Ochrona stacji

Pojęcia, konsola zarządzania i typowe problemy.

- Ochrona stacji: od wirusa Brain do EDR
- Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia
- Agent ochrony na serwerach Linux: instalacja i weryfikacja
- Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM
- ePolicy Orchestrator: konsola zarządzania
- Ochrona stacji: utrzymanie i typowe problemy

Ochrona stacji: od wirusa Brain do EDR

Poziom: podstawy

Dotyczy: dowolny produkt ochrony stacji końcowych, McAfee/Trellix ePO, Microsoft Defender for Endpoint

Czas: ~15 min

Ta strona otwiera książkę o ochronie stacji końcowych: skąd wziął się pomysł skanowania plików w poszukiwaniu wirusów, dlaczego dzisiejsze produkty obserwują zachowanie procesu zamiast tylko porównywać pliki z listą, i co czeka na kolejnych stronach.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
IBM	International Business Machines: firma, w której laboratorium powstał model relacyjny i pierwszy działający silnik SQL
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
RPC	Remote Procedure Call: sposób, w jaki programy wywołują funkcje na innym komputerze w sieci; kontrolery domeny używają go między innymi do replikacji
XDR	Extended Detection and Response: rozszerzenie EDR na wiele źródeł danych naraz (stacje, sieć, poczta): ma ramkę Pojęcie w tekście, ale brakuje w słowniku

Skąd się wzięło

19 stycznia 1986 roku dwaj bracia z Lahaur w Pakistanie, Basit i Amjad Farooq Alvi, wypuścili program o nazwie Brain, pierwszy wirus napisany pod komputery zgodne z IBM PC. Program podmieniał sektor rozruchowy dyskietki, przenosił oryginalny kod w inne miejsce i oznaczał je jako uszkodzone, a w treści zostawiał numery telefonów i adres autorów z prośbą o kontakt w sprawie „szczepionki”. Bracia twierdzili później, że chodziło im wyłącznie o ochronę własnego oprogramowania medycznego przed nielegalnym kopiowaniem, nie o szkodzenie komukolwiek, i że

byli zaskoczeni, kiedy telefon zaczął dzwonić z Wielkiej Brytanii i Stanów Zjednoczonych.

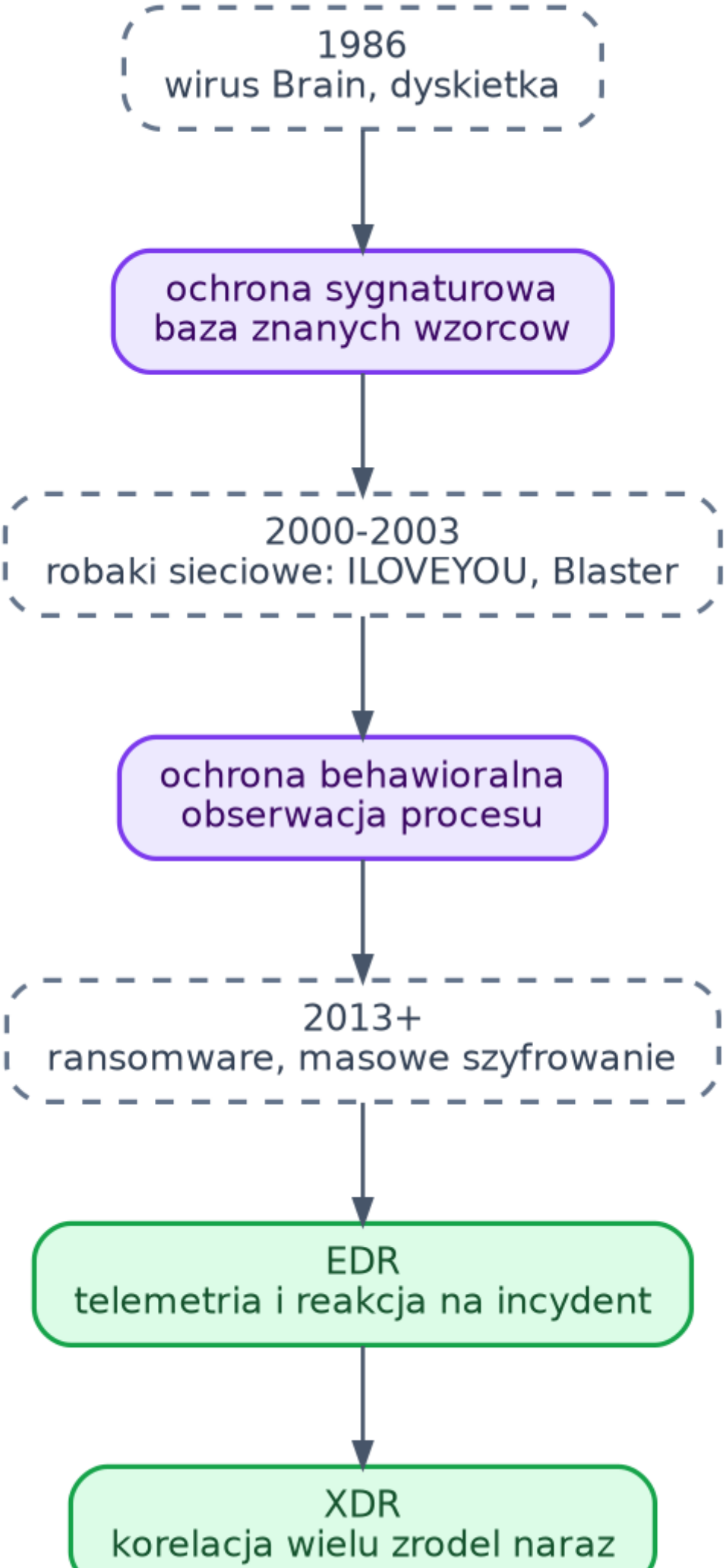
Rok później, w 1987 roku, John McAfee założył firmę i wypuścił VirusScan, jeden z pierwszych komercyjnych programów antywirusowych: porównywał zawartość pliku z listą znanych wzorców złośliwego kodu, czyli sygnatur. Przez kolejną dekadę ten mechanizm wystarczał, bo nowe zagrożenia powstawały powoli, a aktualizacja bazy raz na jakiś czas nadążała za tempem ich pojawiania się.

Internet zmienił tę matematykę. 4 maja 2000 roku e-mail z załącznikiem podszywającym się pod list miłosny obiegł świat w kilka godzin, infekując miliony komputerów samym tylko rozsyłaniem się do każdego kontaktu z książki adresowej ofiary: robak zapamiętany później jako ILOVEYOU. 11 sierpnia 2003 roku robak Blaster wykorzystał lukę w usłudze RPC Windows, załataną miesiąc wcześniej, i zainfekował setki tysięcy komputerów bez żadnego kliknięcia użytkownika, samym podłączeniem do sieci. Tempo tych epidemii pokazało, że baza sygnatur aktualizowana raz dziennie zawsze będzie spóźniona o te kilka godzin, w których szkoda już się dzieje.

Odpowiedzią stała się ochrona behawioralna: zamiast pytać, czy plik figuruje na liście znanych zagrożeń, produkt zaczął pytać, czy proces właśnie robi coś, czego zwykły program nie robi. Fala ransomware z lat 2013 do 2017, od CryptoLockera po WannaCry w maju 2017 (rozprzestrzeniającego się przez tę samą rodzinę luk w usłudze sieciowej Windows co Blaster czternaście lat wcześniej), pokazała, że samo zablokowanie podejrzanego procesu też nie wystarcza. Administrator potrzebuje wiedzieć, co dokładnie działo się na stacji, zanim doszło do wykrycia, i mieć narzędzie do reakcji, nie tylko do alarmu. Stąd EDR, rozszerzenie antywirusa o ciągłą telemetrię i reakcję na incydent, a później XDR, łączący tę telemetrię ze stacji z danymi z sieci, poczty i tożsamości w jednym miejscu.

Jak to działa w jednym obrazku

Trzy kolejne warstwy z historii wyżej nie zastępują się nawzajem, tylko się na siebie nakładają: dzisiejszy produkt ochrony stacji wciąż ma w sobie silnik sygnaturowy z lat 80., dokłada do niego analizę behawioralną z przełomu wieków, a na wierzchu stawia telemetrię i reakcję EDR z ostatniej dekady. Pełny słownik tych pojęć, razem z rozróżnieniem antywirusa, EDR i XDR, stoi na stronie Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia.

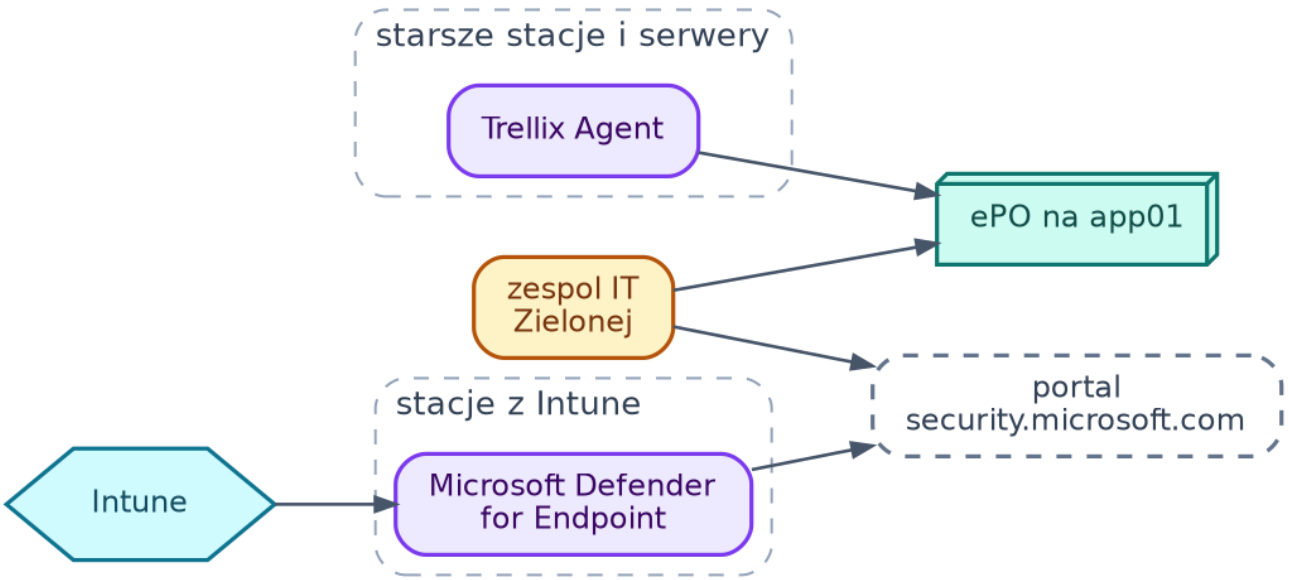

1986
wirus Brain, dyskietka
ochrona sygnaturowa
baza znanych wzorcow
2000-2003
robaki sieciowe: ILOVEYOU, Blaster
ochrona behawioralna
obserwacja procesu
2013+
ransomware, masowe szyfrowanie
EDR
telemetria i reakcja na incydent
XDR
korelacja wielu zrodel naraz

Ewolucja ochrony stacji od wirusa Brain przez sygnatury i analizę behawioralną do EDR i XDR (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Czwartek, 11:20. Kasia w terenie otwiera na laptopie e-mail „pilna faktura do opłacenia” z załącznikiem `faktura.zip`, bo nazwa nadawcy wygląda znajomo. Sekundę po rozpakowaniu Microsoft Defender for Endpoint blokuje skrypt uruchomiony z archiwum i izoluje proces, zanim ten zdąży dotknąć dysku, a zdarzenie ląduje w konsoli zespołu IT z pełną historią tego, co plik próbował zrobić. Gdyby laptop miał tylko ochronę sygnaturową sprzed tygodnia, ten konkretny wariant mógłby przejść bez żadnego alarmu, bo świeżo złożony z gotowych narzędzi plik `.zip` nie figurował jeszcze w żadnej bazie wzorców.

