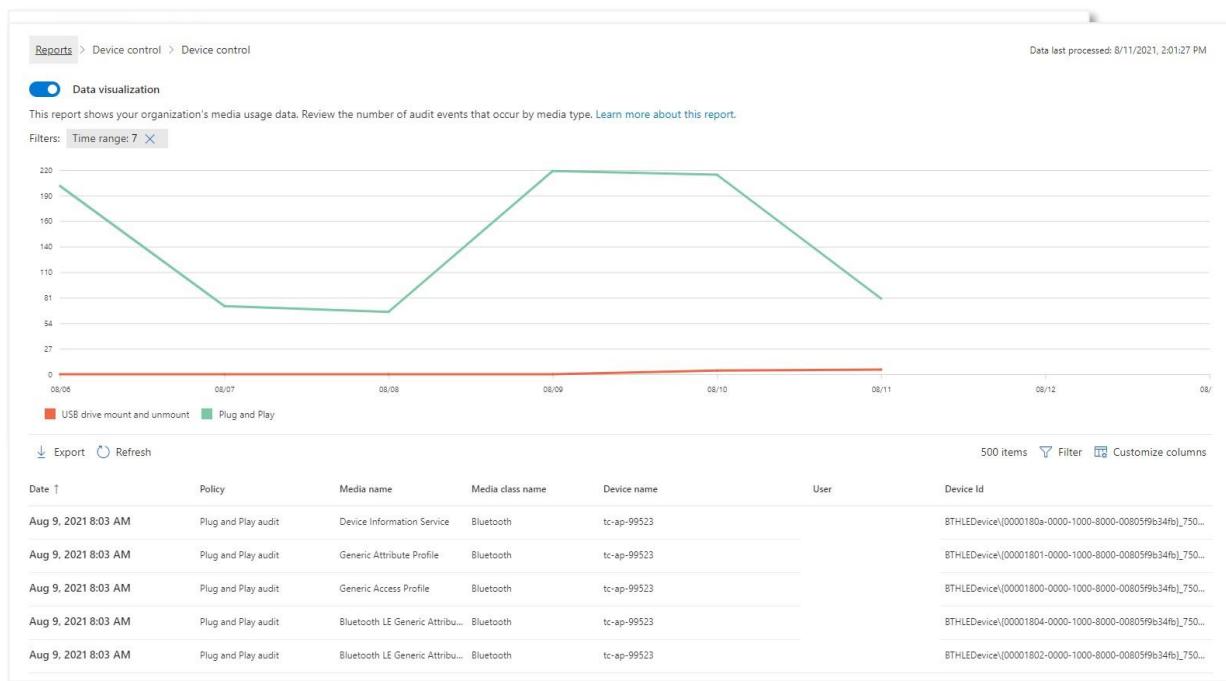


Abbildung 7-54: Konfigurieren des Exploit-Schutzes über das Windows Security Center.

Anzeigen von Exploit-Schutz-Ereignissen in Advanced Hunting

Wenn du Microsoft Defender for Endpoint nutzt, sind alle Ereignisse im Zusammenhang mit dem Exploit-Schutz über Advanced Hunting verfügbar. So kannst du die Auswirkungen deiner Richtlinien überprüfen und eigene Berichte erstellen.

Führe dazu die folgende Abfrage aus. Beachte, dass wir anstelle der Angabe jeder einzelnen Gegenmaßnahme speziell die Ereignisse des Netzwerkschutzes ausschließen:

DeviceEvents

```
| where ActionType startswith 'ExploitGuard' and ActionType !contains  
'NetworkProtection'
```

Um die Anzahl der durch die Gegenmaßnahmenoption blockierten Aktivitäten zu generieren und zu visualisieren, verwende die folgende Abfrage:

DeviceEvents

```
| where ActionType startswith 'ExploitGuard' and ActionType !contains  
'NetworkProtection'  
  
| summarize Actions = count() by ActionType | render piechart
```

Device Control

Mit der Gerätekontrolle kann ein Administrator erkennen, welche (externen) Geräte – wie zum Beispiel USB-Speichermedien – in deiner Umgebung verwendet werden, und steuern, ob sie zulässig sind oder nicht. Letztendlich besteht das Ziel darin, zu verhindern, dass Bedrohungen über einen kompromittierten USB-Treiber oder ein anderes Peripheriegerät, das zur Ausführung von schädlichem Code auf einem deiner Endpunkten verwendet werden könnte, in deine Organisation eindringen.

Überprüfen von Berichten zur Gerätekontrolle

Um auf den Bericht zur Gerätekontrolle zuzugreifen, öffne das Microsoft 365 Security Center und navigiere zu **Berichte > Gerätekontrolle**. Klicke dort auf **Details anzeigen**, um den detaillierten Bericht zu öffnen.

Der Bericht zeigt dir detaillierte Informationen darüber, welche Geräte mit Endpunkten in deiner Umgebung verbunden wurden. Er unterscheidet zwischen USB-Laufwerken (Wechselspeicher) und allgemeineren Plug-&-Play-Ereignissen (PnP). Für jede der Aktivitäten kannst du sehen, um welche Aktivität es sich handelt, auf welchem Gerät sie aufgetreten ist

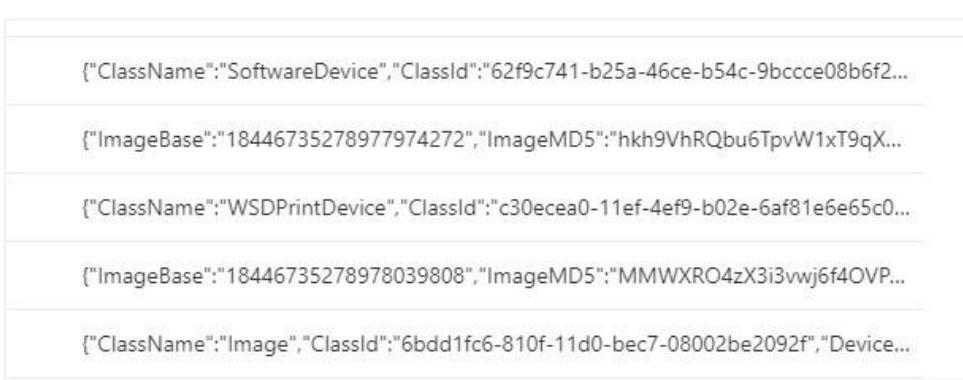
und welcher Benutzer die Aktion durchgeführt hat. Zu den Details gehören auch die Geräte-ID und die Hersteller-ID, die du beide bei der Erstellung einer Richtlinie benötigst.

Gerätekontrolle & Advanced Hunting

Informationen über angeschlossene Geräte sind auch in den Advanced-Hunting-Funktionen verfügbar. Leider sind die Informationen etwas versteckt, da alle Ereignisse der Gerätekontrolle in einer einzigen Eigenschaft namens **AdditionalFields** zusammengefasst sind, wie unten gezeigt:

```
DeviceEvents
| take 10
| project AdditionalFields
```

Was du sehen wirst, ähnelt der Ausgabe in der folgenden Abbildung:



```
[{"ClassName": "SoftwareDevice", "ClassId": "62f9c741-b25a-46ce-b54c-9bccce08b6f2...", "ImageBase": "18446735278977974272", "ImageMD5": "hkh9VhRQbu6TpW1xT9qX...", "AdditionalFields": "..."}, {"ClassName": "WSDPrintDevice", "ClassId": "c30ecea0-11ef-4ef9-b02e-6af81e6e65c0...", "ImageBase": "18446735278978039808", "ImageMD5": "MMWXRO4zX3i3vwj6f4OVP...", "AdditionalFields": "..."}, {"ClassName": "Image", "ClassId": "6bdd1fc6-810f-11d0-bec7-08002be2092f", "Device..."}]
```

Abbildung 7-56: Überprüfen von Ereignissen der Gerätekontrolle in Advanced Hunting.

