Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów

◫ Poziom: średnio

◫ Dotyczy: Microsoft Defender for Business, Windows 11, Intune (Endpoint security)

▯ Czas: ~45 min

Polityki ochrony ustawiają, jak Defender zachowuje się na stacji: co skanuje, co blokuje i czego nie wolno wyłączyć użytkownikowi. Ta strona opisuje zalecane ustawienia, ochronę przed manipulacją, reguły ASR z trybem audytu, wykluczenia, ochronę sieci i filtrowanie treści oraz kontrolowany dostęp do folderów przeciw ransomware.

◫ Skróty użyte na tej stronie (6)

Skrót	Co znaczy
ASR	Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii
FAQ	Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
GUID	Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera
LSASS	Local Security Authority Subsystem Service: proces Windows przechowujący w pamięci dane logowania, częsty cel kradzieży haseł
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Komendy PowerShell wykonujemy na stacji w oknie administratora, a w środowisku zarządzanym używamy ich tylko do odczytu albo do testów na stacji pilotażowej. Trwałe ustawienia zapisujemy w politykach.

> Nazwy menu w portalach Microsoftu bywają zmieniane, a opisy poniżej odpowiadają stanowi z października 2026. Układ ustawień w Intune zmienia się częściej niż w portalu Defender, więc nazwy pozycji sprawdzamy w katalogu ustawień.

□□ KLIKAMY W INTERFEJSIE

Otwarcie domyślnych polityk w portalu Defender

```
security.microsoft.com → Endpoints → Configuration management → Device configuration
```

Lista pokazuje polityki według systemu i typu. Domyślnie są dwie: ochrona nowej generacji i zapora. W Intune te same polityki są widoczne jako Antivirus i Firewall (zapora ma dwie polityki: ochronę i reguły własne).

□□ KLIKAMY W INTERFEJSIE

Wybór miejsca zarządzania politykami

```
security.microsoft.com → Endpoints → Configuration management → Device configuration
→ komunikat: kontynuujemy w Intune albo przechodzimy na uproszczoną konfigurację w
portalu Defender
```

Jedno miejsce zarządzania na całą firmę. Przy przejściu z Intune na portal Defender wcześniej usuwamy istniejące polityki z Intune, bo inaczej się dublują.

□□ KLIKAMY W INTERFEJSIE

Włączenie ochrony przed manipulacją

```
security.microsoft.com → Settings → Endpoints → General → Advanced features
→ Tamper protection: On → Save preferences
```

Dokumentacja Business zaleca włączenie. Ustawienie w Intune (profil Windows Security experience, ustawienie Tamper Protection) obejmuje urządzenia wybranych grup.

🔍 TYLKO ODCZYT

Sprawdzenie ochrony przed manipulacją na stacji: IsTamperProtected

```
Get-MpComputerStatus | Select-Object IsTamperProtected, RealTimeProtectionEnabled
```

Przykład:

```
IsTamperProtected RealTimeProtectionEnabled
----------------- -------------------------
             True                      True
```

🔍 TYLKO ODCZYT

Odczyt kluczowych ustawień ochrony: Get-MpPreference

```
Get-MpPreference | Select-Object MAPSReporting, CloudBlockLevel, PUAProtection,
SubmitSamplesConsent, DisableRealtimeMonitoring, DisableBehaviorMonitoring,
EnableNetworkProtection, EnableControlledFolderAccess
```

Przykład z laptopa `lt-kasia`:

```
MAPSReporting               : 2
CloudBlockLevel             : 0
PUAProtection               : 1
SubmitSamplesConsent        : 1
DisableRealtimeMonitoring   : False
DisableBehaviorMonitoring   : False
EnableNetworkProtection     : 1
EnableControlledFolderAccess: 2
```

Wartości liczbowe: `MAPSReporting` 2 to zaawansowana ochrona w chmurze, `PUAProtection` 1 to blokowanie niechcianych aplikacji, `EnableNetworkProtection` 1 to blokowanie, a `EnableControlledFolderAccess` 2 to tryb audytu.

TYLKO ODCZYT

Sprawdzenie stanu zapory: Get-NetFirewallProfile

```
Get-NetFirewallProfile | Select-Object Name, Enabled
```

Wszystkie trzy profile (Domain, Private, Public) mają mieć `Enabled` równe `True`. Raport zapory w portalu jest dostępny w Reports → Endpoints → Firewall po skonfigurowaniu polityki zapory.