W Zielonej ochrona stacji stoi dziś na dwóch nogach naraz, bo flota rosła etapami i wciąż trwa migracja opisana na stronie Intune obok domeny: audyt GPO i plan migracji. Starsze stacje i serwery mają agenta McAfee/Trellix zarządzanego z konsoli ePO na `app01`, wdrożoną jeszcze przed decyzją o Intune. Nowe stacje i te już przeniesione do Intune dostają Microsoft Defender for Endpoint, onboardowanego razem z resztą polityk bezpieczeństwa w piątej fali migracji z GPO.



Dwa równoległe systemy ochrony stacji w Zielonej: ePO dla starszych maszyn i Microsoft Defender for Endpoint dla stacji w Intune (kliknięcie otwiera pełny rozmiar)

Docelowo obie ścieżki mają się zejść w jedną, ale zespół IT świadomie nie migruje całej floty naraz: agent ochrony stacji to ostatnia linia obrony, więc zamiana produktu na stacji roboczej dzieje się partiami, dokładnie tak jak przy każdej innej migracji opisanej w tej bazie wiedzy.

Mapa tej książki

Strona	Na jakie pytanie odpowiada
Opowieść	Skąd wzięła się ochrona stacji i jak trafiła do Zielonej
Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia	Czym różnią się od siebie te słowa i dlaczego to nie synonimy tego samego produktu
Agent ochrony na serwerach Linux: instalacja i weryfikacja	Jak zainstalować i sprawdzić agenta ochrony na serwerze linuksowym
Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM	Jak objąć ochroną całą flotę stacji roboczych, niezależnie od tego, czym już nimi zarządzamy
ePolicy Orchestrator: konsola zarządzania	Jak zarządzać agentami McAfee/Trellix z jednej konsoli
Utrzymanie i typowe problemy	Jak diagnozować najczęstsze problemy ochrony stacji, niezależnie od producenta

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · Intune obok domeny: audyt GPO i plan migracji

Źródła: Wikipedia, „Brain (computer virus)” · Microsoft Learn, „Virus alert about Blaster worm and its variants” · Kaspersky, „Evolution of security: the story of the ILOVEYOU worm” · Microsoft Security Blog, „WannaCrypt ransomware worm targets out-of-date systems” · Wikipedia, „John McAfee”

Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia

Poziom: podstawy

Dotyczy: dowolny produkt ochrony stacji końcowych (producent, McAfee/Trellix, Microsoft Defender)

Czas: ~20 min

Zanim zajmiemy się konkretnym produktem, ustalamy słownik pojęć wspólny dla wszystkich rozwiązań tej klasy — bo różnice między producentami dotyczą interfejsu i nazewnictwa, nie samych mechanizmów.

Skróty użyte na tej stronie (4)

Skrót	Co znaczy
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
HANA	SAP HANA: baza danych w pamięci firmy SAP, używana do dużych systemów księgowych i magazynowych
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung: niemiecki producent oprogramowania klasy ERP, właściciel silnika HANA i przejętego wcześniej Sybase ASE
XDR	Extended Detection and Response: rozszerzenie EDR na wiele źródeł danych naraz (stacje, sieć, poczta): ma ramkę Pojęcie w tekście, ale brakuje w słowniku

Z życia wzięte

Z ŻYCIA WZIĘTE

O 12:10 Tomek dostaje pytanie od kierownika, czy „ten nowy EDR" zastąpi antywirusa na stacjach roboczych, czy trzeba trzymać oba naraz. Tłumaczy, że EDR to nie inny produkt

obok antywirusa, tylko rozszerzenie tego samego agenta o telemetrię i narzędzia reakcji, więc licencja EDR dokłada się do tej samej instalacji, a nie zastępuje jej osobnym procesem. Po tym wyjaśnieniu kierownik zamawia dodatkową licencję na istniejących agentach zamiast planować migrację na nowy produkt.

Ochrona sygnaturowa kontra behawioralna

Pojęcie: ochrona sygnaturowa. Wykrywanie złośliwego oprogramowania przez porównanie skanowanego pliku z bazą znanych wzorców (sygnatur) — skuteczna wyłącznie przeciwko zagrożeniom już wcześniej zidentyfikowanym i wpisanym do bazy przez producenta. Aktualność tej bazy jest tu warunkiem koniecznym: sygnatura sprzed tygodnia nie rozpozna wariantu złośliwego oprogramowania wypuszczonego wczoraj.

Pojęcie: ochrona behawioralna. Wykrywanie na podstawie zachowania procesu w czasie rzeczywistym — próba masowego szyfrowania plików użytkownika, wstrzyknięcie kodu w inny proces, modyfikacja krytycznych kluczy rejestru — niezależnie od tego, czy konkretny plik binarny figuruje w jakiejkolwiek bazie sygnatur. Ten mechanizm łapie zagrożenia nieznane wcześniej (tzw. zero-day), kosztem wyższego ryzyka fałszywych alarmów na nietypowe, ale legalne zachowanie oprogramowania.

Nowoczesne produkty ochrony stacji łączą oba mechanizmy naraz — sygnatury jako szybki, tani pierwszy filtr, analiza behawioralna jako druga warstwa łapiąca to, czego sygnatury nie znają.

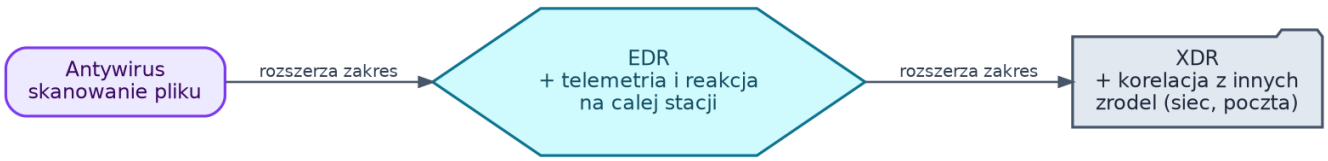
Agent kontra konsola

Pojęcie: agent. Proces instalowany lokalnie na każdej chronionej stacji — wykonuje faktyczne skanowanie, blokowanie i kwarantannę plików, oraz zgłasza swój stan i wykryte zdarzenia do konsoli. Bez połączenia z konsolą agent zwykle nadal chroni stację według ostatniej pobranej polityki, ale przestaje raportować i przestaje otrzymywać aktualizacje polityk oraz definicji.

Pojęcie: konsola zarządzania. Centralny system, przez który administrator zarządza wszystkimi agentami naraz — definiuje polityki, grupuje stacje, rozsyła zadania, zbiera zdarzenia i buduje raporty. Konsola sama w sobie niczego nie skanuje — to agent wykonuje pracę, konsola nią zarządza i ją nadzoruje. W naszym środowisku rolę tę pełnią odpowiednio produkt ochrony stacji Manager, opisany na stronie dokumentacja producenta, oraz ePolicy Orchestrator, opisany na stronie ePolicy Orchestrator: konsola zarządzania.

Antywirus, EDR, XDR — różnica w zasięgu

Trzy nazwy z tytułu tej strony nie są synonimami różnych producentów tego samego produktu — opisują trzy kolejno szersze zakresy działania, z których każdy obejmuje poprzedni i dokłada do niego kolejną warstwę.



Antywirus, EDR i XDR to trzy kolejno szersze zakresy: od pojedynczego pliku, przez całą stację, po korelację wielu źródeł naraz (kliknięcie otwiera pełny rozmiar)

Pojęcie: antywirus (AV). Najwęższy zakres — ochrona pojedynczej stacji przez skanowanie plików (sygnaturowe i behawioralne) oraz blokowanie znanych zagrożeń w czasie dostępu do pliku. Perspektywa antywirusu kończy się na granicy jednej maszyny.

Pojęcie: EDR (Endpoint Detection and Response). Rozszerzenie antywirusu o ciągłe zbieranie telemetrii z całej stacji — uruchamiane procesy, połączenia sieciowe, zmiany w rejestrze czy systemie plików — oraz narzędzia do reagowania na incydent bezpośrednio z konsoli: izolacja stacji od sieci, zdalne zabicie procesu, cofnięcie zmian. EDR odpowiada na pytanie, którego sam antywirus nie zadaje: „co dokładnie działo się na tej maszynie w ciągu ostatnich godzin, zanim doszło do wykrycia".

Pojęcie: XDR (Extended Detection and Response). Rozszerzenie EDR poza granicę pojedynczej stacji — korelacja telemetrii z wielu źródeł naraz (stacje końcowe, ruch sieciowy, poczta, tożsamość) w jednym miejscu, żeby wykryć wzorzec ataku rozłożony na kilka systemów, niewidoczny przy patrzeniu na każdy z nich osobno. XDR jest do zestawu zdarzeń bezpieczeństwa tym, czym centralne logowanie (temat rozdziału Po co centralne logowanie i jak to działa) jest do zwykłych logów operacyjnych — bez zebrania danych z wielu źródeł w jedno miejsce korelacja między nimi w ogóle nie jest możliwa.

Uważaj: produkty konkretnych producentów rzadko mieszczą się czysto w jednej z tych trzech kategorii — funkcje EDR bywają dokupowaną licencją do tego samego agenta antywirusowego, a nie osobnym, niezależnym produktem, co warto sprawdzić przy planowaniu wdrożenia, zamiast zakładać zakres na podstawie samej nazwy marketingowej.

Polityka, grupa, zadanie skanowania

Pojęcie: polityka. Zestaw ustawień definiujących, jak agent ma się zachowywać — co skanować, jak często, co robić z wykrytym zagrożeniem (usunąć, poddać kwarantannie, tylko zalogować), oraz jakie wykluczenia stosować. Polityka nie jest przypisywana do pojedynczej stacji z osobna, tylko do grupy.

Pojęcie: grupa. Logiczny zbiór stacji, do którego przypisujemy wspólną politykę — typowy podział to grupy według roli (serwery, stacje robocze, kontrolery domeny) albo według środowiska (produkcja, testy). Zmiana polityki przypisanej do grupy propaguje się na wszystkie należące do niej stacje bez potrzeby ręcznej zmiany ustawień na każdej z osobna — mechanizm koncepcyjnie identyczny z dziedziczeniem szablonu w Zabbiksie, opisanym na stronie Host, element danych, wyzwalacz, akcja: jak to się składa.

Pojęcie: zadanie skanowania. Zdefiniowany, zaplanowany albo wywołany ręcznie przebieg pełnego lub częściowego skanowania stacji — w odróżnieniu od ochrony w czasie rzeczywistym (skanującej pliki w momencie dostępu), zadanie skanowania przechodzi przez cały wskazany zakres (dysk, katalog) jednorazowo, w zaplanowanym oknie czasowym.

Kwarantanna i wykluczenia

> **Pojęcie: kwarantanna.** Izolowane miejsce, do którego agent przenosi plik uznany za zagrożenie, zamiast usuwać go od razu — plik w kwarantannie jest zaszyfrowany i niewykonywalny, ale odzyskiwalny, jeśli okaże się, że wykrycie było fałszywym alarmem.
>
> Przywracanie pliku z kwarantanny opisujemy na stronie Utrzymanie i typowe problemy.

> **Pojęcie: wykluczenie (exclusion).** Ścieżka, proces albo typ pliku jawnie pominięty przez skaner — ani skanowanie w czasie rzeczywistym, ani zadanie skanowania nie dotyka wykluczonego obiektu. Wykluczenia konfigurujemy z osobna dla odczytu, zapisu, albo obu naraz, oraz z opcją objęcia nimi też podkatalogów.

Wykluczenia jako najczęstsza przyczyna problemów wydajnościowych

Wykluczenia nie są tematem drugorzędnym — to jeden z najważniejszych elementów polityki na serwerach bazodanowych i aplikacyjnych, bo skanowanie w czasie rzeczywistym plików danych silnika bazy danych przy każdym odczycie i zapisie potrafi wielokrotnie spowolnić operacje I/O. Plik danych PostgreSQL albo Oracle otwierany i modyfikowany tysiące razy na sekundę, skanowany przy każdym takim dostępie, generuje obciążenie procesora i opóźnienie zupełnie nieproporcjonalne do realnego ryzyka — pliki danych silnika bazy nie są wektorem infekcji w sposób, w jaki jest nim np. katalog pobranych załączników pocztowych.