Da wir die Ausgabe ein wenig bereinigen wollen, müssen wir zuerst die Informationen aus der Eigenschaft **AdditionalFields** analysieren, wie folgt:

```
DeviceEvents
| extend parsed=parse_json(AdditionalFields)
```

Bevor wir etwas Nützliches aus den geparssten Informationen herausbekommen können, müssen wir die relevanten Informationen daraus extrahieren, wie folgt:

```
DeviceEvents
| extend parsed=parse_json(AdditionalFields)
| extend MediaClass = tostring(parsed.ClassName)
| extend MediaDeviceId = tostring(parsed.DeviceId)
| extend MediaDescription = tostring(parsed.DeviceDescription)
| extend MediaSerialNumber = tostring(parsed.SerialNumber)
```

Schließlich können wir sicherstellen, dass nur Ereignisse angezeigt werden, die relevante Informationen enthalten, und dass wir nur die Felder abrufen, an denen wir interessiert sind:

DeviceEvents

```
| extend parsed=parse_json(AdditionalFields)
| extend MediaClass = tostring(parsed.ClassName)
| extend MediaDeviceId = tostring(parsed.DeviceId)
| extend MediaDescription = tostring(parsed.DeviceDescription)
| extend MediaSerialNumber = tostring(parsed.SerialNumber)
| where MediaDeviceId != ""
| project Timestamp, DeviceId, DeviceName, AccountName, AccountDomain,
MediaClass,
MediaDeviceId, MediaDescription, MediaSerialNumber, parsed
```

Eine Eigenschaft, die wirklich nützlich sein kann, ist **MediaClass**, da sie die verschiedenen Gerätetypen voneinander unterscheidet. Du wirst zum Beispiel **DiskDrive**, **Camera**, **Mouse**, **Keyboard**, **CDROM** usw. sehen. Genau wie im vorherigen Abschnitt kannst du die **DeviceID** oder **DeviceClass** verwenden, um deine Richtlinie zu erstellen.

Eine Richtlinie zur Gerätekontrolle erstellen

Um eine neue Richtlinie zur Gerätekontrolle zu erstellen, öffne das Endpoint Manager Portal und navigiere zu **Endpunktsicherheit > Attack Surface Reduction**. Klicke auf *Richtlinie erstellen*. Wähle **Windows 10 und höher** als Plattform und **Gerätekontrolle** als Profiltyp. Klicke anschließend auf *Erstellen*.

Sobald du einen Namen und eine Beschreibung definiert hast, gehe weiter zu den **Konfigurationseinstellungen**. Hier kannst du eine Reihe von Einstellungen definieren.

Administrativvorlagen	
System > Geräteinstallation > Einschränkungen bei der Geräteinstallation	Mit den Einschränkungen bei der Geräteinstallation können Sie steuern, welche Geräte (basierend auf Geräte-IDs oder Geräteinstanz-IDs) auf einem Endpunkt installiert werden dürfen. Die verschiedenen Richtlinien ermöglichen es, die Installation von Hardware explizit zu erlauben oder zu verhindern.

System > Zugriff auf Wechselmedien	Der Abschnitt „Zugriff auf Wechselmedien“ steuert, ob und wie Ihr Endpunkt über Windows Portable Devices (WPD) mit angeschlossenen Medien- und Speichergeräten kommunizieren kann. Die Verwendung von WPD ermöglicht eine detailliertere Kontrolle, z. B. die nachfolgende Speicherrichtlinie für externe Datenträger.
Defender	
Vollständigen Scan von Wechselmedien zulassen	Steuert, ob Microsoft Defender Antivirus Wechselmedien scannen darf.
Datenschutz	
Direkten Speicherzugriff (DMA) zulassen	Hier steuern Sie den direkten Speicherzugriff (DMA) außerhalb einer Benutzersitzung.
DMA-Schutz	
Richtlinie zur Geräteaufzählung	DMA-Schutz erweitert die reguläre DMA-Kontrolle, indem Windows einem Peripheriegerät einen bestimmten Speicherbereich zuweist. Versucht ein Gerät, außerhalb dieses Bereichs zu lesen oder zu schreiben, wird die Aktion blockiert. Funktioniert nur, wenn Kernel-DMA-Schutz unterstützt wird.
Speicher	
Schreibzugriff auf Wechselmedien verweigern	Steuert, ob Daten auf externe Speichermedien geschrieben werden dürfen. Diese Richtlinie unterscheidet sich von BitLocker: Bei BitLocker kann Verschlüsselung verlangt werden, bevor geschrieben wird. Hier ist die Regel binär: Schreiben ist entweder erlaubt oder verboten.
Konnektivität	

Ermöglicht die Steuerung des USB-Zugriffs für bestimmte Geräte und das Einschränken der Bluetooth-Nutzung.

Bluetooth

Bietet eine feinere Kontrolle über die Bluetooth-Nutzung. Die vorherige Einstellung schaltet Bluetooth nur ein oder aus; hier können Sie z. B. festlegen, ob Geräte gekoppelt werden dürfen.

GUIDs: Wenn Du eine Richtlinie erstellst und bestimmte Geräte und Geräteklassen zulässt oder blockierst, musst du die entsprechenden Kennungen für diese Geräte oder Geräteklassen angeben. Diese Informationen kannst du über die Berichte und Advanced Hunting abrufen. In großen Umgebungen kann es jedoch etwas schwieriger sein, die große Menge an Daten zu durchforsten, die möglicherweise verfügbar sind. In diesem Fall kannst du die Kennungen auch direkt vom lokalen Gerät abrufen, indem du die Eigenschaften des Geräts im Geräte-Manager ansiehst!

Endpoint Detection & Response (EDR)

Die Funktionen zur Endpunktterkennung und -reaktion (Endpoint Detection and Response, EDR) von Microsoft Defender for Endpoint sind eine der Kernfunktionen, die das Produkt bietet. Ihr Ziel ist einfach, aber umfassend: eine Vielzahl von Aktivitäten auf dem Endpunkt überwachen und diese Telemetriedaten an den Cloud-Dienst zur weiteren Analyse senden. Im Gegenzug leitet der Cloud-Dienst eine Reaktion ein, wenn (potenziell) bösartige Aktivitäten erkannt werden.

Es gibt keine erschöpfende Liste, die im Detail beschreibt, welche Aktivitäten genau überwacht werden und welche nicht. Dieser Ansatz der *Security by Obscurity* ist verständlich – man möchte bösen Akteuren nicht genau sagen, was man tut. Andererseits ist das auch eine Qual für die Verteidiger, denn man muss selbst herausfinden, was genau durch das System nicht überwacht wird. Zum Zeitpunkt des Schreibens überwacht Defender for Endpoint die folgenden Aktivitäten:

- **Prozesserstellungssereignisse**
- **Netzwerkereignisse**, einschließlich erfolgreicher und fehlgeschlagener Verbindungen, überwachter Verbindungen usw.
- **Dateiereignisse** wie Erstellung, Löschung, Änderung und Umbenennung. Zusätzlich zu diesen Arten von Aktivitäten werden auch Informationen wie die Häufigkeit einer Datei, verschiedene Hashes und Zertifikatsinformationen (falls vorhanden) gesammelt.
- **Registrierungsereignisse** wie das Hinzufügen, Entfernen und Ändern von Schlüsseln

- **Anmeldeereignisse** wie (erfolgreiche) Anmeldeversuche
- **Image-Ladeereignisse**, bei denen das Laden von DLL-Dateien überwacht und erfasst wird
- **Sonstige Ereignisse**, z.B. ob geplante Aufgaben erstellt oder gelöscht wurden, Screenshots aufgenommen wurden, Dienste installiert wurden, Treiber geladen wurden, Geräte angeschlossen wurden usw.

Wie du der obigen Liste entnehmen kannst, werden eine Menge Informationen gesammelt. Diese Informationen werden nicht nur dem Cloud-Dienst zur Verfügung gestellt. Als Administrator hast du vollen Zugriff auf diese Daten, sodass du sie zur Erstellung eigener Berichte und – was vielleicht noch wichtiger ist – für Suchabfragen verwenden kannst. Weitere Informationen zu Suchabfragen findest du später in diesem Kapitel.