KLIKAMY W INTERFEJSIE

Utworzenie polityki reguł ASR w Intune

```
intune.microsoft.com → Endpoint security → Attack surface reduction → Create policy
→ Platform: Windows, Profile: Attack Surface Reduction Rules
→ każdą regułę ustawiamy na Audit (nie na Block), przypisujemy do grupy pilotażowej
```

Dokumentacja FAQ Defender for Business podaje, że reguły ASR i kontrolowany dostęp do folderów konfigurujemy w centrum administracyjnym Intune. Ogólna dokumentacja ASR dopuszcza też szablon w portalu Defender (Endpoints → Configuration management → Endpoint security policies, szablon Attack surface reduction rules). W naszym tenancie sprawdzamy, który z nich jest dostępny.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Create policy dla profilu Attack Surface Reduction Rules w Intune, widoczna lista reguł z wybranym trybem Audit przy każdej z nich i przypisana grupa pilotażowa.

ASR = Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii · **FAQ** = Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami

ZMIENIA SYSTEM

Włączenie reguły ASR w trybie audytu na stacji pilotażowej

```
Add-MpPreference -AttackSurfaceReductionRules_Ids IdentyfikatorReguly -
AttackSurfaceReductionRules_Actions AuditMode
```

> (gdzie `IdentyfikatorReguly` to GUID reguły z tabeli w sekcji Jak to działa, a `AuditMode` zamieniamy na `Enabled` dla blokowania albo `Warn` dla ostrzeżenia)

Lokalna zmiana służy wyłącznie do testu na jednej stacji. Polityka z Intune ma pierwszeństwo, więc trwałe ustawienia zapisujemy tam.

ASR = Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii · **GUID** = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera

TYLKO ODCZYT

Odczyt skonfigurowanych reguł ASR: Get-MpPreference

```
$p = Get-MpPreference; 0..($p.AttackSurfaceReductionRules_Ids.Count-1) | ForEach-Object
{ [pscustomobject]@{Id=$p.AttackSurfaceReductionRules_Ids[$_];
Action=$p.AttackSurfaceReductionRules_Actions[$_]} } | Format-Table -AutoSize
```

Przykład:

```
Id                                   Action
--                                   ------
56a863a9-875e-4185-98a7-b882c64b5ce5      1
9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2      1
e6db77e5-3df2-4cf1-b95a-636979351e5b      1
be9ba2d9-53ea-4cdc-84e5-9b1eeee46550      2
```

Wartość akcji: 0 wyłączona, 1 blokowanie, 2 audyt, 5 nieskonfigurowana, 6 ostrzeżenie.

ASR = Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii

□□ TYLKO ODCZYT

Odczyt zdarzeń audytu ASR: Get-WinEvent

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows
Defender/Operational'; Id=1122} -MaxEvents 20 | Select-Object TimeCreated, Message
```

Zdarzenie 1122 oznacza, że reguła w trybie audytu wykryłaby działanie i je zablokowała. Przegląd zbiorczy dla całej floty daje raport w portalu.

□□ **ASR** = Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii

□□ KLIKAMY W INTERFEJSIE

Otwarcie raportu ASR

```
security.microsoft.com → Reports → Endpoints → Attack surface reduction rules
→ zakładki: Detections, Configuration, Add exclusions
```

W Defender for Business nie ma advanced hunting, więc ten raport i dziennik zdarzeń na stacji to dwa główne źródła do oceny audytu.

□□ **ASR** = Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii

□□ ZMIENIA SYSTEM

Włączenie kontrolowanego dostępu do folderów w trybie audytu

```
Set-MpPreference -EnableControlledFolderAccess AuditMode
```

Tryb audytu zapisuje próby dostępu, nie blokując ich. Po zebraniu danych przełączamy na `Enabled`. Wyłączenie to `Disabled`.

□□ ZMIENIA SYSTEM

Dodanie programu dozwolonego i folderu chronionego

```
Add-MpPreference -ControlledFolderAccessAllowedApplications "SciezkaDoProgramu"
Add-MpPreference -ControlledFolderAccessProtectedFolders "SciezkaDoFolderu"
```

> (gdzie `SciezkaDoProgramu` to pełna ścieżka pliku wykonywalnego, któremu pozwalamy zapisywać w chronionych folderach, a `SciezkaDoFolderu` to dodatkowy folder chroniony)

TYLKO ODCZYT

Odczyt zdarzeń kontrolowanego dostępu do folderów

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-Windows
Defender/Operational'; Id=1123,1124} -MaxEvents 20 | Select-Object TimeCreated, Id,
Message
```

Zdarzenie 1124 to audyt, a 1123 to zablokowanie próby zapisu.