Typowe kategorie katalogów wykluczanych na serwerach aplikacyjnych i bazodanowych: katalogi danych silnika bazy (PostgreSQL, Oracle, SAP HANA), katalogi kopii zapasowych, katalogi robocze systemów kolejkowania i indeksowania, oraz katalogi tymczasowe środowisk uruchomieniowych (Java, .NET, Node.js) intensywnie zapisujące i kasujące pliki tymczasowe w trakcie normalnej pracy.

Uważaj: wykluczenie zbyt szerokiego katalogu (np. całego `/home` zamiast konkretnego podkatalogu aplikacji) rozwiązuje problem wydajnościowy kosztem stworzenia miejsca, w którym faktyczne zagrożenie może swobodnie operować bez wykrycia — każde wykluczenie zawężamy maksymalnie do tego, co faktycznie wymaga pominięcia, i dokumentujemy powód jego istnienia.

Częste błędy

Traktowanie ochrony sygnaturowej jako wystarczającej samej w sobie. Definicje aktualizowane raz dziennie nie chronią przed zagrożeniem, które pojawiło się i rozeszło w ciągu tych 24 godzin — stąd znaczenie warstwy behawioralnej jako uzupełnienia, nie dodatku.

Kopiowanie wykluczeń między środowiskami bez weryfikacji. Zestaw wykluczeń przygotowany dla jednego środowiska bazodanowego, przeniesiony bez zmian na serwer z inną rolą, zostawia niepotrzebnie otwarte wykluczenie w miejscu, gdzie faktycznie powinno być skanowane, i jednocześnie może pomijać katalog, który akurat na tym serwerze wymaga wykluczenia.

Modyfikacja ustawień lokalnie na stacji zamiast w polityce. Zmiana wprowadzona ręcznie na agencie, z pominięciem konsoli, zostaje nadpisana przy najbliższej synchronizacji polityki z grupy — to jest ten sam mechanizm i to samo ryzyko, co nadpisanie wartości makra bezpośrednio na hoście w Zabbiksie, tyle że tutaj nadpisanie jest tymczasowe i znika bez ostrzeżenia.

□□ Ćwiczenia

> Zadania sprawdzające.

Ćwiczenie 1 — dobór wykluczenia

Serwer aplikacyjny Jenkinsa zaczął działać zauważalnie wolniej po wdrożeniu agenta ochrony stacji. Wskazujemy, co sprawdzamy najpierw i jakie wykluczenie prawdopodobnie trzeba dodać.

Odpowiedź

Sprawdzamy najpierw obciążenie procesu skanującego w czasie rzeczywistym w monitorze zasobów w chwili budowania zadania Jenkinsa — jeśli rośnie razem z aktywnością Jenkinsa, dodajemy wykluczenie na katalog roboczy agenta Jenkinsa (miejsce, gdzie rozpakowywane są zależności i budowane artefakty), bo to tam powstaje intensywny ruch tworzenia i kasowania plików tymczasowych typowy dla procesu budowania.

Pytania kontrolne

1. Czym różni się zakres EDR od zakresu zwykłego antywirusu?

Odpowiedź

Antywirus ocenia i blokuje pojedyncze pliki w momencie dostępu do nich. EDR dodatkowo zbiera ciągłą telemetrię z całej stacji (procesy, połączenia sieciowe, zmiany systemowe) i daje narzędzia do reakcji na incydent — izolację stacji, zdalne zatrzymanie procesu — a nie tylko do zablokowania jednego złośliwego pliku.

2. Dlaczego wykluczenie katalogu danych bazy danych nie jest tym samym co wyłączenie ochrony na całym serwerze?

Odpowiedź

Wykluczenie dotyczy wyłącznie wskazanej ścieżki (i ewentualnie jej podkatalogów) — reszta systemu plików serwera nadal podlega pełnemu skanowaniu w czasie rzeczywistym. Wyłączenie ochrony na całym serwerze usuwa tę warstwę zabezpieczeń wszędzie, łącznie z katalogami niemającymi nic wspólnego z powodem, dla którego wykluczenie w ogóle rozważano.

Powiązane: dokumentacja producenta · dokumentacja producenta · ePolicy Orchestrator: konsola zarządzania · Utrzymanie i typowe problemy

Źródła: dokumentacja produkt ochrony stacji, rozdział „Understanding Endpoint Protection features" · dokumentacja McAfee/Trellix ePolicy Orchestrator, rozdział „Endpoint Security concepts"

Agent ochrony na serwerach Linux: instalacja i weryfikacja

Poziom: średnio

Dotyczy: agenci EDR na Rocky Linux 9, na przykładzie Microsoft Defender for Endpoint na Linuksie

Czas: ~30 min

Serwer linuksowy dostaje agenta ochrony stacji dokładnie tak samo jak stacja robocza, tylko innym pakietem i innym poleceniem weryfikacji. Instalujemy repozytorium producenta, sam pakiet, uruchamiamy skrypt onboardingu i sprawdzamy stan agenta, zanim uznamy wdrożenie za zakończone.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
eBPF	extended Berkeley Packet Filter: mechanizm jądra Linux pozwalający programowi obserwować zdarzenia systemowe (pliki, procesy, sieć) bez ładowania własnego modułu jądra
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
EICAR	European Institute for Computer Antivirus Research: instytut, od którego nazwy pochodzi nazwa bezpiecznego pliku testowego rozpoznawanego przez każdy silnik antywirusowy jako zagrożenie testowe
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Komendy wykonujemy w CLI bash jako użytkownik z uprawnieniami sudo albo root, na serwerze z rozwiązywaniem nazw DNS i ruchem wychodzącym do internetu.

ZMIENIA SYSTEM

Dodanie repozytorium pakietów Microsoftu na Rocky Linux 9

```
sudo dnf config-manager --add-repo
https://packages.microsoft.com/config/rocky/9/prod.repo
```

Rocky Linux ma własną ścieżkę repozytorium, inną niż ogólna ścieżka `rhel`, mimo że pakiety są identyczne. Kanał `prod` to wydania produkcyjne, w odróżnieniu od kanałów `insiders-fast` i `insiders-slow` przeznaczonych do wcześniejszego testowania nowych wersji.

dnf = Dandified YUM: menedżer pakietów RHEL/Rocky

TYLKO ODCZYT

Zaimportowanie klucza GPG producenta

```
sudo rpm --import https://packages.microsoft.com/keys/microsoft.asc
```

Bez zaimportowanego klucza `dnf` odrzuci instalację pakietu jako niepodpisanego.

GPG = GNU Privacy Guard: program do podpisywania i szyfrowania plików oraz sprawdzania podpisów paczek · **rpm** = RPM Package Manager: format i narzędzie paczek RHEL

ZMIENIA SYSTEM

Instalacja pakietu agenta: dnf install mdatp

```
sudo dnf install mdatp
```

Pakiet instaluje binaria agenta w `/opt/microsoft/mdatp/`, usługę systemd `mdatp` oraz narzędzie wiersza poleceń `mdatp`, ale sam agent zostaje nieaktywny do czasu onboardingu.

dnf = Dandified YUM: menedżer pakietów RHEL/Rocky

TYLKO ODCZYT

Uruchomienie skryptu onboardingu

```
unzip WindowsDefenderATPOnboardingPackage.zip
sudo python3 MicrosoftDefenderATPOnboardingLinuxServer.py
```

Plik `WindowsDefenderATPOnboardingPackage.zip` pobieramy z portalu Microsoft Defender, z sekcji Ustawienia, Punkty końcowe, Onboarding, wybierając system Linux Server. Skrypt zapisuje w konfiguracji agenta identyfikator naszej organizacji, dzięki czemu agent wie, do którego portalu wysyłać dane.

python3 = uruchom interpreter Pythona w wersji 3 albo wskazany skrypt

TYLKO ODCZYT

Sprawdzenie usługi agenta: systemctl status mdatp

```
sudo systemctl status mdatp
```

Przykład:

```
● mdatp.service - Microsoft Defender for Endpoint
   Loaded: loaded (/lib/systemd/system/mdatp.service; enabled)
   Active: active (running) since Mon 2026-09-28 06:14:02 CEST
 Main PID: 21044 (wdavdaemon)
   CGroup: /system.slice/mdatp.service
           └─21044 /opt/microsoft/mdatp/sbin/wdavdaemon
```

systemctl = system control: sterowanie usługami systemd

TYLKO ODCZYT

Sprawdzenie zdrowia agenta: mdatp health

```
sudo mdatp health
```

Przykład (skrócony) z `ora01`:

```
healthy: true
health_issues: []
licensed: true
org_id: 8f1c2e4a-91b3-4d7c-a2e5-3c0b1f9a6d21
real_time_protection_enabled: true
```

```
definitions_status: up_to_date
definitions_updated: 2026-09-28 05:02:11
engine_version: 1.1.24080.2
```

Pole `healthy` na `true` jest pierwszym, najogólniejszym potwierdzeniem, że agent działa i komunikuje się z portalem, a dopiero potem sprawdzamy szczegóły.

mdatp = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

TYLKO ODCZYT

Sprawdzenie pojedynczego pola stanu: mdatp health --field

```
mdatp health --field real_time_protection_enabled
```

Przydatne w skrypcie, który sprawdza flotę serwerów automatem: jedno pole zamiast parsowania całego wyniku.

mdatp = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

TYLKO ODCZYT

Dodanie wykluczenia katalogu: mdatp exclusion folder add

```
sudo mdatp exclusion folder add --path "SciezkaKatalogu"
```

> (gdzie `SciezkaKatalogu` to katalog danych silnika bazy albo katalog kontenerów, bez cudzysłowu, jeśli ścieżka nie zawiera spacji)

Przykład z `docker01`:

```
sudo mdatp exclusion folder add --path /docker/
```

Domyślny zasięg wykluczenia to `epp`, czyli ochrona w czasie rzeczywistym, skanowanie na żądanie i monitorowanie zachowania procesu naraz. Wykluczenie w zasięgu `global` (od wersji agenta 101.24092.0001) dodajemy flagą `--scope global`, gdy ma dotyczyć też innych

modułów.

mdatp = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

TYLKO ODCZYT

Sprawdzenie listy wykluczeń: mdatp exclusion list

```
mdatp exclusion list
```

Sprawdzamy tym poleceniem, czy wykluczenie faktycznie zostało zapisane, zanim uznamy problem wydajnościowy za rozwiązany.

mdatp = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

TYLKO ODCZYT

Wskazanie procesów generujących najwięcej skanowań: mdatp diagnostic real-time-protection-statistics

```
sudo mdatp diagnostic real-time-protection-statistics --sort --top 5
```

Wypisuje procesy, których pliki agent skanował najczęściej w danym oknie czasu, posortowane malejąco. Wynik tego polecenia jest podstawą do decyzji, co dokładnie wykluczyć, zamiast zgadywania.

mdatp = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

TYLKO ODCZYT

Pobranie bezpiecznego pliku testowego EICAR

```
curl -o /tmp/eicar.com.txt https://secure.eicar.org/eicar.com.txt
```

> **Pojęcie: plik EICAR.** Tekstowy plik testowy ustandaryzowany przez European Institute for Computer Antivirus Research, rozpoznawany przez praktycznie każdy silnik antywirusowy jako zagrożenie testowe, mimo że nie zawiera żadnego faktycznego złośliwego kodu. Służy wyłącznie do sprawdzenia, czy ochrona w czasie rzeczywistym w ogóle reaguje, bez ryzyka uruchomienia prawdziwego złośliwego oprogramowania na produkcyjnym serwerze.

EICAR = European Institute for Computer Antivirus Research: instytut, od którego nazwy pochodzi nazwa bezpiecznego pliku testowego rozpoznawanego przez każdy silnik antywirusowy jako zagrożenie testowe · **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

TYLKO ODCZYT

Sprawdzenie wykrytych zagrożeń: mdatp threat list

```
mdatp threat list
```

Po pobraniu pliku EICAR powinniśmy zobaczyć tu jeden wpis z wykryciem, potwierdzający, że agent faktycznie skanuje pliki na dysku w czasie rzeczywistym, a nie tylko melduje się jako zainstalowany.