Sysmon vs. Defender for Endpoint

Viele Organisationen verwenden das Windows Sysinternals-Tool **Sysmon**, um bestimmte Aktivitäten auf ihren Windows-Geräten zu überwachen. Das war vor allem vor dem Aufkommen der EDR-Lösungen der Fall. Da letztere – wie Microsoft Defender for Endpoint – jedoch ebenfalls eine Vielzahl von Aktivitäten überwachen, stellt sich oft die Frage, ob der Einsatz von Sysmon noch sinnvoll ist.

Die Antwort ist nicht so einfach, wie man vielleicht denkt, und hängt wirklich von der aktuellen Situation ab. Wenn du Sysmon noch nicht verwendest und nur wenige Erkennungs- und Reaktionsmöglichkeiten hast, denke ich nicht, dass die Einbeziehung von Sysmon dir einen großen Mehrwert bringt.

Andererseits gibt es Elemente, die (noch) nicht von Microsoft Defender for Endpoint überwacht werden, und der zusätzliche Einsatz von Sysmon kann helfen, bestimmte (ausweichende) Verhaltensweisen zu erkennen. Obwohl Defender for Endpoint über einen Manipulationsschutz verfügt, der lokale Änderungen an der Konfiguration der Lösung verhindert, gibt es einige Möglichkeiten, die Erkennung zu umgehen. Ein gutes Beispiel dafür findest du [\[hier\]f.underline](#). In dem Artikel wird beschrieben, wie lokale Ausschlüsse zur Registrierung des Geräts hinzugefügt werden können. Diese Änderungen werden von Microsoft Defender for Endpoint nicht erkannt und könnten dazu führen, dass Dateien und Prozesse nicht gescannt werden, weil ein Angreifer sie manuell ausgeschlossen hat. Um also erkennen zu können, dass jemand (oder etwas) die Ausschlüsse lokal ändert, kann die Verwendung eines Tools wie Sysmon hilfreich sein.

Komplexität: Der Einsatz von *Sysmon* erhöht die Komplexität deines Deployments. Da es in keiner Weise in Defender for Endpoint integriert ist, musst du die *Sysmon*-Ereignisse irgendwie und irgendwo erfassen und zentral speichern. Der ideale Ort dafür wäre ein SIEM, wie Microsoft Sentinel, das in Kapitel 13 besprochen wird. Mit den Informationen im SIEM könntest

du dann Erkennungen auf der Grundlage von Ereignissen erstellen, die du über *Sysmon* siehst, und dem, was von Defender for Endpoint erfasst wird.

Indikatoren für Kompromittierungen

Bedrohungen können auf unterschiedliche Weise entdeckt werden. Während Antivirenlösungen früher einfach die Signatur einer Datei oder eines Prozesses überprüften, müssen heute viele andere Dinge berücksichtigt werden, um gutartige Aktivitäten und Binärdateien von bösartigen zu unterscheiden. Aktivitäten allein liefern nicht immer ausreichende Informationen darüber, ob sie bösartig sind oder nicht. Ein Download von einem Standort innerhalb des gleichen Landes wie deine Organisation kann zum Beispiel völlig harmlos sein, während die gleiche Aktivität aus einem entfernten Standort darauf hindeuten könnte, dass jemand Daten exfiltriert. Obwohl der Kontext einer Aktivität wichtig ist, können manchmal auch bestimmte Informationen wie der Hash einer Datei verwendet werden, um potenziell bösartige Aktivitäten zu erkennen.

Indikatoren für Kompromittierungen (Indicators of Compromise, IOCs) sind einzelne Elemente – Informationsteile, die zu einer bestimmten Bedrohung oder einem bestimmten Angriff gehören. Diese Informationen werden in der Regel im Rahmen einer Untersuchung gesammelt. Beispiele für einen IOC sind Datei-Hashes, IP-Adressen oder bestimmte Domänennamen, die während eines (früheren) Angriffs verwendet wurden. Indikatoren für Kompromittierungen sind – wie der Name schon sagt – meist Artefakte eines erfolgreichen Angriffs. Eine Malware-Probe, die auf einem Gerät gefunden wird, bedeutet zum Beispiel, dass die Anfangsphase eines Angriffs möglicherweise bereits erfolgreich durchgeführt wurde.

Indikatoren können verwendet werden, um ähnliche Aktivitäten oder Vorfälle an anderen Orten und in anderen Systemen zu erkennen. Häufig wird ein Indikator, der in einem System erkannt wurde, verwendet, um eine Abfrage in einem anderen System auszuführen. Wenn eine Übereinstimmung mit einem Indikator gefunden wurde, kann eine tiefere Untersuchung eingeleitet werden, um zu überprüfen, ob eine böswillige Absicht dahintersteckt oder nicht.

Arbeiten mit Indikatoren für Kompromittierungen

Microsoft nutzt ein ganzes Netzwerk von Bedrohungsinformationen, um bösartiges Verhalten in seinen Produkten zu erkennen. Welche IOCs Microsoft verwendet, ist nicht bekannt – sie veröffentlichen ihre Liste der Indikatoren nicht. Das liegt zum einen daran, dass man böswilligen Akteuren nicht zeigen möchte, welche ihrer Systeme und Nutzlasten möglicherweise bereits entdeckt wurden, zum anderen aber auch daran, dass Indikatoren für Kompromittierungen in der Regel nur für einen kurzen Zeitraum gültig sind. Die Pflege einer solchen Liste hat daher wenig Wert, da Kunden mit Defender for Endpoint automatisch geschützt werden, sobald Aktivitäten im Zusammenhang mit bekannten Indikatoren erkannt werden.

Trotz der großen Menge an Bedrohungsinformationen, die Microsoft pflegt, ist es nicht ungewöhnlich, dass ein Sicherheitsteam seine eigene Liste von Indikatoren konfiguriert und pflegt. Das kann daran liegen, dass einige Indikatoren spezifisch für die jeweilige Organisation sind oder weil das Team zusätzliche Kontrolle darüber haben möchte, was passiert, wenn ein Artefakt entdeckt wurde.

In Defender for Endpoint kannst du die folgenden Indikatoren für Kompromittierungen definieren:

- Datei-Hash-Wert
- IP-Adresse
- Domänenname (oder URL)
- Zertifikate

Indikatoren werden von verschiedenen Komponenten in Defender for Endpoint verarbeitet – an den folgenden Stellen, wo jeweils die im IOC definierte Aktion ausgeführt wird:

- Cloud Detection Engine (EDR), die die entsprechende Aktion ausführt, sobald sie eine Übereinstimmung in der Telemetrie erkennt, die sie von den lokalen Geräten und anderen Systemen in Microsoft 365 erhält.
- Defender Antivirus, das lokal erkannte Aktivität verhindert und meldet.
- Automatisierte Untersuchung und Reaktion.

Für jeden Indikator kannst Du die folgenden Aktivitäten definieren:

- Zulassen
- Nur warnen
- Warnen und blockieren

Erstellen eines benutzerdefinierten Indikators für Kompromittierungen

Indikatoren können auf verschiedene Weise erstellt werden:

- Manuelles Hinzufügen zur Liste der Indikatoren
- Erstellen im Rahmen einer Untersuchung (Vorfall)
- Über die [Indikator-API](#).

Um einen Indikator hinzuzufügen, öffne das Microsoft 365 Security Center und navigiere zu **Einstellungen > Endpunkt > Indikatoren**. Wechsle dann zur Registerkarte, für die du einen Indikator hinzufügen möchtest. Wenn du zum Beispiel einen Datei-Hash hinzufügen möchtest, klicke auf die Registerkarte **Datei-Hashes** und dann auf **Element hinzufügen**.

Füge die relevanten Informationen über den Indikator im Bereich auf der rechten Seite des Bildschirms hinzu und durchlaufe den Rest des Assistenten, wie in Abbildung 7-57 dargestellt.