ZMIENIA SYSTEM

Włączenie ochrony sieci w trybie audytu

```
Set-MpPreference -EnableNetworkProtection AuditMode
```

Trwała polityka powstaje w Intune: Endpoint security → Attack surface reduction → Create policy. Po kilku dniach audytu przełączamy na `Enabled`.

KLIKAMY W INTERFEJSIE

Utworzenie polityki filtrowania treści www

```
security.microsoft.com → Settings → Endpoints → Rules → Web content filtering → + Add
policy
→ nazwa i opis
→ kategorie do blokowania (bez kategorii Uncategorized)
→ zapis (odświeżenie do dwóch godzin)
```

Polityka bez zaznaczonych kategorii działa w trybie samego audytu. W Defender for Business obowiązuje jedna polityka na całą organizację i brak zawężania do grup urządzeń.

□□ KLIKAMY W INTERFEJSIE

Sprawdzenie ochrony sieci testową stroną

```
Edge albo Chrome → smartscreentestratings2.net
→ w trybie blokowania strona jest zablokowana, zdarzenie widać w raporcie Reports →
Endpoints → Web protection
```

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Piątek, 16:05. Pani Halina dzwoni, że Optima nie może wyeksportować zestawienia do folderu Dokumenty, a komunikat mówi o braku uprawnień. Tomek sprawdza zdarzenia i widzi 1123: kontrolowany dostęp do folderów zablokował zapis, bo wczoraj przełączył go z audytu na blokowanie bez przeglądu logu. Dopisuje program Optimy do listy dozwolonych w polityce, a w poniedziałek wraca do zasady: najpierw audyt, potem blokowanie.

Jak to działa

□□ Rozwiń: jak to działa pod spodem

Pojęcie: ochrona nowej generacji. Antywirus Defendera, który łączy sygnatury, analizę zachowania procesów i ochronę z chmury. Nowa generacja oznacza, że decyzję o podejrzanym pliku często podejmuje chmura w ułamku sekundy, a nie lokalna lista wzorców.

Pojęcie: ochrona przed manipulacją (tamper protection). Blokada, która nie pozwala złośliwemu programowi (ani nieostrożnemu administratorowi) wyłączyć ochrony

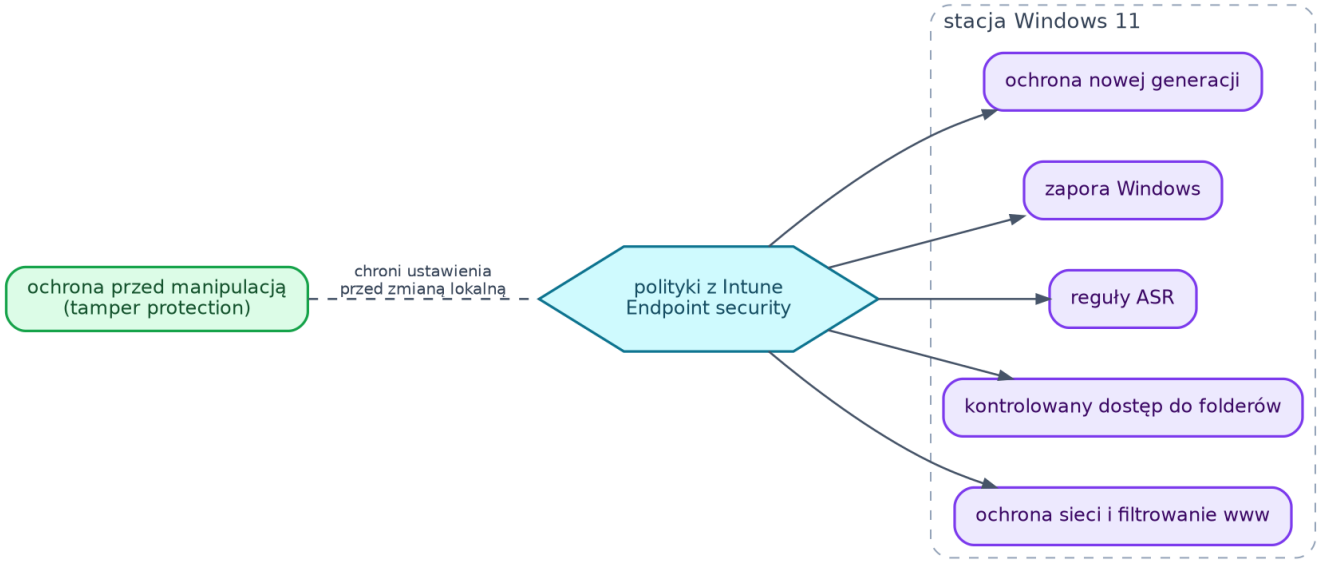
w czasie rzeczywistym, monitorowania zachowania, ochrony w chmurze ani aktualizacji sygnatur. Przy włączonej blokadzie nie da się też lokalnie dodawać wykluczeń antywirusa.