EICAR = European Institute for Computer Antivirus Research: instytut, od którego nazwy pochodzi nazwa bezpiecznego pliku testowego rozpoznawanego przez każdy silnik antywirusowy jako zagrożenie testowe · **mdatp** = CLI: Microsoft Defender Advanced Threat Protection, narzędzie wiersza poleceń agenta Microsoft Defender for Endpoint na Linuksie: sprawdza stan agenta, zarządza wykluczeniami i uruchamia diagnostykę

Z życia wzięte

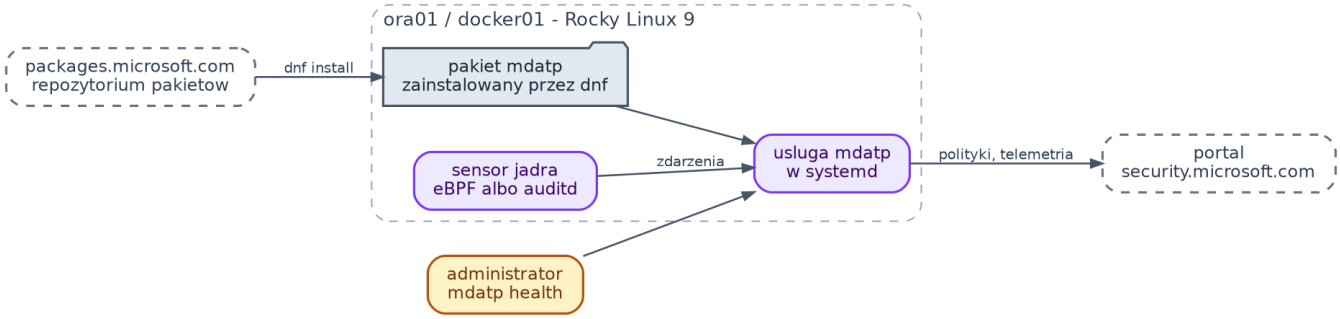
Z ŻYCIA WZIĘTE

Poniedziałek, 5:58 w Swarzędzu. Tomek dzień wcześniej zainstalował Microsoft Defender for Endpoint na `ora01` według checklisty, ale pominął krok z wykluczeniami katalogu danych Oracle. O 6:00 loguje się naraz czterdzieści skanerów magazynowych, WMS zaczyna odpowiadać z kilkusekundowym opóźnieniem na każdy skan kodu kreskowego, a Marek dzwoni z pytaniem, czy coś się zepsuło w nocy. `mdatp diagnostic real-time-protection-statistics --sort --top 5` pokazuje proces silnika Oracle na szczycie listy, a dodanie wykluczenia katalogu danych bazy rozwiązuje problem przed kolejną zmianą.

Jak to działa

Rozwiń: jak to działa pod spodem

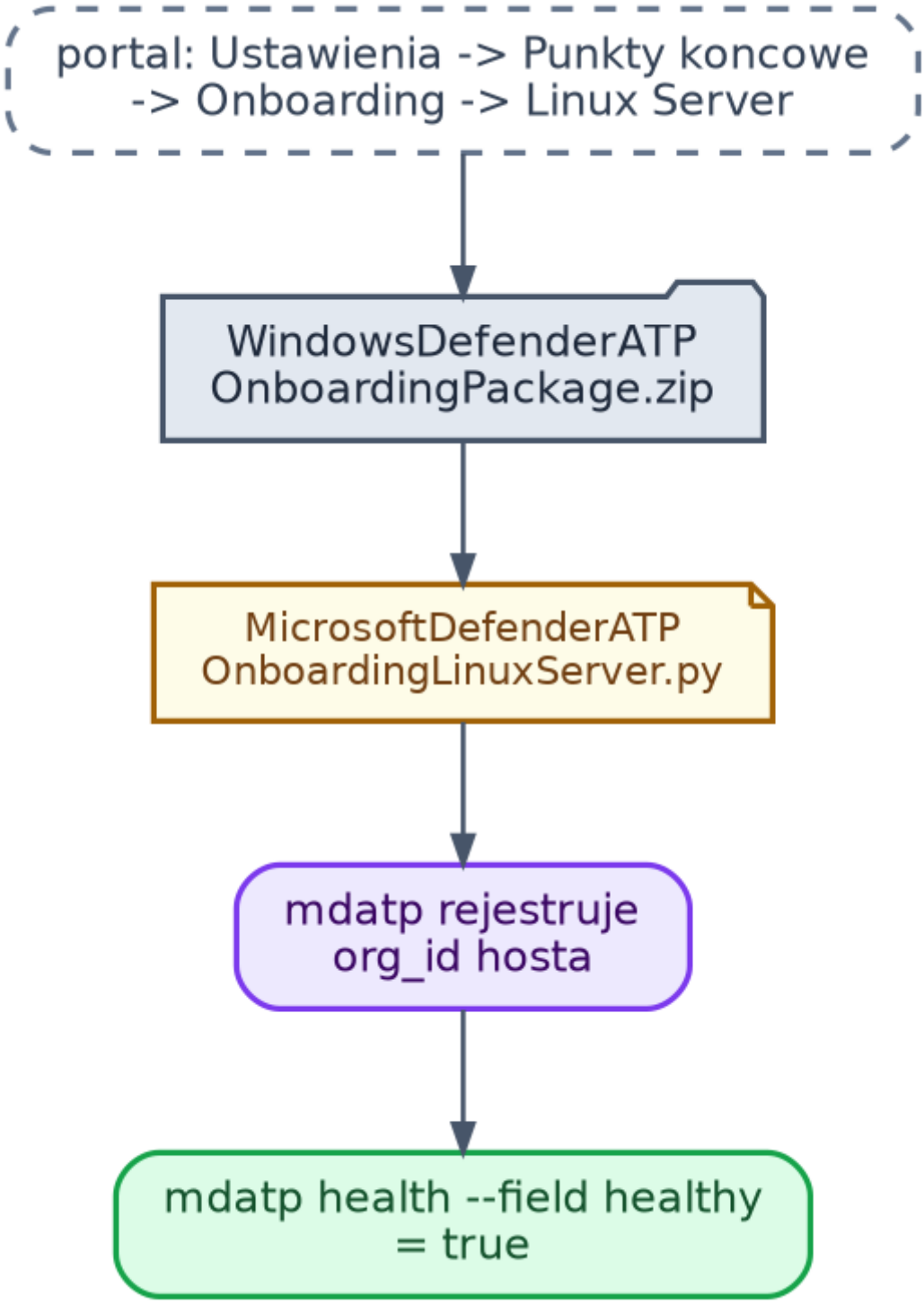
> **Pojęcie: agent EDR na Linuksie.** Tak samo jak na Windowsie, agent to proces działający lokalnie, tu jako usługa systemd, który skanuje pliki, obserwuje zachowanie procesów i wysyła zdarzenia do konsoli w chmurze. Różnica leży w mechanizmie, którym agent w ogóle widzi, co się dzieje w systemie plików i wśród procesów.



Architektura agenta Microsoft Defender for Endpoint na Rocky Linux 9: repozytorium, pakiet, sensor jądra i portal (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: sensor jądra (eBPF).** Mechanizm jądra Linux (extended Berkeley Packet Filter) pozwalający agentowi obserwować operacje na plikach i procesach bez modyfikowania samego jądra ani ładowania własnego modułu. Na starszych jądrach, gdzie eBPF nie jest dostępny albo nie jest wspierany, agent korzysta zamiast tego z podsystemu `auditd`, wolniejszego i bardziej inwazyjnego w konfigurację systemu.

Instalacja przebiega w dwóch niezależnych krokach, które łatwo pomylić: sama instalacja pakietu `mdatp` z repozytorium tylko kładzie binaria na dysku, a dopiero uruchomienie skryptu onboardingu wiąże agenta z konkretną organizacją w portalu.



Przebieg onboardingu agenta na Linuksie: od pobrania pakietu z portalu do potwierdzenia mdatp health (kliknięcie otwiera pełny rozmiar)

Wykluczenia dla katalogów baz danych i katalogu /docker

Zasada, dlaczego w ogóle wykluczamy katalogi danych silnika bazy i katalog `/docker`, jest ogólna dla każdego produktu ochrony stacji i opisana na stronie Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia. Dla Microsoft Defender for Endpoint na Linuksie dochodzi jeden dodatkowy powód: sensor eBPF przechwytuje zdarzenia na poziomie jądra dla każdej operacji na pliku, więc intensywny ruch zapisu i odczytu w katalogach danych PostgreSQL, Oracle czy MariaDB generuje wielokrotnie więcej zdarzeń do przeanalizowania niż zwykły katalog użytkownika.

Katalog `/docker` na `docker01` wykluczamy z podobnego powodu: demon Dockera rozpakowuje i kasuje warstwy obrazów, a kontenery piszą dane aplikacji intensywnie i często tymczasowo. Ryzyko tego konkretnego wykluczenia ograniczamy tym, że obrazy w Zielonej pochodzą z kontrolowanych źródeł (Gitea Actions albo oficjalne rejestry z przypiętą wersją), a nie z przypadkowych, niezweryfikowanych źródeł w internecie.

> ⚠ Wykluczenie katalogu nie jest decyzją jednorazową. Za każdym razem, gdy na serwerze pojawia się nowa rola albo nowa aplikacja, sprawdzamy `mdatp diagnostic real-time-protection-statistics`, zanim uznamy, że wydajność jest w porządku.

Wpływ na wydajność

Ochrona w czasie rzeczywistym przechwytuje każdą operację odczytu i zapisu pliku, zanim ta dojdzie do faktycznego wykonania, więc obciążenie procesora rośnie proporcjonalnie do intensywności operacji dyskowych na serwerze. Na serwerach aplikacyjnych i bazodanowych o dużym ruchu I/O ten narzut bywa zauważalny bez odpowiednich wykluczeń, a na serwerach o niskim ruchu (np. `ipa01` albo `mon01`) praktycznie niezauważalny. Diagnozę zawsze zaczynamy od `mdatp diagnostic real-time-protection-statistics`, nie od zgadywania, który katalog wykluczyć.

Częste błędy

Objaw	Przyczyna	Co robimy

`dnf install mdatp` kończy się błędem podpisu pakietu	brak zaimportowanego klucza GPG Microsoftu	uruchamiamy `rpm --import` na kluczu przed ponowną instalacją
`mdatp health` pokazuje `healthy: false` zaraz po instalacji	skrypt onboardingu nie został jeszcze uruchomiony	uruchamiamy skrypt pobrany z portalu i sprawdzamy `mdatp health --field org_id`
Wysokie obciążenie procesora na serwerze bazodanowym po wdrożeniu agenta	brak wykluczenia katalogu danych silnika bazy	sprawdzamy `mdatp diagnostic real-time-protection-statistics --sort --top 5` i dodajemy wykluczenie wskazanego katalogu
Agent zainstalowany, ale nie widać zdarzeń plikowych	starsze jądro bez wsparcia dla eBPF, przełączenie na `auditd` nie zaszło poprawnie	sprawdzamy wspierane wersje jądra w dokumentacji producenta i status sensora w `mdatp health --details edr`
Wykluczenie dodane komendą znika po jakimś czasie	wykluczenie ustawione lokalnie zostało nadpisane przez politykę zarządzaną centralnie z portalu	trwałe wykluczenie dodajemy w polityce w portalu, komendę lokalną traktujemy jako test przed wprowadzeniem zmiany

□□ Ćwiczenia

1. Dlaczego wykluczamy katalog `/docker` na `docker01`, mimo że to jeden z najważniejszych katalogów w firmie, trzymający Giteę, NetBox i Grayloga naraz?

Odpowiedź

Demon Dockera intensywnie zapisuje i kasuje warstwy obrazów oraz dane aplikacji, co przy pełnym skanowaniu w czasie rzeczywistym generuje nieproporcjonalnie duże obciążenie w stosunku do realnego ryzyka: same pliki danych kontenerów nie są typowym wektorem infekcji, w odróżnieniu od np. katalogu pobranych załączników pocztowych. Ryzyko tego wykluczenia ograniczamy tym, że obrazy pochodzą z kontrolowanych źródeł, a nie z przypadkowych rejestrów w internecie, tak jak opisano na stronie Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia.

1. `mdatp health` pokazuje `healthy: true` na serwerze, ale w portalu od kilku dni nie widać żadnych nowych zdarzeń z tego hosta. Co sprawdzamy?