Widersprüchliche Einstellungen vermeiden: Die von dir gewählte Aktion für einen Indikator kann beeinflussen, wie Defender for Endpoint eine Bedrohung behandelt. Wenn z.B. die Ausführung einer Datei durch die Attack Surface Reduction zugelassen, aber ein Indikator sie blockiert, wird sie blockiert. Umgekehrt gilt: Wenn die ASR die Datei blockiert, der Indikator sie aber zulässt, wird sie zugelassen. Das gilt jedoch nicht für die Anwendungssteuerung oder für einen Defender-Antivirus-Ausschluss - diese haben immer Vorrang vor der Einstellung eines Indikators. Wenn du also widersprüchliche Konfigurationen in verschiedenen Richtlinien hast, kann es zu unerwartetem Verhalten führen und die Fehlerbehebung erschweren.

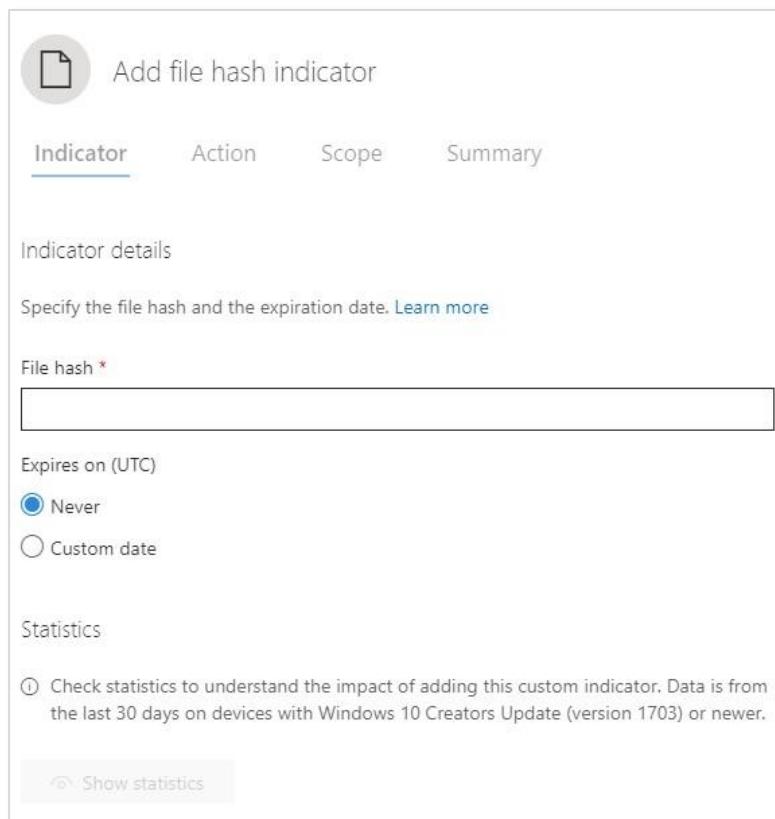


Abbildung 7-57: Hinzufügen eines Indikators für Kompromittierung zu Defender for Endpoint.

Ein Indikator kann auch im Rahmen einer Untersuchung hinzugefügt werden. Wenn dir beispielsweise eine bestimmte Datei auffällt, kannst du einen Eintrag direkt von der Datei-Entitätsseite aus hinzufügen – entweder über die Schaltfläche **Regel für Erlaubnis-/Sperrliste für diese Datei hinzufügen** in der Auswahl oder über **Indikator hinzufügen** auf der Entitätsseite selbst.

Automatisierte Untersuchung & Reaktion (AIR)

Eine der größten Herausforderungen in der Cybersicherheit ist der Mangel an qualifiziertem Personal, das mit dem nicht enden wollenden Strom von Ereignissen und Vorfällen umgehen

kann, mit denen Organisationen täglich konfrontiert sind. Selbst mit gutem Personal ist es kaum möglich, alle Ereignisse manuell zu prüfen – einfach weil es zu viele potenziell relevante Aktivitäten gibt. Vermutlich war das auch noch nie eine praktikable Vorgehensweise. Erfolgreiche Angreifer tun alles, um nicht entdeckt zu werden. Sie vermeiden es, kritische Warnungen auszulösen. Wenn es doch zu einer Warnung kommt, ist diese oft nur niedrig oder mittel priorisiert. Und wenn so etwas passiert, ist es häufig schon zu spät. Deshalb sage ich oft: Erfolgreiche Angreifer „leben“ in den niedrigen und mittleren Warnungen – dort, wo die Masse der Ereignisse liegt, wo es am schwierigsten ist, verdächtige Aktivitäten zu erkennen, einfach aufgrund der schieren Anzahl.

Die automatisierte Untersuchung und Reaktion (Automated Investigation & Response, AIR) soll das Sicherheitsteam entlasten, indem sie Ereignisse automatisch analysiert, klassifiziert und – wo möglich – darauf reagiert.

Es gibt zwei Möglichkeiten, wie eine automatisierte Untersuchung gestartet wird:

- **Wenn eine Warnung ausgelöst wird:** In einigen Fällen, z.B. wenn eine Malware-Warnung ausgelöst wurde, greift AIR ein und untersucht die Aktivität auf dem betroffenen Gerät. Wenn währenddessen neue (verwandte) Warnungen auftreten, werden sie automatisch dem Vorfall im Portal hinzugefügt.
- Du kannst eine Untersuchung auch **manuell** von einem Vorfall oder einem Ereignis aus starten, das es bei der Überprüfung der Umgebung entdeckt hat.

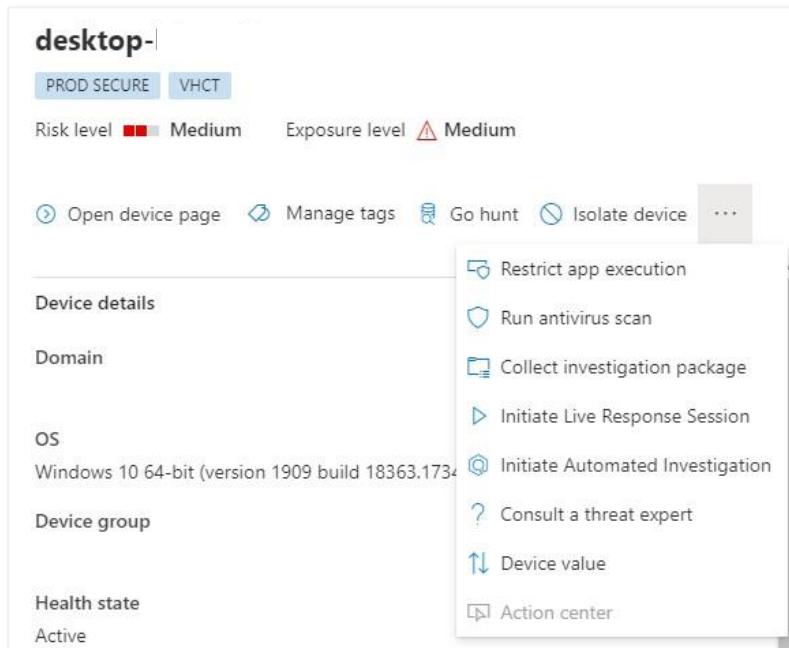
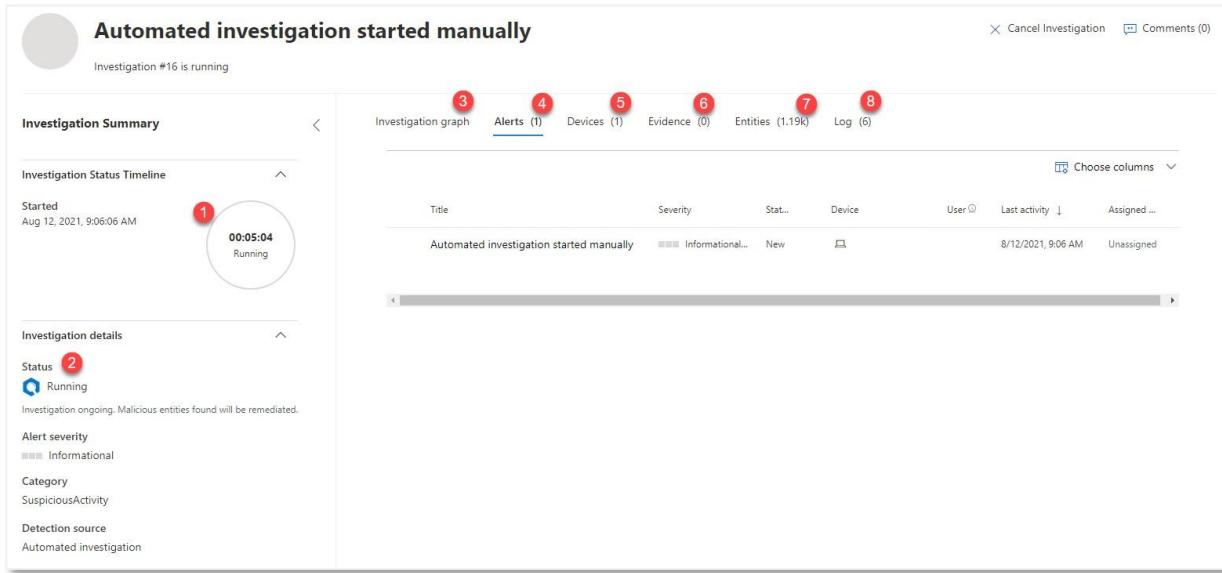