Pojęcie: reguły ASR (Attack Surface Reduction). Reguły redukcji powierzchni ataku blokują zachowania, których zwykłe programy nie potrzebują, a z których korzysta złośliwe oprogramowanie: uruchamianie plików z makr Office, kradzież poświadczeń z procesu LSASS, ukryte skrypty. Każda reguła ma tryb: wyłączona, blokowanie, audyt, ostrzeżenie (użytkownik może odblokować na 24 godziny) albo nieskonfigurowana.

Pojęcie: kontrolowany dostęp do folderów. Mechanizm przeciw ransomware: zapisywać w chronionych folderach (Dokumenty, Obrazy, Wideo, Muzyka, Ulubione i ich odpowiedniki publiczne) mogą tylko zaufane programy. Przekierowane foldery, na przykład przez OneDrive Known Folder Move, są chronione w nowym miejscu.

Pojęcie: ochrona sieci i filtrowanie treści. Ochrona sieci blokuje połączenia wychodzące do domen i adresów o złej reputacji na poziomie systemu. Filtrowanie treści www opiera się na niej: w Edge działa przez SmartScreen, w Chrome, Firefox, Brave i Operze przez ochronę sieci.

Wszystkie elementy działają na jednej stacji i są dostarczane przez polityki. Ochrona przed manipulacją pilnuje, żeby zmiany lokalne ich nie obeszły.



Polityki z Intune rozdają ustawienia ochrony nowej generacji, zapory, ASR, kontrolowanego dostępu do folderów i ochrony sieci, a ochrona przed manipulacją blokuje zmiany lokalne (kliknięcie otwiera pełny rozmiar)

Warunek: Defender Antivirus w trybie aktywnym

Reguły ASR, ochrona sieci i kontrolowany dostęp do folderów działają tylko wtedy, gdy Defender Antivirus jest głównym antywirusem w trybie aktywnym, z włączoną ochroną w czasie rzeczywistym i ochroną w chmurze. W trybie pasywnym (stacje ze starym McAfee/Trellix) te mechanizmy nie działają, co opisuje strona Onboarding urządzeń: Intune, skrypt lokalny, GPO, serwery i Linux.

Najważniejsze reguły ASR

Trzy reguły Microsoft nazywa standardowymi regułami ochrony i zaleca włączanie ich w trybie blokowania bez długich testów. Pozostałe najpierw uruchamiamy w audycie. Identyfikatory poniżej pochodzą ze strony referencyjnej Microsoftu z października 2026, a przed użyciem w polityce porównujemy je z aktualną stroną „Attack surface reduction rules reference".