Odpowiedź

Skoro agent lokalnie zgłasza się jako zdrowy, sprawdzamy łączność sieciową serwera do adresów chmury Microsoft Defender (firewall, DNS), pole `definitions_updated` w `mdatp health` pod kątem tego, czy aktualizacje w ogóle dochodzą, oraz czy identyfikator organizacji `org_id` zgadza się z oczekiwanym: `healthy: true` potwierdza tylko, że sam proces agenta działa

poprawnie lokalnie, nie że dane faktycznie docierają do portalu.

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · ePolicy Orchestrator: konsola zarządzania · Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM · Utrzymanie i typowe problemy

Źródła: Microsoft Learn, „Deploy Microsoft Defender for Endpoint on Linux manually" · Microsoft Learn, „Linux exclusions for Microsoft Defender for Endpoint" · Microsoft Learn, „Troubleshoot performance issues for Microsoft Defender for Endpoint on Linux" · Microsoft Learn, „Investigate agent health issues" · `mdatp health --help`

Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM

Poziom: średnio

Dotyczy: Microsoft Defender Antivirus i Microsoft Defender for Endpoint na Windows 11, wdrożenie przez GPO, Intune albo RMM

Czas: ~35 min

Microsoft Defender Antivirus stoi na każdej stacji Windows od pierwszego uruchomienia, więc wdrożenie ochrony to w praktyce dopisanie do niego warstwy EDR: onboarding do Microsoft Defender for Endpoint. Drogę do tego celu wybieramy zależnie od tego, czym już zarządzamy flotą: domeną przez GPO, chmurą przez Intune, albo osobną platformą RMM.

Skróty użyte na tej stronie (4)

Skrót	Co znaczy
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
EICAR	European Institute for Computer Antivirus Research: instytut, od którego nazwy pochodzi nazwa bezpiecznego pliku testowego rozpoznawanego przez każdy silnik antywirusowy jako zagrożenie testowe
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
RMM	Remote Monitoring and Management: platforma do zdalnego zarządzania i monitorowania stacji roboczych

Fiszka

Komendy PowerShell wykonujemy na stacji Windows z uprawnieniami administratora lokalnego.

TYLKO ODCZYT

Sprawdzenie pełnego stanu Defender Antivirus: Get-MpComputerStatus

```
Get-MpComputerStatus
```

Zwraca pełny stan silnika: czy ochrona w czasie rzeczywistym jest włączona, kiedy ostatnio zaktualizowano sygnatury, kiedy było ostatnie skanowanie.

□□ TYLKO ODCZYT

Sprawdzenie trybu pracy silnika: AMRunningMode

```
Get-MpComputerStatus | Select-Object AMRunningMode
```

Przykład:

```
AMRunningMode
-------------
Normal
```

Wartość `Normal` oznacza, że Defender Antivirus jest głównym silnikiem ochrony na stacji. Wartość `Passive` oznacza tryb pasywny, w którym Defender nie blokuje zagrożeń, bo tę rolę pełni inny zainstalowany produkt, a wartość `EDR Block Mode` oznacza, że Defender Antivirus jest pasywny, ale sam EDR (funkcja Defender for Endpoint) i tak potrafi blokować zagrożenia wykryte przez inny silnik.

□□ **EDR** = Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury

□□ TYLKO ODCZYT

Wymuszenie aktualizacji sygnatur: MpCmdRun.exe -SignatureUpdate

```
& "C:\Program Files\Windows Defender\MpCmdRun.exe" -SignatureUpdate
```

Przydatne, gdy podejrzewamy, że zaplanowana aktualizacja nie zaszła, zamiast czekać na najbliższy cykl.

□□ TYLKO ODCZYT

Uruchomienie szybkiego skanowania: MpCmdRun.exe -Scan

```
& "C:\Program Files\Windows Defender\MpCmdRun.exe" -Scan -ScanType 1
```

> (gdzie `-ScanType 1` to skanowanie szybkie, `-ScanType 2` to skanowanie pełne całego dysku)

ZMIENIA SYSTEM

Dodanie wykluczenia ścieżki: Add-MpPreference

```
Add-MpPreference -ExclusionPath "SciezkaDoFolderu"
```

> (gdzie `SciezkaDoFolderu` to katalog wykluczany ze skanowania w czasie rzeczywistym)

Gdy włączona jest ochrona przed manipulacją (tamper protection) i stacja jest zarządzana przez Intune albo Defender for Business, lokalna komenda nie doda wykluczenia: wykluczenia ustawiamy w polityce antywirusowej. Lokalnie działa to na stacji testowej bez tej ochrony. Szczegóły na stronie Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów.

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

Sprawdzenie listy wykluczeń: Get-MpPreference

```
Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
```

Sprawdzamy tym poleceniem, czy wykluczenie faktycznie zostało zapisane lokalnie, zanim uznamy je za wprowadzone, szczególnie na stacji zarządzanej centralnie, gdzie polityka może je nadpisać.

□□ KLIKAMY W INTERFEJSIE

Ustawienia onboardingu przez Intune: profil wykrywania i reagowania

```
Zabezpieczenia punktu końcowego → Wykrywanie i reagowanie na punkty końcowe → Utwórz zasady
→ platforma: Windows 10, Windows 11 i Windows Server
→ profil: Wykrywanie i reagowanie na punkty końcowe (EDR)
→ przypisanie do grupy urządzeń
```

Ten sam ekran, tylko z profilem Microsoft Defender Antivirus zamiast EDR, ustawia centralnie politykę samego silnika antywirusowego: harmonogram skanowania, ochronę przed manipulacją, wykluczenia.

□□ **EDR** = Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury

□□ KLIKAMY W INTERFEJSIE

Podgląd stanu onboardingu floty w Intune

```
Zabezpieczenia punktu końcowego → Przegląd
→ wizualizacja „Urządzenia z systemem Windows dołączone do Microsoft Defender for Endpoint”
```

Pierwsze miejsce do sprawdzenia, ile stacji z całej floty faktycznie zgłasza się już do Defender for Endpoint, zanim zaczniemy szukać pojedynczych brakujących komputerów.

□□ KLIKAMY W INTERFEJSIE

Uruchomienie skryptu onboardingu z GPO: zadanie natychmiastowe

```
Konfiguracja komputera → Preferencje → Ustawienia Panelu sterowania → Zaplanowane zadania
→ nowe zadanie natychmiastowe
→ program: \\NazwaSerwera\UdzialSieciowy\WindowsDefenderATPOnboardingScript.cmd
→ uruchom jako: NT AUTHORITY\SYSTEM
```

Skrypt `WindowsDefenderATPOnboardingScript.cmd` pochodzi z tego samego miejsca w portalu co skrypt na Linuksa, tylko wybieramy system Windows i metodę Group Policy zamiast Local Script. Plik musi leżeć na udziale sieciowym dostępnym do odczytu przez konta komputerów, bo zadanie uruchamia się jako `SYSTEM`, nie jako zalogowany użytkownik.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

TYLKO ODCZYT

Raport stanu floty przez PowerShell Remoting

```
Invoke-Command -ComputerName (Get-Content NazwaPlikuZListaStacji) -ScriptBlock {
    Get-MpComputerStatus | Select-Object PSComputerName, AMRunningMode,
AntivirusSignatureAge, RealTimeProtectionEnabled
} | Export-Csv RaportOchronyStacji.csv -NoTypeInformation
```

Zebranie stanu z listy stacji naraz, przydatne zwłaszcza tam, gdzie flota jeszcze nie jest w pełni onboardowana do Intune ani do Defender for Endpoint, więc jedyny wgląd w jej stan daje zapytanie bezpośrednio na stacjach.

Z życia wzięte

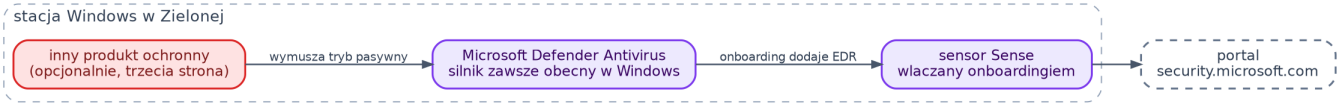
Z ŻYCIA WZIĘTE

Wtorek po Patch Tuesday, 9:15. Pan Zbigniew narzeka, że jego nowy laptop „strasznie zwolnił” od rana. Tomek sprawdza `Get-MpComputerStatus | Select-Object AMRunningMode` i widzi wartość `Normal`, mimo że tydzień wcześniej firma kupiła dla działu handlowego dodatkowy produkt ochronny do testów, wciąż zainstalowany na tym laptopie. Dwa silniki skanujące te same pliki naraz tłumaczą spowolnienie, a właściwym krokiem jest dokończenie testu i odinstalowanie jednego z produktów, nie ręczne wymuszanie trybu pasywnego na chybił trafił.

Jak to działa

Rozwiń: jak to działa pod spodem

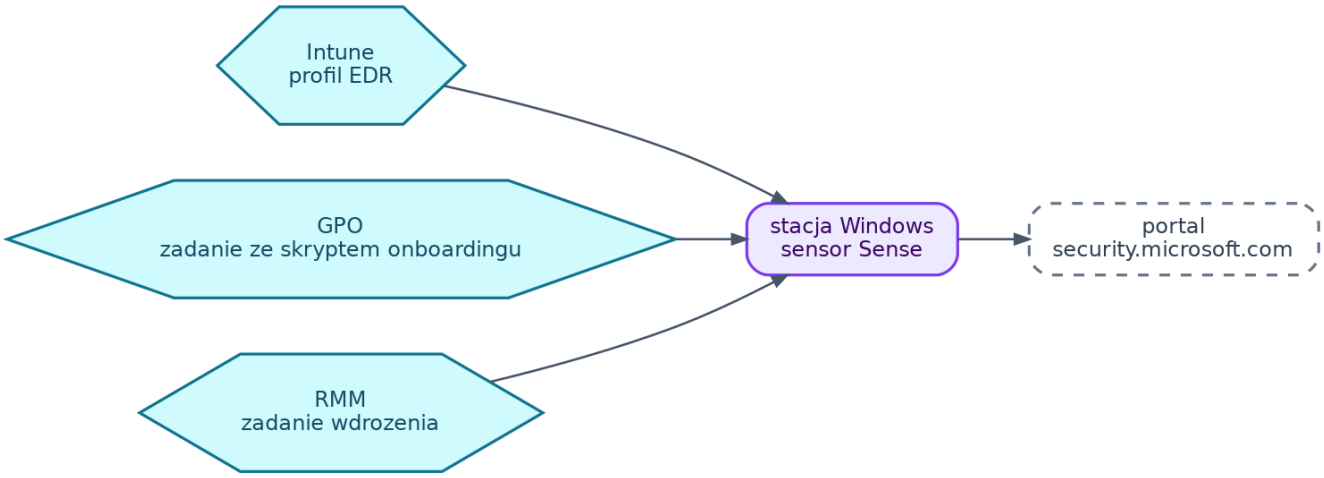
> **Pojęcie: warstwa bazowa.** Microsoft Defender Antivirus instaluje się razem z systemem Windows i działa od pierwszego uruchomienia stacji, niezależnie od tego, czy firma w ogóle korzysta z Defender for Endpoint. Onboarding nie instaluje nowego silnika antywirusowego: włącza na już istniejącym silniku dodatkowy sensor (nazywany Sense), który zbiera telemetrię i daje dostęp do funkcji EDR z portalu.



Warstwy ochrony na stacji Windows w Zielonej: silnik antywirusowy, sensor Sense i ewentualny produkt trzeciej strony (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: tryb pasywny.** Stan, w którym Defender Antivirus nie blokuje zagrożeń samodzielnie, bo tę funkcję przejął inny zainstalowany produkt ochronny, ale nadal skanuje pliki w tle i wysyła telemetrię do Defender for Endpoint, jeśli stacja jest onboardowana. Windows powinien przełączyć się w ten tryb automatycznie po wykryciu innego produktu, ale przy nietypowej kolejności instalacji potrafi tego nie zrobić, dlatego sprawdzenie `AMRunningMode` po każdej zmianie produktu ochronnego jest krokiem obowiązkowym, nie opcjonalnym.