Abbildung 7-58: Manuelles Starten einer automatisierten Untersuchung von der Geräteseite aus.

Während der Untersuchung prüft AIR eine Vielzahl an Artefakten, darunter Aktivitäten auf dem Gerät, laufende Prozesse, vorhandene Dateien, Netzwerkverbindungen und mehr. Wenn du manuell eine automatische Untersuchung startest, wird für das betroffene Gerät eine Warnung und ein Vorfall angelegt. Automatische Untersuchungen hingegen werden dem bestehenden Vorfall zugeordnet, der sie ursprünglich ausgelöst hat.

Über die Untersuchungsseite kannst du aktive Untersuchungen überwachen, die Ergebnisse abgeschlossener Analysen einsehen und Aktionen freigeben, die eine Bestätigung durch Administratoren erfordern.



The screenshot shows the 'Automated investigation started manually' page. At the top, it says 'Investigation #16 is running'. Below that is the 'Investigation Summary' section with a timeline showing 'Started Aug 12, 2021, 9:06:06 AM' and a status of 'Running' (indicated by a red circle with '1'). The 'Alerts' tab (4) is selected, showing one alert titled 'Automated investigation started manually' with severity 'Informational' and status 'New'. Other tabs include 'Investigation graph' (3), 'Devices' (5), 'Evidence' (6), 'Entities' (7), and 'Log' (8). The 'Investigation details' sidebar shows 'Status: Running' (2), 'Alert severity: Informational', 'Category: SuspiciousActivity', and 'Detection source: Automated investigation'.

Abbildung 7-59: Überprüfung einer automatisierten Untersuchung.

- Auf der Hauptseite siehst du zunächst den Status der aktuellen Untersuchung (z.B. Status 1 und 2), ob sie läuft, wann sie gestartet wurde, wie lange sie bereits läuft usw.
- Der **Untersuchungsgraph** (3) bietet dir einen Überblick über die aktuelle Untersuchung. Er stellt visuell verschiedene Entitäten wie Dateien, Prozesse, Treiber, IP-Adressen und Angriffstechniken in Bezug zu dem oder den Geräten dar, auf denen die Untersuchung durchgeführt wurde.
- Auf der Seite **Warnungen** (4) siehst du alle Warnungen, die sich auf diese Untersuchung beziehen.
- Die Seite **Geräte** (5) zeigt Informationen über die Geräte im Rahmen dieser Untersuchung an. Wenn eine Untersuchung gestartet wird und von anderen Geräten Warnungen ausgelöst werden, die mit demselben Vorfall korreliert werden können, erweitert AIR seinen Umfang automatisch und bezieht diese Geräte ebenfalls in die Untersuchung ein.
- Die Seite **Beweise** (6) enthält die endgültigen Informationen, auf deren Grundlage AIR seine Schlussfolgerung gezogen hat. Diese Seite enthält nur dann Informationen, wenn eine Bedrohung erkannt wurde.

- Auf der Seite **Entitäten** (7) siehst du eine Übersicht über alle Entitäten, die während der Untersuchung überprüft wurden. Zu den Entitäten gehören die folgenden:
 - **Dateien**: gescannte ausführbare Dateien und DLL-Dateien.
 - **Prozesse**, die derzeit auf dem Gerät laufen.
 - **Dienste**, die auf dem Gerät vorhanden sind.
 - **Treiber**, die geladen wurden.
 - **IP-Adressen**, mit denen sich das Gerät kürzlich verbunden hat
 - **Persistenzmethoden**, eine Liste häufig verwendeter Persistenztechniken, die explizit überprüft werden. Überprüft werden geplante Aufgaben, Autoruns, verknüpfte Dateien,
- Das **Protokoll** (8) bietet einen Überblick über die von AIR durchgeföhrten Aktivitäten. Hier kannst du sehen, welche Aktivität gerade durchgeführt wird, oder du kannst es verwenden, um weitere Einblicke und Details darüber zu erhalten, was genau durchgeführt wurde. So kannst du beispielsweise über das Protokoll die Rohdaten der Analyse von Persistenzmethoden exportieren, die du mit anderen Informationen abgleichen oder einfach daraus lernen kannst.

Automatisierungsstufen

AIR verfügt über verschiedene Automatisierungsstufen, die es einem Administrator ermöglichen, zu steuern, wie autonom eine Untersuchung sein kann. Die verfügbaren Automatisierungsstufen sind die folgenden:

- **Vollständig - Bedrohungen automatisch beheben (Standard)**: Diese Einstellung stellt sicher, dass nach Abschluss einer Untersuchung, bei der Behebungsmaßnahmen durchgeführt werden müssen, diese Aktivitäten vollständig automatisch, ohne Eingreifen eines Administrators, ausgeführt werden. Bei Bedarf kann ein Administrator eingreifen und die vom System ergriffene Maßnahme rückgängig machen.
- **Halbautomatisch - Genehmigung für jede Behebung erforderlich**: Diese Einstellung führt die Untersuchung zwar durch, führt aber keine Behebung durch. Ein Administrator muss die Untersuchung manuell öffnen, zur Aktion navigieren - die sich in einem ausstehenden Zustand befindet - und sie genehmigen.
- **Halbautomatisch - Genehmigung für die Behebung von Kernordnern erforderlich**: Ähnlich wie bei der obigen Einstellung, nur dass eine Genehmigung nur für Korrekturen erforderlich ist, die Kern-Betriebssystemordner wie C:\Windows betreffen. Alle anderen Korrekturmaßnahmen werden automatisch durchgeführt.
- **Halbautomatisch - Genehmigung für die Behebung von Nicht-Temp-Ordnern erforderlich**: AIR führt Korrekturmaßnahmen für Dateien und ausführbare Dateien, die in temporären Ordnern gespeichert sind, automatisch durch. Diese Ordner sind typischerweise die folgenden. Jede andere Behebung muss zunächst genehmigt werden.
 - \users*\appdata\local\temp*
 - \documents and settings*\local settings\temp*

- \documents and settings*\local settings\temporary*
 - \windows\temp*
 - \users*\downloads*
 - \program files\
 - \program files (x86)*
 - \documents and settings*\users*
- **Keine automatische Reaktion:** Führt keine automatische Behebung durch. Alle Korrekturmaßnahmen müssen zunächst von einem Administrator genehmigt werden.

Kapitel 12 geht näher auf die praktischen Details der verschiedenen Sicherheitslösungen von Microsoft ein und erläutert beispielsweise, wie man verschiedene Warnungen untersucht und darauf reagiert. Dazu gehört auch, wie man ausstehende Aktionen aus einer automatisierten Untersuchung bestätigt.