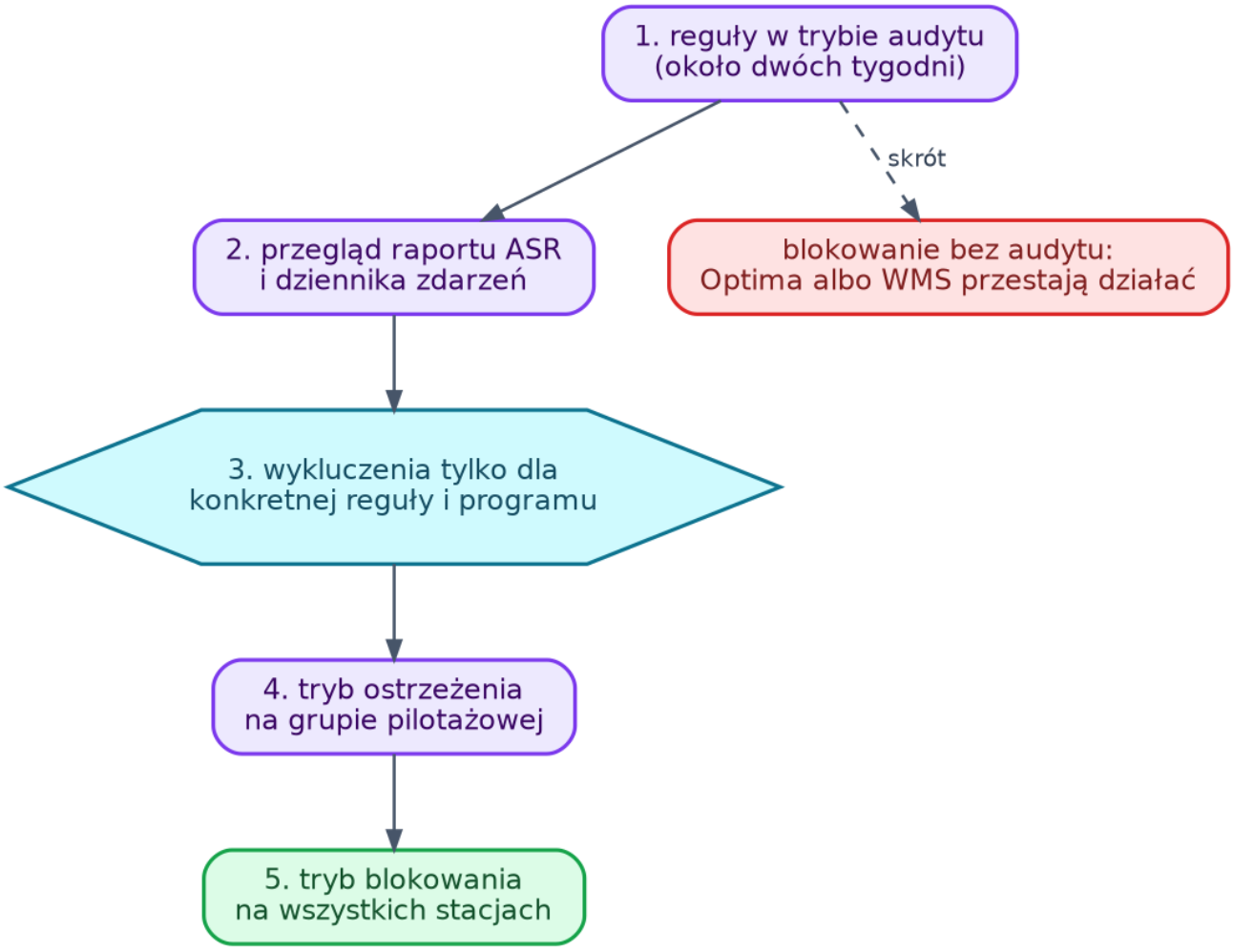
Reguła	Identyfikator	Uwaga dla Zielonej
Block abuse of exploited vulnerable signed drivers (Device)	`56a863a9-875e-4185-98a7-b882c64b5ce5`	standardowa, blokowanie