Trzy drogi onboardingu prowadzą do tego samego miejsca: włączonego sensora Sense i widocznej stacji w portalu. Różnią się tylko tym, skąd stacja dostaje instrukcję, żeby się onboardować.



Trzy drogi onboardingu stacji Windows do Microsoft Defender for Endpoint: Intune, GPO i RMM (kliknięcie otwiera pełny rozmiar)

Droga	Kiedy pasuje	Wymaganie
Intune	stacja już zarządzana przez Intune, tak jak opisano na stronie Intune obok domeny: audyt GPO i plan migracji	profil EDR przypisany do grupy urządzeń
GPO	stacja w domenie `ad.zielona.example`, jeszcze nieobjęta Intune	udział sieciowy ze skryptem, dostępny dla kont komputerów
RMM	stacja poza domeną i poza Intune, zarządzana wyłącznie platformą do zdalnego zarządzania	zadanie wdrożenia pakietu onboardingowego wysyłane na stacje z poziomu RMM

W Zielonej stacje nowe i już przeniesione do Intune idą drogą Intune, reszta floty domenowej wciąż czeka na GPO w piątej fali migracji, a droga RMM zostaje w odwodzie na wypadek stacji poza domeną, których dziś w firmie nie ma, ale mogą się pojawić przy kolejnym przejęciu albo oddziale.

Wykluczenia i ich ryzyko

Zasada wykluczeń jest identyczna jak na Linuksie, opisana na stronie Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia: im szersze wykluczenie, tym większe ryzyko, że faktyczne zagrożenie znajdzie w nim bezpieczną kryjówkę. Na stacji Windows dochodzi jedno ryzyko dodatkowe: wykluczenie dodane lokalnie komendą `Add-MpPreference` jest widoczne i modyfikowalne przez każdego z uprawnieniami administratora lokalnego na tej stacji, więc

trwałe wykluczenia ustawiamy w polityce w Intune albo w GPO, a lokalną komendę traktujemy jak na Linuksie: jako test przed wprowadzeniem zmiany do polityki.

Test wykrycia plikiem EICAR

Test bezpiecznym plikiem EICAR, opisany szczegółowo na stronie Agent ochrony na serwerach Linux: instalacja i weryfikacja, działa identycznie na Windows: pobranie pliku testowego powinno wywołać natychmiastowe wykrycie, widoczne zarówno lokalnie, jak i w portalu, jeśli stacja jest już onboardowana.

Częste błędy

Objaw	Przyczyna	Co robimy
`AMRunningMode` pokazuje wartość inną niż `Passive` mimo zainstalowanego innego produktu ochronnego	Windows nie wykrył poprawnie drugiego silnika, zwykle przez nietypową kolejność instalacji	sprawdzamy oba produkty ręcznie, w razie potrzeby wymuszamy tryb pasywny wskazaniami producenta drugiego produktu, zamiast zakładać, że system zrobi to sam
Stacja w domenie nie pojawia się w widoku onboardingu w portalu mimo wdrożonego GPO	konto komputera nie ma dostępu odczytu do udziału sieciowego ze skryptem `WindowsDefenderATPOnboardingScript.cmd`	sprawdzamy uprawnienia NTFS i udziału dla grupy `Domain Computers`, nie tylko dla kont użytkowników
Stacja onboardowana przez Intune, ale zasady EDR do niej nie dochodzą	urządzenie nie należy do grupy, do której przypisano profil w Intune	sprawdzamy przypisanie grupy urządzeń w Intune, sam onboarding nie wciąga urządzenia pod żadną politykę automatycznie
`Add-MpPreference -ExclusionPath` dodane lokalnie znika po restarcie stacji	wykluczenie nadpisane przy najbliższej synchronizacji polityki z Intune albo GPO, bo sama polityka go nie zawiera	trwałe wykluczenie dopisujemy w profilu antywirusowym w Intune albo w GPO, nie tylko lokalnie na stacji
Plik EICAR pobrany, ale `MpCmdRun.exe -Scan` nic nie wykrywa	ochrona w czasie rzeczywistym wyłączona albo katalog docelowy objęty zbyt szerokim wykluczeniem	sprawdzamy `Get-MpComputerStatus` pod kątem `RealTimeProtectionEnabled` i listę wykluczeń poleceniem `Get-MpPreference`

□□ Ćwiczenia

1. Firma kupuje 20 nowych laptopów dla nowych pracowników, od razu rejestrowanych w Entra ID i obejmowanych politykami Intune. Którą drogą onboardingu wybieramy dla tej

grupy i dlaczego nie GPO?

Odpowiedź

Wybieramy drogę Intune, bo te stacje od początku są zarządzane przez Intune, a nie przez domenowe GPO, więc profil EDR w Intune trafia do nich naturalnie razem z resztą polityk. GPO wymagałoby, żeby stacja miała stałą łączność z kontrolerem domeny przy uruchamianiu zaplanowanego zadania, co dla nowych stacji zarządzanych chmurowo jest zbędną zależnością, opisaną też przy okazji migracji GPO na stronie Intune obok domeny: audyt GPO i plan migracji.

1. `Get-MpComputerStatus | Select-Object AMRunningMode` na stacji zwraca `Normal`, ale portal Defender pokazuje tę stację jako nieonboardowaną od tygodnia. Co to oznacza i co sprawdzamy?

Odpowiedź

`AMRunningMode: Normal` mówi wyłącznie o samym silniku antywirusowym Defender Antivirus, nie o sensorze Sense odpowiedzialnym za EDR i łączność z portalem: te dwie rzeczy działają niezależnie od siebie. Sprawdzamy, czy skrypt onboardingu (z Intune, GPO albo RMM) w ogóle dotarł i wykonał się na tej stacji, oraz łączność sieciową stacji do adresów chmury Defender, zamiast zakładać, że skoro antywirus działa, to EDR też musi działać.

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · Agent ochrony na serwerach Linux: instalacja i weryfikacja · Intune obok domeny: audyt GPO i plan migracji · Utrzymanie i typowe problemy

Źródła: Microsoft Learn, „Onboard Windows devices to Microsoft Defender for Endpoint using Microsoft Intune" · Microsoft Learn, „Onboard Windows devices to Microsoft Defender for Endpoint with Group Policy" · Microsoft Learn, „Microsoft Defender Antivirus compatibility with other security products" · Microsoft Learn, „Configure and manage the mpcmdrun.exe command-line tool" · Microsoft Learn, „Monitor Microsoft Defender for Endpoint with Microsoft Intune" · `Get-Help Get-MpComputerStatus`

ePolicy Orchestrator: konsola zarządzania

Poziom: średnio

Dotyczy: McAfee/Trellix ePolicy Orchestrator (ePO), Trellix Agent, Endpoint Security (ENS) na Linux

Czas: ~30 min

ePO zarządza agentami tego samego producenta co producent zarządza swoimi klientami — pojęcia z Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia obowiązują tu jeden do jednego, zmienia się tylko nazewnictwo interfejsu.

Skróty użyte na tej stronie (3)

Skrót	Co znaczy
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
SQL	Structured Query Language: język zapytań do relacyjnych baz danych

Fiszka

Rozróżnienie usług systemowych na Linuksie odzwierciedla podział ról między agentem a modułami ochrony.

TYLKO ODCZYT

Sprawdzenie usługi agenta: systemctl status mcafee.ma.service

```
sudo systemctl status mcafee.ma.service
```

systemctl = system control: sterowanie usługami systemd

□□ TYLKO ODCZYT

Sprawdzenie usługi Threat Prevention: systemctl status mfetpd.service

```
sudo systemctl status mfetpd.service
```

□□ **systemctl** = system control: sterowanie usługami systemd

□□ TYLKO ODCZYT

Sprawdzenie usługi platformy Endpoint Security: systemctl status mfeespd.service

```
sudo systemctl status mfeespd.service
```

□□ **systemctl** = system control: sterowanie usługami systemd

□□ ZMIENIA SYSTEM

Pobranie i uruchomienie skryptu instalacyjnego na Linux

```
cd /tmp
chmod +x ./TrellixSmartInstall.sh
sudo ./TrellixSmartInstall.sh
```

Skrypt instalacyjny generowany jest przez konsolę w sekcji wdrożenia agenta (Agent Deployment) w widoku drzewa systemów — domyślna nazwa pliku to `TrellixSmartInstall.sh`, a sam skrypt sam wykrywa dystrybucję i instaluje właściwy pakiet agenta oraz od razu rejestruje stację w ePO pod adresem konsoli wpisanym w skrypcie przy generowaniu.

□□ **cd** = change directory: przejdź do katalogu · **chmod** = change mode: zmień prawa dostępu

□□ TYLKO ODCZYT

Wymuszenie wysyłki właściwości hosta: cmdagent -c

```
sudo /opt/McAfee/agent/bin/cmdagent -c
```

🔒 TYLKO ODCZYT

Wymuszenie wyegzekwowania polityk lokalnie: cmdagent -p

```
sudo /opt/McAfee/agent/bin/cmdagent -p
```

🔒 TYLKO ODCZYT

Wysłanie zaległych zdarzeń z kolejki lokalnej: cmdagent -e

```
sudo /opt/McAfee/agent/bin/cmdagent -e
```

🔒 TYLKO ODCZYT

Wymuszenie pełnej komunikacji z serwerem: cmdagent -f

```
sudo /opt/McAfee/agent/bin/cmdagent -f
```

Uważaj: `-c`, `-p` i `-e` działają lokalnie na tym, co agent już ma — dopiero `-f` faktycznie pyta serwer o nowości; jeśli po zmianie polityki w konsoli chcemy, żeby konkretny host zastosował ją natychmiast, właściwym poleceniem jest `-f`, nie `-p`.

🔒 TYLKO ODCZYT

Sprawdzenie aktualnej listy wykluczeń na hoście: mfetpcli --getoasconfig

```
sudo /opt/McAfee/ens/tp/bin/mfetpcli --getoasconfig --profile standard --exclusionlist
```

Sprawdzamy, czy host faktycznie pobrał już wykluczenia zdefiniowane w polityce — przydatne, gdy podejrzewamy, że zmiana w konsoli jeszcze nie dotarła do konkretnego hosta.

Przykład typowego zestawu wykluczeń katalogów danych na serwerze aplikacyjno-bazodanowym:

```
/postgres/
/backup/
/db2/
```

```
/hana/
/sapmnt/
/solr/
/sybase/
/tmp/gradle*
/tmp/yarn*
/usr/sap/*
/var/log/
/var/tmp/
```

TYLKO ODCZYT

Dodanie wykluczenia lokalnie (do czasu synchronizacji z polityką): mfetpcli --setoasprofileconfig

```
sudo /opt/McAfee/ens/tp/bin/mfetpcli --setoasprofileconfig --profile standard --
addexclusionrw --excludepaths "SciezkaDoPliku" --excludesubfolder
```

(gdzie `--excludesubfolder` jest opcjonalne i obejmuje wykluczeniem też wszystkie podkatalogi wskazanej ścieżki)

Uważaj: wykluczenie dodane tą komendą bezpośrednio na hoście zostanie nadpisane przy najbliższej synchronizacji polityki z ePO, jeśli sama polityka go nie zawiera — trwałe wykluczenie dopisujemy docelowo w polityce w konsoli, komendę lokalną traktujemy jako test przed wprowadzeniem zmiany do polityki.

Włączamy logowanie aktywności skanera na czas diagnozowania konkretnego problemu (np. wysokiego obciążenia procesora), a wyłączamy je z powrotem po zakończeniu prac — dziennik aktywności rośnie szybko i sam w sobie generuje dodatkowe operacje zapisu na dysku.

TYLKO ODCZYT

Włączenie logowania aktywności skanera: mfetpcli --oasactivitylog enable

```
sudo /opt/McAfee/ens/tp/bin/mfetpcli --oasactivitylog enable
```

□□ TYLKO ODCZYT

Wyłączenie logowania aktywności skanera: mfetpcli --oasactivitylog disable

```
sudo /opt/McAfee/ens/tp/bin/mfetpcli --oasactivitylog disable
```

□□ TYLKO ODCZYT

Podgląd dziennika aktywności skanera: less

```
sudo less -f /var/McAfee/ens/log/tp/mfetpdactivity.log
```

□□ **less** = przeglądarka tekstu z przewijaniem (nazwa to żart: less is more)

□□ TYLKO ODCZYT

Sprawdzenie zaplanowanej samokontroli agenta: crontab -l

```
sudo crontab -l
```

Wpis w crontabie roota uruchamiający okresowe sprawdzenie zdrowia agenta.