Konfigurieren von Automatisierungsstufen für AIR

Die verschiedenen Automatisierungsstufen für AIR werden über Gerätegruppen (siehe weiter oben in diesem Kapitel) konfiguriert; immer wenn eine neue Gerätegruppe erstellt wird, musst du die Automatisierungsstufe auf der Registerkarte **Allgemein** angeben, wie unten dargestellt:

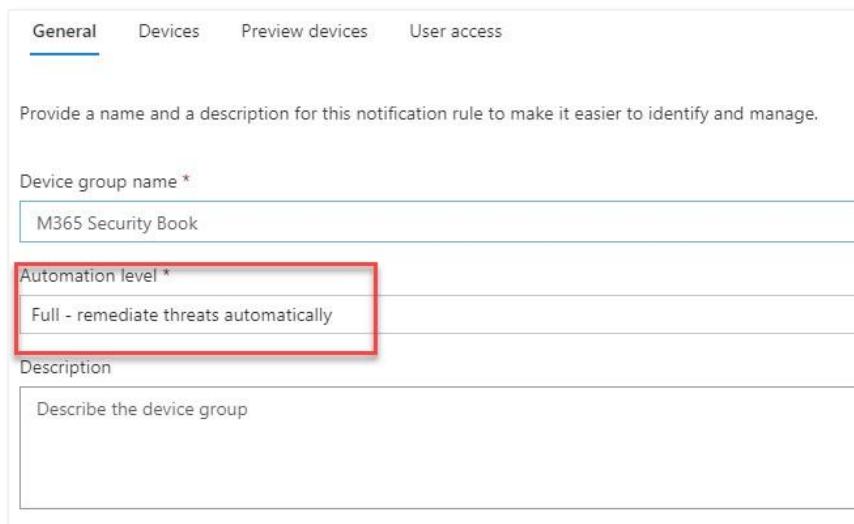


Abbildung 7-60: Festlegen der Automatisierungsstufe für eine neue Gerätegruppe.

Vollautomatisch? Um die Belastung deines SecOps-Teams zu reduzieren, möchtest du so viel wie möglich automatisieren; ein schrittweiser Übergang von der Standardeinstellung zu einem vollautomatischen Ansatz wird empfohlen. Vorsicht ist jedoch nach wie vor geboten. Auch wenn vollautomatische Antworten in unserer Erfahrung nicht zu einem Systemabsturz geführt haben, könnten sie theoretisch einen Systemabsturz verursachen oder andere Anwendungen daran hindern, korrekt zu laufen. Daher sehen wir meist, dass die vollständige Automatisierung

auf unkritischen Geräten wie allgemeinen (Büro-)Geräten eingesetzt wird. Maschinen, die zur Steuerung von Produktionssystemen benötigt werden, sind in der Regel nicht vollständig automatisiert. Dies ermöglicht eine letzte Plausibilitätsprüfung durch einen Administrator, bevor eine Korrekturmaßnahme auf diesen Geräten ergriffen wird.

Live Response

Live Response ist eine Funktion in Microsoft Defender for Endpoint, die es Sicherheitsteams ermöglicht, in Echtzeit mit einem Endpunktgerät zu interagieren, um Untersuchungen durchzuführen und Informationen über potenzielle Bedrohungen zu sammeln. Mit Live Response können Sicherheitsteams Skripte ausführen, Dateien und Prozesse überprüfen sowie Systemprotokolle und andere Informationen direkt vom Endpunkt abrufen.

Live Response ermöglicht es Sicherheitsteams, schnell Informationen über einen Vorfall zu sammeln und fundierte Entscheidungen über das weitere Vorgehen zu treffen. Wenn beispielsweise auf einem Endpunkt ein Schadprogramm erkannt wird, kann ein Sicherheitsanalyst mit Live Response das infizierte Gerät überprüfen, Dateien von dem Gerät sammeln und das Ausmaß der Kompromittierung feststellen.

Live Response ist besonders nützlich in Situationen, in denen ein herkömmliches Remote-Zugriffstool möglicherweise nicht verfügbar ist oder in denen es zu lange dauern würde, die erforderlichen Informationen auf andere Weise zu beschaffen.

Zum Zeitpunkt des Schreibens ist Live Response für alle unterstützten Betriebssysteme mit Ausnahme von Android und iOS verfügbar. Um die Funktion zu aktivieren, navigierst du zum Microsoft 365 Security Center > **Einstellungen** > **Endpunkte** > **Erweiterte Funktionen**. Suche in der Liste nach den folgenden Einstellungen:

- **Live Response**, um das Feature im Allgemeinen zu aktivieren oder zu deaktivieren.
- **Live Response für Server**, um zu steuern, ob das Feature für Server-Betriebssysteme verwendet werden kann.
- **Ausführung von nicht signierten Skripten in Live Response**, um zu steuern, ob nicht signierte Skripte remote über eine Live-Response-Sitzung ausgeführt werden können.

Die in Live Response verwendete Syntax erfordert möglicherweise eine gewisse Eingewöhnung. Wie bei allem gilt auch hier: Übung macht den Meister. Um dir den Einstieg zu erleichtern, wirf einen Blick auf einige der von Microsoft bereitgestellten [Befehlsbeispiele](#).

Ebenen durchbrechen? Live Response läuft im Systemkontext des Remote-Geräts. Daher verfügt es über viele Berechtigungen. Das bedeutet, dass derjenige, der eine Live-Response-Sitzung durchführen kann, möglicherweise auch die volle Kontrolle über das Gerät hat. In hochregulierten und sicheren Umgebungen kann dies das mehrstufige Verwaltungsmodell durchbrechen, insbesondere wenn Live Response auf so genannten Tier-0-Diensten wie

Domänencontrollern, AD FS-Servern und Entra ID Connect durchgeführt werden kann. Überlege dir, wem du die Möglichkeit geben möchtest, Live Response zu nutzen, und verwende benutzerdefinierte Rollen, wenn du Live Response nur für wenige Personen aktivieren möchtest.

Eine Verbindung zu einem Gerät ist möglich, indem du eine Geräteseite öffnest, auf die Ellipse klickst und dann „**Live Response initiieren**“ auswählst (siehe Abbildung unten) oder ähnliche Schritte im Rahmen der Untersuchung einer aktiven Warnung oder eines Vorfalls durchführst. Im letzteren Fall wird die Aktion verfügbar, wenn ein Gerät als Entität in die Warnung aufgenommen wird.

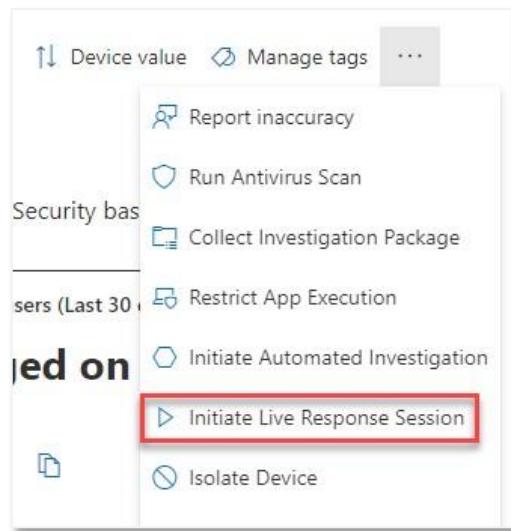


Abbildung 7-61: Starten einer Live-Response-Sitzung.

Advanced Hunting

Obwohl Hunting eine der Kernfunktionen und -fähigkeiten von Microsoft Defender for Endpoint ist, gehen Hunting-Aktivitäten weit über deine Endpunkte hinaus. Daher wird Hunting in Kapitel 12, Microsoft 365 Defender, ausführlicher besprochen.

Microsoft Defender for IoT

Mit der zunehmenden Nutzung von internetfähigen Geräten im geschäftlichen Umfeld stellt der Einsatz solcher Geräte mehrere Sicherheitsherausforderungen dar, darunter:

- **Angriffe auf die Lieferkette:** IoT-Geräte werden oft von Drittanbietern hergestellt. Diese Anbieter verfügen möglicherweise nicht über angemessene Sicherheitsmaßnahmen,

sodass Organisationen anfällig für Angriffe auf die Lieferkette sind. Selbst wenn sie es tun, sind beliebte Anbieter ein interessantes Ziel, da die Kompromittierung eines Anbieters zur leichteren Ausnutzung von Hunderten, wenn nicht Tausenden von Umgebungen weltweit führen kann.