Reguła	Identyfikator	Uwaga dla Zielonej
Block credential stealing from the Windows local security authority subsystem	`9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2`	standardowa, blokowanie
Block persistence through WMI event subscription	`e6db77e5-3df2-4cf1-b95a-636979351e5b`	standardowa, blokowanie
Block executable content from email client and webmail	`be9ba2d9-53ea-4cdc-84e5-9b1eeee46550`	zwykle bezpieczna, audyt tydzień
Block all Office applications from creating child processes	`d4f940ab-401b-4efc-aadc-ad5f3c50688a`	sprawdzamy makra Optimy i arkusze działu handlowego
Block Office applications from creating executable content	`3b576869-a4ec-4529-8536-b80a7769e899`	audyt, potem blokowanie
Block Office applications from injecting code into other processes	`75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84`	audyt, potem blokowanie
Block Win32 API calls from Office macros	`92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b`	audyt, makra w starych arkuszach
Block execution of potentially obfuscated scripts	`5beb7efe-fd9a-4556-801d-275e5ffc04cc`	audyt, część własnych skryptów zespołu Oli
Block JavaScript or VBScript from launching downloaded executable content	`d3e037e1-3eb8-44c8-a917-57927947596d`	audyt
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	`01443614-cd74-433a-b99e-2ecdc07bfc25`	najczęściej daje alarmy na własne programy, długi audyt
Use advanced protection against ransomware	`c1db55ab-c21a-4637-bb3f-a12568109d35`	audyt, potem blokowanie
Block process creations originating from PSExec and WMI commands	`d1e49aac-8f56-4280-b9ba-993a6d77406c`	wpływa na zdalne narzędzia administracyjne, audyt obowiązkowy
Block untrusted and unsigned processes that run from USB	`b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4`	skanery z magazynu w Swarzędzu
Block Adobe Reader from creating child processes	`7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c`	audyt
Block Office communication application from creating child processes	`26190899-1602-49e8-8b27-eb1d0a1ce869`	audyt
Block Webshell creation for Servers	`a8f5898e-1dc8-49a9-9878-85004b8a61e6`	tylko serwery

Microsoft dodaje nowe reguły, na przykład blokowanie restartu w trybie awaryjnym i użycia podmienionych narzędzi systemowych. Pełną listę sprawdzamy na stronie referencyjnej.

Tryb audytu przed blokowaniem

Microsoft zaleca blokowanie standardowych reguł bez wielkich testów, a pozostałe reguły najpierw w audycie. Audyt udaje blokowanie, ale tylko zapisuje zdarzenie, więc nikomu nie przeszkadza w pracy.



Pięć etapów wdrożenia reguł ASR: audyt, przegląd raportu, wykluczenia dla konkretnej reguły, tryb ostrzeżenia na grupie pilotażowej i blokowanie, oraz skrót prowadzący do awarii Optimy (kliknięcie otwiera pełny rozmiar)

W Zielonej przyjmujemy dwa tygodnie audytu, bo zawierają zamknięcie miesiąca, kiedy Optima pracuje najintensywniej i najbardziej ujawnia niepożądane skutki. Po audycie reguły przechodzą w tryb ostrzeżenia dla grupy pilotażowej, a potem w blokowanie.

Wykluczenia i ich ryzyko

Wykluczenia są trzech rodzajów. Wykluczenia antywirusa Defendera nie są honorowane przez wszystkie reguły ASR, ale wszystkie reguły honorują wykluczenia procesów. Globalne wykluczenia ASR działają dla wszystkich reguł. Wykluczenia dla pojedynczej reguły są najbezpieczniejsze, bo zawężają obejście do jednej reguły i jednego programu; obsługują je GPO, polityki w Intune i polityki w portalu Defender.

Każde wykluczenie to dziura w ochronie. Dlatego wykluczamy konkretny proces, a nie cały katalog, zapisujemy w polityce powód i osobę, która je zatwierdziła, i przeglądamy listę co kwartał. Przy włączonej ochronie przed manipulacją polecenie `Add-MpPreference -ExclusionPath` wykonane lokalnie jest blokowane, więc wykluczenia trzymamy w politykach, tak jak sugeruje strona Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM.

Kontrolowany dostęp do folderów przeciw ransomware

Domyślnie chronione są Dokumenty, Ulubione, Muzyka, Obrazy i Wideo użytkownika oraz publiczne odpowiedniki, a także sektory rozruchowe dysku. Mamy pięć trybów: wyłączony (0), włączony (1), audyt (2), blokowanie tylko modyfikacji sektorów dysku (3) i audyt modyfikacji sektorów (4). Zalecana kolejność jest ta sama co przy ASR: audyt, przegląd zdarzeń 1124, uzupełnienie listy dozwolonych programów, potem tryb 1.