Przykład:

```
0,30 * * * * /opt/McAfee/agent/scripts/ma checkhealth >/dev/null 2>/dev/null
```

Skrypt `ma checkhealth` sprawdza cyklicznie, czy usługi agenta faktycznie działają, i restartuje je w razie potrzeby — jego brak w crontabie (np. usunięty przypadkowo przy ręcznej edycji) jest częstym, cichym powodem, dla którego zatrzymana usługa agenta nie wraca sama.

□□ **crontab** = cron table: tabela zadań cyklicznych

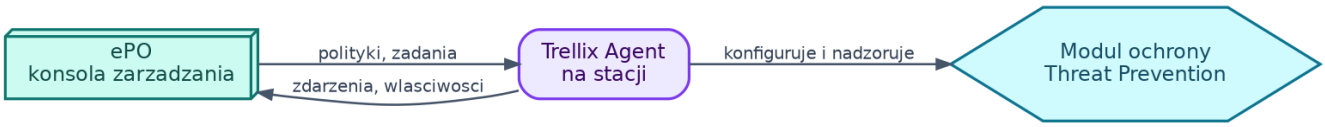
Z życia wzięte

□□ Z ŻYCIA WZIĘTE

O 9:05 nowy serwer aplikacyjny trafia do konsoli, ale po dwóch godzinach wciąż nie pokazuje żadnych zdarzeń, chociaż administrator jest pewien, że skrypt instalacyjny zakończył się bez błędu. Tomek sprawdza trzy usługi agenta komendą `systemctl status` i wszystkie są aktywne, więc podejrzewa, że host po prostu jeszcze nie doczekał zaplanowanego cyklu komunikacji. Wymusza pełną komunikację `cmdagent -f`, a host pojawia się w konsoli w ciągu minuty, wciąż w grupie „Lost and Found", więc od razu przenosi go do właściwej grupy z polityką serwera aplikacyjnego.

Czym jest ePO i jak ma się do agentów

Pojęcie: ePolicy Orchestrator (ePO). Centralna konsola zarządzania produktami ochrony stacji McAfee, obecnie rozwijanymi pod marką Trellix po zmianie brandingu w 2022 roku — w praktyce ten sam produkt, agent i mechanizmy komunikacji, ale w nowszych wersjach z nazwami „Trellix” zamiast „McAfee” w interfejsie i nazwach plików instalacyjnych. Konsola sama niczego nie skanuje — tę pracę wykonuje **Trellix Agent** zainstalowany na stacji, wraz z modułami ochrony (Endpoint Security Threat Prevention, Endpoint Security Firewall) zarządzanymi przez ten agent.



ePO wysyła do agenta polityki i zadania, agent konfiguruje moduł ochrony i odsyła z powrotem zdarzenia oraz właściwości hosta (kliknięcie otwiera pełny rozmiar)

Pojęcie: Trellix Agent (dawniej McAfee Agent). Proces pośredniczący między konsolą a modułami ochrony na stacji — to on pobiera polityki z ePO, przekazuje je modułom ochrony, zbiera ich zdarzenia i właściwości, i odsyła je z powrotem do konsoli. Sam agent nie skanuje plików — to zadanie modułu Endpoint Security Threat Prevention, który agent tylko konfiguruje i nadzoruje na podstawie otrzymanej polityki.

Pojęcie: mcafee.ma.service. Usługa samego agenta — komunikacja z ePO, pobieranie polityk, wysyłka zdarzeń. **Pojęcie: mfetpd.service.** Usługa modułu Threat Prevention — właściwy silnik skanujący. **Pojęcie: mfeespd.service.** Usługa platformy Endpoint Security, na której osadzone są pozostałe moduły. Poprawny stan hosta to wszystkie trzy usługi uruchomione i ustawione w autostarcie — brak którejkolwiek z nich, mimo poprawnej instalacji, jest pierwszym sygnałem do sprawdzenia.

Drzewo systemów

Pojęcie: drzewo systemów (System Tree). Hierarchiczna struktura grup, w której konsola organizuje wszystkie zarządzane stacje — korzeniem jest zawsze „My Organization”, a poniżej administrator buduje własny podział, typowo według roli (np. grupa „Serwery”) albo lokalizacji. Nowo zainstalowany agent, zanim zostanie ręcznie przeniesiony, trafia domyślnie do grupy „Lost and Found” — sprawdzenie tej grupy po wdrożeniu nowego hosta jest pierwszym krokiem potwierdzającym, że agent w ogóle zameldował się w ePO.

Pojęcie: sortowanie drzewa systemów (System Tree sorting). Mechanizm automatycznego przenoszenia hosta do właściwej grupy na podstawie reguł dopasowania (np. adresu IP, nazwy domenowej) — z jawną opcją włączenia albo wyłączenia sortowania dla konkretnych systemów, gdy chcemy, żeby dany host pozostał tam, gdzie umieściliśmy go ręcznie, niezależnie od dalszych zmian reguł.

Tagi

Pojęcie: tag. Etykieta przypisywana do hosta niezależnie od jego miejsca w drzewie systemów, służąca do filtrowania i grupowania zapytań bez przenoszenia hosta fizycznie między grupami — typowe tagi w praktyce to `Server`, `Workstation`, oraz tagi procesowe jak `Excluded from Compliance Check` dla hostów świadomie wyłączonych z raportów zgodności (np. na czas planowanej migracji).

Przypisanie tagu wykonujemy z poziomu widoku systemów w konsoli, wybierając hosty i stosując akcję przypisania tagu z odpowiedniej grupy tagów — jeden host może mieć przypisanych kilka tagów naraz, z różnych grup.

Polityki i przypisania

> **Pojęcie: katalog polityk (Policy Catalog).** Miejsce, w którym definiujemy same polityki — zestawy ustawień dla poszczególnych modułów ochrony (Threat Prevention, Firewall) — niezależnie od tego, do jakiej grupy w drzewie systemów zostaną potem przypisane.

> **Pojęcie: przypisanie polityki (policy assignment).** Powiązanie konkretnej zdefiniowanej polityki z węzłem drzewa systemów, z takim samym mechanizmem dziedziczenia jak w konsoli producent opisanym na stronie dokumentacja producenta — polityka przypisana wyżej w drzewie spływa w dół, chyba że zostanie zablokowana (`Lock policy inheritance`) albo jawnie nadpisana niżej.

Uważaj: zablokowanie dziedziczenia (`Lock policy inheritance`) na węźle pośrednim uniemożliwia jakiekolwiek dalsze nadpisanie polityki poniżej tego punktu — nawet administrator z dostępem do niższej gałęzi drzewa nie zmieni już tej konkretnej polityki bez odblokowania jej wyżej.

Zadania klienckie i serwerowe

> **Pojęcie: zadanie klienckie (client task).** Akcja zaplanowana do wykonania przez agenta na stacji — najczęściej wdrożenie produktu, aktualizacja sygnatur, albo uruchomienie skanowania na żądanie, przypisywana do węzła drzewa systemów tak samo jak polityka.

> **Pojęcie: zadanie serwerowe (server task).** Akcja wykonywana przez sam serwer ePO, nie przez agenty — cykliczne czyszczenie starych zdarzeń z bazy, generowanie i wysyłka raportów, replikacja repozytorium aktualizacji.

Repozytorium aktualizacji i jego replikacja

>

Pojęcie: repozytorium (repository). Miejsce, z którego agenty pobierają aktualizacje sygnatur i samego oprogramowania — domyślnie serwer ePO pobiera je z repozytorium producenta w internecie i udostępnia dalej lokalnie.

Pojęcie: replikacja repozytorium. Rozprowadzenie zawartości repozytorium głównego do repozytoriów rozproszonych bliżej geograficznie chronionych stacji, żeby ograniczyć ruch sieciowy do centralnego serwera przy jednoczesnej aktualizacji dużej liczby agentów naraz.

Wdrożenie agenta i wymuszenie komunikacji

Wymuszenie komunikacji agenta z serwerem

Pojęcie: cmdagent. Narzędzie wiersza poleceń agenta, wywoływane po stronie hosta, gdy nie chcemy czekać na zaplanowany cykl komunikacji z ePO (ASCI — Agent-Server Communication Interval). Poszczególne przełączniki wykonują różne fragmenty tego cyklu z osobna: `-c` zbiera i wysyła właściwości hosta do konsoli, `-p` wymusza natychmiastowe wyegzekwowanie już posiadanych polityk lokalnie, `-e` wysyła zaległe zdarzenia z kolejki lokalnej, `-f` każe agentowi zapytać serwer o nowe polityki i zadania od razu, zamiast czekać na najbliższy zaplanowany cykl.

Wykluczenia On-Access Scan

Wykluczenia modułu Threat Prevention (On-Access Scan) konfigurujemy w polityce w konsoli, ale sprawdzamy i diagnozujemy je bezpośrednio na hoście narzędziem `mfetpcli`.

Zdarzenia i raporty

Zdarzenia wykryte przez moduły ochrony na wszystkich stacjach trafiają do wspólnej bazy konsoli i są dostępne w widoku zdarzeń zagrożeń (Threat Event Log) — filtrowanym po hoście, typie zagrożenia, module i przedziale czasu, analogicznie do przeglądania zdarzeń w konsoli producent.

Diagnostyka agenta, który się nie melduje

Sprawdzenie usług lokalnie na hoście — trzy usługi wymienione wyżej (`mcafee.ma.service`, `mfetpd.service`, `mfeespd.service`) muszą być aktywne; brak którejś to pierwszy trop.

Wymuszenie pełnej komunikacji poleceniem `cmdagent -f` opisanym wyżej, jako ostatni krok przed zgłoszeniem problemu jako poważniejszej awarii agenta.

Kopia zapasowa konsoli i bazy

Kopię zapasową serwera ePO wykonujemy dwuwarstwowo, dokładnie tak samo jak w przypadku SEPM opisanego na stronie dokumentacja producenta: kopia bazy danych konsoli (SQL Server) oraz kopia katalogu instalacyjnego serwera, zawierającego klucze bezpieczeństwa komunikacji agent–serwer. Odtworzenie samej bazy bez kluczy z katalogu instalacyjnego kończy się utratą zaufanej komunikacji z już wdrożonymi agentami.

Częste błędy

Mylenie `cmdagent -p` z pełną synchronizacją polityki. `-p` egzekwuje politykę, którą agent już posiada lokalnie — jeśli zmiana została wprowadzona w konsoli po ostatnim pobraniu, `-p` nic nowego nie sprowadzi; właściwym poleceniem jest `-f`.

Ignorowanie grupy Lost and Found. Świeżo zainstalowane hosty trafiające tam i pozostawione bez ręcznego przeniesienia dziedziczą domyślną politykę korzenia drzewa, zwykle nieprzystosowaną do roli konkretnego serwera.

Trwałe wykluczenia dodawane wyłącznie komendą lokalną. Wykluczenie wprowadzone `mfetpcli` bezpośrednio na hoście, bez odzwierciedlenia w polityce w konsoli, znika przy najbliższej synchronizacji polityki — administrator odkrywa to dopiero wtedy, gdy problem wydajnościowy wraca bez wyraźnej przyczyny.

Ćwiczenia

> Zadania sprawdzające.

Ćwiczenie 1 — kolejność diagnostyki

Host od dwóch dni nie pokazuje nowych zdarzeń w konsoli, mimo że lokalnie usługi `mcafee.ma.service`, `mfetpd.service` i `mfeespd.service` są aktywne. Proponujemy kolejne kroki diagnostyki.

Odpowiedź

Skoro usługi lokalnie działają, sprawdzamy: crontab roota pod kątem obecności wpisu `ma checkhealth`, log agenta pod kątem błędów komunikacji sieciowej z serwerem ePO, a następnie wymuszamy pełną komunikację poleceniem `cmdagent -f` i obserwujemy, czy host pojawia się w konsoli z aktualną datą ostatniej komunikacji. Brak jakiejkolwiek reakcji po `-f` wskazuje na problem sieciowy (firewall, DNS) między hostem a serwerem, a nie na sam agent.