- **Shadow IT:** Mitarbeiter bringen möglicherweise ihre eigenen IoT-Geräte mit oder verwenden nicht genehmigte Geräte, was eine potentielle Sicherheitslücke in der Organisation darstellt, insbesondere wenn diese Geräte mit dem Unternehmensnetzwerk verbunden sind.
- **Fehlende zentrale Verwaltung:** Bei vielen im Einsatz befindlichen IoT-Geräten kann es schwierig sein, sie effektiv zu verwalten und zu überwachen, sodass Sicherheitslücken entstehen, die ausgenutzt werden können. Häufig führt dies dazu, dass Geräte zwar eingesetzt, aber nie oder nur selten aktualisiert werden. Dies wiederum vergrößert die Angriffsfläche und die [Anzahl der Versuche, diese Geräte in einem Angriff zu nutzen](#).
- **Schwachstellen in Geräten:** IoT-Geräte verfügen oft über schwache Sicherheitsmechanismen und werden nicht regelmäßig mit Sicherheitspatches aktualisiert, was sie anfällig für Angriffe macht.
- **Unsichere Kommunikation:** Daten, die zwischen IoT-Geräten und Netzwerken übertragen werden, können von Angreifern abgefangen werden, was zu Datendiebstahl oder -manipulation führen kann.
- **Schwache Authentifizierung:** Viele IoT-Geräten fehlen geeignete Authentifizierungsprotokolle, so dass es für Angreifer einfacher ist, Zugang zu Unternehmensnetzwerken zu erhalten.

Der Enterprise-IoT-Markt wird in den nächsten Jahren voraussichtlich [jährlich zweistellig wachsen](#). Es ist daher nicht verwunderlich, dass auch der Einsatz von IoT – oder besser gesagt: der Missbrauch – zunimmt. Da immer mehr Organisationen einige bis viele IoT-Geräte mit ihrem Netzwerk verbinden, versuchen Angreifer immer häufiger, diese Geräte als Einstiegspunkt in eine Umgebung zu nutzen.

Was ist Microsoft Defender for IoT?

Microsoft Defender for IoT ist Microsofts Lösung, um Organisationen dabei zu helfen, Einblick in ihre Netzwerke zu gewinnen, indem sie eine Lösung bereitstellt, die die Nutzung (oder den Missbrauch) von internetfähigen Geräten erkennt und überwacht. Da nicht alle Geräte gleich sind, gibt es drei unterschiedliche Funktionen von Microsoft Defender for IoT:

- **Überwachung des Enterprise-IoT-Netzwerks:** Diese Lösung zielt auf den Einsatz von Enterprise-IoT-Geräten ab, die üblicherweise in Unternehmensnetzwerken zu finden sind. Beispiele für Geräte, die als "Enterprise IoT" gelten, sind Netzwerkkameras, netzwerkfähige Drucker, Scanner, intelligente Bürosensoren usw.
- **OT-Netzwerküberwachung**, die darauf abzielt, die Nutzung von Betriebstechnologie zu sichern, die häufiger in der Fertigung, im Gesundheitswesen, in der Logistik usw. zu finden ist. Obwohl es einige Überschneidungen zwischen IoT und OT gibt, stützt sich

letztere stark auf industrielle Steuerungen wie SPSen, proprietäre Lösungen, die oft atypische Protokolle im Vergleich zu IoT-Geräten verwenden. Beispiele für solche Protokolle sind Modbus, Optomux, Profibus, ControlNet usw.

- **IoT für Gerätehersteller** soll Geräteherstellern eine Lösung bieten, die sie auf ihren Geräten implementieren können, um Transparenz zu schaffen und die Sicherheit zu erhöhen. In gewisser Weise ähnelt der eingesetzte Agent sehr dem Microsoft Defender for Endpoint-Agenten, nur speziell für IoT-Geräte.

In diesem Kapitel konzentrierst du dich auf den Enterprise-IoT-Teil der Lösung, da dieser am stärksten in Microsoft Defender for Endpoint integriert ist.

Geräte erkennen

Ein wichtiger Bestandteil der Enterprise-IoT-Netzwerküberwachung ist die Möglichkeit, zu erkennen, welche Geräte im Netzwerk vorhanden sind. Das ist oft eine Herausforderung, da die IT nicht immer für die Verwaltung von IoT-Geräten zuständig ist und auch nicht entscheidet, welche Geräte in welchem Umfang eingesetzt werden. Im besten Fall – so meine Erfahrung – beschränkt sich die Einbindung der IT, wenn sie denn erfolgt, oft darauf, ein (getrenntes) Netzwerksegment bereitzustellen, damit die IoT-Geräte entweder untereinander oder zum Internet hin kommunizieren können.

Man kann nicht überwachen, was man gar nicht erst kennt. Daher ist es sehr wichtig herauszufinden, welche Geräte angeschlossen sind und wie ihr aktueller Zustand ist. Zum Zeitpunkt des Schreibens gibt es zwei Möglichkeiten, wie Geräte im Netzwerk entdeckt werden können:

- Nutzung der Erkennungsfunktionen von Microsoft Defender for Endpoint
- Verwendung eines dedizierten IoT-Sensors

Geräte mit Microsoft Defender for Endpoint erkennen

Dieselbe Geräteerkennung, die verwendet wird, um nach Geräten zu suchen, die in Microsoft Defender for Endpoint integriert werden können, wird auch genutzt, um andere netzwerkfähige Geräte zu finden und zu identifizieren. Sobald du ein in Microsoft Defender for Endpoint integriertes Gerät mit dem Netzwerk verbunden hast, lauscht es auch nach anderen Gerätetypen, die in den anderen Abschnitten deines Gerät-Inventars angezeigt werden:
Netzwerkgeräte, IoT-Geräte, nicht kategorisierte Geräte:



Abbildung 7-62: Geräteliste für netzwerkfähige Geräte

Der Vorteil dieses Ansatzes besteht darin, dass die IT nur sehr wenig Aufwand betreiben muss, um die Sichtbarkeit dessen zu schaffen, was mit dem Netzwerk verbunden ist. Es gibt jedoch auch einige Einschränkungen zu beachten. So überwindet die von Microsoft Defender for Endpoint verwendete Netzwerkerkennung beispielsweise keine Firewalls. Daher werden stark segmentierte Netzwerke wahrscheinlich nicht viele Ergebnisse liefern. Obwohl Firewalls so konfiguriert werden können, dass eine Geräteerkennung über Segmente hinweg möglich ist, ist das nicht immer erwünscht.

Eine andere Möglichkeit wäre, in jedem Segment, in das du Einblick gewinnen möchtest, ein MDE-integriertes Gerät einzusetzen. Obwohl das erfordert, dass du solche Geräte aufbaust und wartest, kann es deutlich einfacher (und weniger aufdringlich) sein als die Option, die wir als Nächstes besprechen werden: den Einsatz eines dedizierten Sensors.

Geräte mit einem dedizierten Sensor erkennen

Ein dedizierter Sensor ist ein Gerät oder eine virtuelle Maschine, die du im Netzwerk einsetzt und so konfigurierst, dass sie den Netzwerkverkehr von Geräten wie Switches und Firewalls mit Hilfe von SPAN (Switched Port Analyzer) oder RSPAN (Remote SPAN) überwacht.

- SPAN ermöglicht es dir, den Netzwerkverkehr von einem oder mehreren Ports zu kopieren und zur Analyse an einen anderen Port zu senden. Das ist nützlich für die Fehlerbehebung, Netzwerkanalyse und Sicherheitsüberwachung. Mit SPAN kannst du bestimmte zu überwachende Ports auswählen und den Verkehr an einen Zielport auf demselben Switch senden.
- RSPAN hingegen ermöglicht es dir, den Datenverkehr von mehreren Switches in einem Netzwerk zu überwachen. Bei RSPAN wird der Datenverkehr auf ein Remote-VLAN gespiegelt, das dann an einen Zielport auf einem anderen Switch weitergeleitet wird. Auf diese Weise kannst du den Datenverkehr auf mehreren Switches von einem einzigen Standort aus überwachen.