Na stacjach Zielonej, na których użytkownicy zapisują dane w Dokumentach przekierowanych do OneDrive, kontrolowany dostęp obejmuje ten sam folder w nowym miejscu. Programy księgowe, WMS i aplikacje własnego zespołu trafiają na listę dozwolonych w polityce, a nie w komendach lokalnych.

Częste błędy

Objaw	Przyczyna	Co robimy
Reguły ASR „włączone", a w raporcie brak detekcji	Defender Antivirus jest w trybie pasywnym (stary antywirus)	sprawdzamy `AMRunningMode`, najpierw kończymy migrację z innego produktu
Optima nie zapisuje plików do Dokumentów	kontrolowany dostęp do folderów blokuje nieznany program	przeglądamy zdarzenie 1123, dopisujemy program do dozwolonych w polityce

Objaw	Przyczyna	Co robimy
Lokalne `Add-MpPreference -ExclusionPath` nie działa	ochrona przed manipulacją blokuje zmianę	wykluczenie wprowadzamy w polityce Intune, a nie lokalnie
Reguła PSExec i WMI zatrzymuje zdalne narzędzia administracyjne	blokuje tworzenie procesów przez te mechanizmy	zostaje w audycie, wykluczamy konkretny proces administracyjny albo rezygnujemy z reguły dla serwerów
Polityka z Intune nie zmienia ustawień na stacji	polityka w portalu Defender i w Intune konfliktują, albo jeden program zarządza lokalnie	wybieramy jedno miejsce zarządzania i usuwamy duplikaty
Filtrowanie www nie działa w Chrome	wyłączona ochrona sieci	włączamy ochronę sieci w trybie blokowania
Filtrowanie dotyka wszystkich użytkowników	w Defender for Business jest jedna polityka na organizację	zawężamy kategorie do tych bez wyjątków albo różnicujemy dostęp na zaporze `fw01`
Ustawienia ASR w Intune i GPO różnią się	to samo ustawienie z dwóch źródeł	zostawiamy jedno źródło, w Zielonej Intune

□□ Ćwiczenia

1. Chcemy włączyć blokowanie reguły o identyfikatorze `d4f940ab-401b-4efc-aadc-ad5f3c50688a`. Jak postępujemy?

Odpowiedź

Reguła nie należy do standardowych, więc najpierw włączamy ją w trybie audytu w polityce dla grupy pilotażowej, przez dwa tygodnie obserwujemy raport ASR i zdarzenia 1122, dopisujemy wykluczenia dla konkretnych programów i dopiero potem przechodzimy na ostrzeżenie i blokowanie.

1. `Get-MpComputerStatus` pokazuje `AMRunningMode: Passive` na laptopie z McAfee. Co to znaczy dla reguł ASR?

Odpowiedź

W trybie pasywnym reguły ASR, ochrona sieci i kontrolowany dostęp do folderów nie działają. Nawet gdy polityka jest przypisana, nic nie jest blokowane, więc ocena audytu na takiej stacji niczego nie pokaże.

1. Dlaczego wykluczenie dla pojedynczej reguły jest lepsze niż globalne?

Odpowiedź

Obejście dotyczy tylko jednej reguły i jednego programu, a pozostałe reguły nadal chronią ten sam program. Globalne wykluczenie omija wszystkie reguły ASR naraz.

Powiązane: Onboarding urządzeń: Intune, skrypt lokalny, GPO, serwery i Linux · Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie · Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM · Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia

Źródła: Microsoft Learn, „Set up and review security policies in Microsoft Defender for Business" · Microsoft Learn, „Review and edit settings in Microsoft Defender for Business" · Microsoft Learn, „Web content filtering in Microsoft Defender for Business" · Microsoft Learn, „Attack surface reduction rules overview", „reference", „deployment" i „configure" (learn.microsoft.com/defender-endpoint) · Microsoft Learn, „Controlled folder access" · Microsoft Learn, „Network protection" · Microsoft Learn, „Prevent changes to security settings with tamper protection" · Microsoft Learn, „Microsoft Defender Antivirus compatibility with other security products" · Microsoft Learn, „Microsoft Defender for Business FAQ"

Revision #15
Created 2026-10-03 11:23:16 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:03 UTC by Tomasz Konieczny