Je nach Größe und Komplexität deines Netzwerks kann die Konfiguration von SPAN/RSPAN einen erheblichen Aufwand erfordern, insbesondere wenn du mehrere VLANs überwachen möchtest. Andererseits benötigst du nur einen einzigen Sensor, der den gesamten Datenverkehr analysiert, den er empfängt – was möglicherweise einfacher zu warten ist als mehrere MDE-integrierte Geräte im gesamten Netzwerk.

Single Point of Failure: Beim Einsatz eines einzelnen Sensors ist zu beachten, dass es sich um einen Single Point of Failure handelt. Bei Ausfällen wird kein Datenverkehr mehr an Microsoft Defender for IoT zur Analyse gesendet, so dass man (vorübergehend) blind ist.

Einrichten von Microsoft Defender for Enterprise IoT

Wie bereits erwähnt, musst du nichts tun, um Defender for (Enterprise) IoT einzurichten, wenn du MDE-integrierte Geräte hast – netzwerkfähige Geräte werden automatisch erkannt. Der Sensor erfordert jedoch einige zusätzliche Schritte:

1. Navigiere in den Einstellungen von Microsoft Defender for Endpoint zu **Geräte-Erkennung > Enterprise IoT**. Erstelle dort einen Plan nur für Enterprise IoT. Du kannst auch einen Plan für Enterprise IoT und OT erstellen, aber das sprengt vorerst den Rahmen. Der Defender for IoT-Plan wird in Azure erstellt, was du überprüfen kannst, indem du das Azure-Portal öffnest und zu **Microsoft Defender for IoT > Pläne und Preise** navigierst.
2. Sobald du einen Plan hast, solltest du den Sensor in deinem lokalen Netzwerk einsetzen. Der Sensor ist ein Paket, das auf Ubuntu Server installiert werden muss. Du kannst den Sensor sowohl virtuell als auch als physischen Server betreiben. Letzteres kann in größeren Netzwerken erforderlich sein, in denen mehr Durchsatz und Kapazität benötigt werden. Um einen Sensor zu integrieren, navigiere zu **Standorte und Sensoren** und klicke auf **Sensor integrieren**. Folge den Anweisungen auf dem Bildschirm, um den Sensor mit dem eindeutigen Befehl zu installieren, der für dich generiert wird.

Sobald der Sensor installiert wurde, wird er in der Liste der integrierten Sensoren angezeigt, wie unten dargestellt:

	Sensor name	Sensor type	Zone	Subscription ...	Sensor health
<input type="checkbox"/>	Enterprise-network - Enterprise network				
<input type="checkbox"/>	LAB	EIoT	default	Microsoft Azure !	 Healthy

Abbildung 7-63: Überprüfung des Defender for IoT-Sensorstatus.

Kurz darauf wirst du sehen, dass Geräte im **Geräte-Inventar** auftauchen. Diese Informationen werden automatisch mit Microsoft 365 Defender geteilt, sodass die Geräte auch dort angezeigt werden.

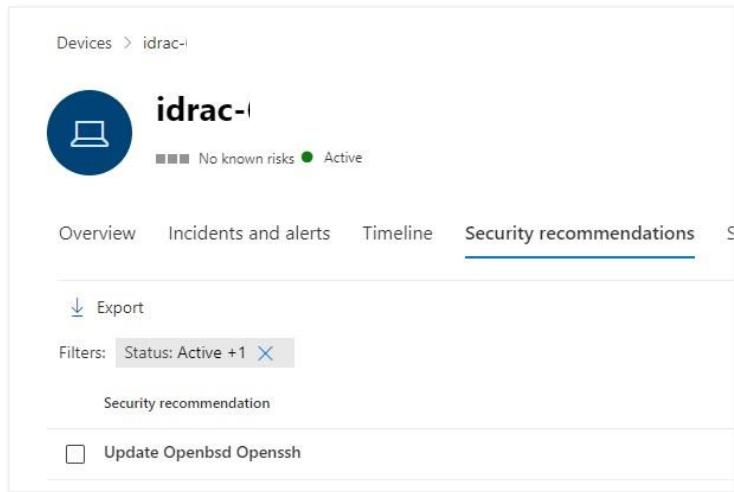
Duplikate en masse: Einer der Nachteile, dass sowohl MDE als auch der Sensor Geräte erkennen können, ist, dass die Oberfläche in Azure (Microsoft Defender for IoT) möglicherweise mehrere doppelte Geräte anzeigt - eines, das von einem MDE-integrierten Gerät entdeckt wurde, ein anderes vom Sensor erkannt. Behalte dies im Hinterkopf, bis Microsoft beschließt, das Geräte-Inventar zu bereinigen. In Microsoft 365 Defender wird es jedoch keine Duplikate geben.

IoT-Geräte überprüfen

Nachdem Geräte erkannt wurden, versucht Defender for IoT, einen Schwachstellenbericht basierend auf den Informationen zu erstellen, die er aus dem Netzwerkverkehr sammeln kann. Die Ergebnisse sind jedoch nicht immer konsistent. Während Defender oft in der Lage ist, das Modell, die Marke und die Version des Geräts zu bestimmen, gelingt es ihm manchmal nicht, für bestimmte Geräte Informationen zu Schwachstellen oder Sicherheitsempfehlungen bereitzustellen. Für einige Geräte liefert er wiederum zahlreiche Sicherheitsempfehlungen.

So konnte Defender for IoT während meiner Tests beispielsweise keine Informationen über Schwachstellen oder Sicherheitsempfehlungen für meine Ubiquiti-Netzwerkgeräte oder eine meiner FortiGate-Firewalls bereitstellen, obwohl sie eine ältere Betriebssystemversion mit bekannten Schwachstellen ausführten. Andererseits erkannte es erfolgreich mehrere Schwachstellen im iDRAC (Dell) meines Heimlabor-Servers und gab Empfehlungen zu deren Behebung.

Während Defender for IoT ein nützliches Werkzeug zur Erkennung von Schwachstellen und zur Gewährleistung der Netzwerksicherheit ist, kann seine Leistung inkonsistent sein, und du solltest bei der Interpretation der Ergebnisse vorsichtig sein. Wie viele andere ähnliche Lösungen gibt es noch einige Herausforderungen zu bewältigen, aber die Lösung hat sich in den letzten Monaten bereits deutlich verbessert.



The screenshot shows the Microsoft Defender for Endpoint interface for an IoT device named 'idrac-1'. The device status is 'No known risks' and 'Active'. The 'Security recommendations' tab is selected. A single recommendation is listed: 'Update Openbsd Openssh'. There is also an 'Export' button and a 'Filters' section.

Abbildung 7-64: Überprüfung der Sicherheitsempfehlungen für IoT-Geräte.

Über den Endpunkt und IoT hinaus

In diesem Kapitel hast du gesehen, auf welche Weise Microsoft Defender for Endpoint deine Geräte vor der Vielzahl von Bedrohungen schützen kann, mit denen sie täglich konfrontiert sind. Natürlich gibt es noch viele weitere Dinge zu beachten – nicht nur innerhalb von Microsoft 365 oder auf dem Gerät selbst. Im nächsten Kapitel beschäftigen wir uns mit Microsoft Cloud App Security, einem Cloud Application Security Broker, der nicht nur darauf ausgelegt ist, Aktivitäten innerhalb deiner eigenen Microsoft 365-Umgebung abzusichern, sondern dies auch auf andere Cloud-Anwendungen auszuweiten und dabei die Leistungsfähigkeit des gesamten Ökosystems durch seine Integrationen mit Microsoft Defender for Endpoint, Microsoft Defender for Identity und mehr zu nutzen.