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · dokumentacja producenta · Utrzymanie i typowe problemy

Źródła: dokumentacja Trellix ePolicy Orchestrator, rozdział „Organizing the System Tree" i „Working with policies" · `mfetpcli --help` na kliencie Linux

Ochrona stacji: utrzymanie i typowe problemy

Poziom: średnio **Dotyczy: McAfee/Trellix ePO i ENS** **Czas: ~25 min**

Poniższe problemy powtarzają się niezależnie od producenta — mechanizmy diagnostyki różnią się nazwami komend, ale kolejność sprawdzania jest identyczna.

Skróty użyte na tej stronie (2)

Skrót	Co znaczy
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
SEP	Stowarzyszenie Elektryków Polskich: wydaje świadectwa kwalifikacyjne elektryków

Z życia wzięte

Z ŻYCIA WZIĘTE

O 15:50 przed długim weekendem okazuje się, że pięć serwerów przeniesionych tydzień wcześniej do nowej podsieci nie melduje się do konsoli ochrony stacji. Tomek przechodzi kolejno przez listę: usługi agenta lokalnie działają, samokontrola w crontabie jest na miejscu, ale rozwiązanie nazwy serwera zarządzającego z nowej podsieci zwraca stary, już nieaktualny adres. Poprawia wpis DNS i wymusza `cmdagent -f` na wszystkich pięciu hostach naraz, po czym każdy z nich melduje się w konsoli jeszcze przed końcem dnia.

Agent nie melduje się do konsoli

Zanim zaczniemy podejrzewać awarię samej konsoli, sprawdzamy po kolei — w tej właśnie kolejności, od najbardziej lokalnego do najbardziej odległego elementu:



Diagnostykę prowadzimy od usługi agenta, przez samokontrolę i trasę sieciową, aż po certyfikat, zanim wymusimy pełną komunikację (kliknięcie otwiera pełny rozmiar)

1. **Usługa agenta lokalnie na hoście.** Zatrzymana albo niewystartowana usługa (usługa agenta na Windows, `mcafee.ma.service` na Linuksie z ekosystemu Trellix) jest najczęstszą i najprostszą do wykluczenia przyczyną.
2. **Mechanizm samokontroli agenta.** Zadanie cykliczne restartujące usługę w razie jej zatrzymania (wpis w crontabie `ma checkhealth` po stronie Trellix) — jego brak oznacza, że raz zatrzymana usługa pozostaje zatrzymana bez automatycznej naprawy.
3. **Rozstrzygnięcie nazwy i trasa sieciowa do serwera.** Host musi rozwiązywać nazwę serwera zarządzającego i mieć do niego otwarty ruch na odpowiednim porcie — zmiana adresu serwera po migracji, o której zapomniano poinformować już wdrożone agenty, jest częstą przyczyną cichej utraty łączności.
4. **Certyfikat komunikacyjny.** Odtworzenie serwera zarządzającego z samej kopii bazy danych, bez katalogu certyfikatów (temat poruszony na stronach dokumentacja producenta i ePolicy Orchestrator: konsola zarządzania), unieważnia zaufanie już wdrożonych agentów do „nowego” serwera, mimo identycznej nazwy i adresu.
5. **Wymuszenie komunikacji.** Dopiero po wykluczeniu powyższych czterech punktów wymuszamy pełną komunikację ręcznie (`cmdagent -f` w ekosystemie Trellix, ponowna rejestracja klienta w SEPM) i obserwujemy, czy host pojawia się z aktualną datą ostatniego kontaktu.

Definicje nieaktualne

Rozróżnienie stanu online od stanu aktualnych definicji. Host melduje się do konsoli regularnie, co nie jest tym samym co posiadanie aktualnych sygnatur — te dwie metryki sprawdzamy osobno, bo cykl komunikacji agenta z konsolą i cykl pobierania definicji bywają skonfigurowane z różną częstotliwością.

Najczęstsze przyczyny zatrzymanych definicji mimo działającego agenta:

- lokalny mechanizm aktualizacji (LiveUpdate po stronie SEP, mechanizm aktualizacji sygnatur po stronie ENS) zablokowany przez firewall stacji albo firewall sieciowy między stacją a źródłem aktualizacji,
- wyczerpane miejsce na dysku systemowym uniemożliwiające zapis nowego pakietu definicji,
- ręcznie wyłączony harmonogram aktualizacji na stacji, pozostawiony po testach albo diagnostyce, o czym nikt już nie pamięta.

Wymuszenie ręcznej aktualizacji, opisane w procedurach agenta na stronach ePolicy Orchestrator: konsola zarządzania, jest zawsze pierwszym krokiem diagnostycznym — jeśli wymuszona aktualizacja się powiedzie, problem leży w harmonogramie, a nie w łączności czy uprawnieniach.

Skanowanie zjada procesor na serwerze

Diagnoza przed reakcją. Zanim dodamy wykluczenie, potwierdzamy, że to faktycznie proces skanujący w czasie rzeczywistym generuje obciążenie — monitor zasobów systemu (`top`, Menedżer zadań) pokazujący wysokie zużycie procesora przez proces skanera (`rtvscand`, `mfetpd` i pochodne) w momencie, gdy dzieje się intensywna operacja I/O na konkretnym katalogu, potwierdza korelację.

Ustawienie wykluczeń. Wykluczenia katalogów danych silnika bazy danych i katalogów roboczych aplikacji, opisane szczegółowo na stronach Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia i ePolicy Orchestrator: konsola zarządzania, rozwiązują większość takich przypadków bez kompromisu w zakresie realnego bezpieczeństwa — pliki danych silnika bazy nie są typowym wektorem infekcji.

Ustawienie okien skanowania. Skanowanie planowe (nie w czasie rzeczywistym, tylko cykliczne zadanie pełnego przeglądu dysku) przenosimy poza godziny szczytowego obciążenia serwera — w praktyce najczęściej na noc albo weekend, z jednoczesnym ograniczeniem priorytetu procesu skanującego w systemie operacyjnym, jeśli produkt na to pozwala.

Uważaj: obniżenie priorytetu skanowania w czasie rzeczywistym (nie planowego) jest rozwiązaniem ryzykownym — to właśnie ta warstwa łapie zagrożenie w momencie faktycznego dostępu do pliku; jeśli problem dotyczy konkretnie czasu rzeczywistego, właściwym rozwiązaniem jest wykluczenie konkretnej ścieżki, nie obniżenie priorytetu całego mechanizmu.

Konflikt dwóch produktów ochronnych

> **Pojęcie: konflikt produktów ochronnych.** Sytuacja, w której dwa niezależne silniki ochrony w czasie rzeczywistym (np. wbudowany Windows Defender razem z zainstalowanym produktem trzeciej strony, albo pozostałości po niecałkowicie odinstalowanym poprzednim produkcie) próbują jednocześnie przechwytywać te same operacje na plikach — objawia się to skrajnym spowolnieniem systemu, sporadycznymi błędami dostępu do plików, a czasem wzajemnym oznaczaniem plików drugiego produktu jako zagrożenie.

Diagnozę zaczynamy od potwierdzenia, że faktycznie działają dwa silniki naraz — na Windows sprawdzamy stan Windows Defender, który powinien przejść automatycznie w tryb pasywny po wykryciu innego zainstalowanego produktu ochronnego, ale nie zawsze robi to poprawnie przy nietypowej kolejności instalacji:

```
Get-MpComputerStatus | Select-Object AMRunningMode
```

Przykład:

```
AMRunningMode
-------------
Passive
```

Wartość inna niż `Passive` przy jednocześnie zainstalowanym produkcie trzeciej strony jest sygnałem konfliktu wymagającego dalszej diagnostyki, zanim przejdziemy do odinstalowania jednego z produktów.

Odinstalowanie zablokowanego agenta

Agent zablokowany hasłem odinstalowania ustawionym w polityce, albo z uszkodzoną instalacją uniemożliwiającą standardowe odinstalowanie, wymaga dedykowanego narzędzia producenta — oficjalne narzędzie deinstalacyjne producenta, wskazywane w jego bazie wiedzy dla konkretnej wersji agenta.

Uważaj: próba ręcznego usunięcia plików i usług agenta z pominięciem dedykowanego narzędzia (np. ręczne kasowanie katalogu instalacyjnego i wpisów usług) zostawia zwykle sterowniki jądra systemu (na Windows) w stanie wymagającym trybu awaryjnego do usunięcia — dedykowane narzędzie producenta zna dokładną listę komponentów do usunięcia w bezpiecznej kolejności, ręczne czyszczenie tej wiedzy nie ma.

Kwarantanna i przywrócenie pliku

> **Pojęcie: przywrócenie z kwarantanny.** Operacja odwracająca umieszczenie pliku w kwarantannie — stosowana wyłącznie po potwierdzeniu, że wykrycie było fałszywym alarmem (false positive), nigdy jako pierwsza reakcja na samo zgłoszenie użytkownika „program przestał działać”.

Kolejność postępowania przy zgłoszeniu podejrzenia fałszywego alarmu:

1. sprawdzenie w konsoli, jaki dokładnie plik i jakim mechanizmem (sygnaturowym czy behawioralnym) został wykryty,
2. weryfikacja pliku niezależnym źródłem — suma kontrolna porównana z oficjalnym wydaniem producenta oprogramowania, którego plik dotyczy, albo przesłanie próbki do analizy producenta ochrony stacji,
3. dopiero po potwierdzeniu przywrócenie pliku z kwarantanny z poziomu konsoli albo agenta,
4. dodanie trwałego wykluczenia dla tego konkretnego pliku albo procesu, żeby uniknąć powtórnego, identycznego alarmu przy następnym skanowaniu.

Uważaj: pominięcie kroku 4 oznacza ponowne wykrycie i ponowną kwarantannę tego samego pliku przy najbliższym zaplanowanym skanowaniu — przywrócenie bez dodania wykluczenia jest rozwiązaniem tymczasowym, nie trwałym.

Migracja z jednego produktu ochrony na inny

Kolejność działań przy zmianie produktu ochrony stacji (np. przejście z jednego producenta na drugiego na całym środowisku) różni się od zwykłej aktualizacji tym, że przez pewien okres świadomie akceptujemy chwilowy brak ochrony w czasie rzeczywistym na migrowanej stacji — dwa niezależne silniki ochrony w czasie rzeczywistym działające jednocześnie kończą się dokładnie konfliktem opisanym wyżej.

Kolejność, która minimalizuje to okno bez ochrony: odinstalowanie starego produktu dedykowanym narzędziem producenta, natychmiastowa instalacja nowego produktu z konsoli docelowej, i weryfikacja w nowej konsoli, że stacja się zameldowała i pobrała politykę, zanim przejdziemy do kolejnej stacji z partii migracyjnej. Migrację całego środowiska naraz, wszystkimi stacjami jednocześnie, unikamy — partiami po kilkanaście–kilkadziesiąt stacji łatwiej cofnąć się z błędnie skonfigurowaną polityką na nowym produkcie, zanim dotknie ona całego środowiska.

Częste błędy

Reakcja na pojedyncze zgłoszenie bez sprawdzenia skali. Problem wydajnościowy albo fałszywy alarm zgłoszony przez jednego użytkownika bywa objawem szerszego problemu (błędna aktualizacja definicji, źle zaprojektowana reguła behawioralna) dotykającego całą grupę stacji — sprawdzenie liczby podobnych zdarzeń w konsoli, zanim zareagujemy punktowo, oszczędza powtarzania tej samej naprawy wielokrotnie.

Trwałe wyłączenie ochrony jako rozwiązanie tymczasowego problemu. Wyłączenie ochrony w czasie rzeczywistym na czas diagnozowania innego problemu i pozostawienie jej wyłączonej po zakończeniu prac jest jednym z najczęstszych, a jednocześnie najbardziej ryzykownych przeoczeń — dyscyplina wymaga zapisania w zgłoszeniu momentu wyłączenia i jawnego zadania przywrócenia ochrony po zakończeniu prac.

Odinstalowanie bez dedykowanego narzędzia producenta. Ręczne usuwanie plików i usług zamiast oficjalnego narzędzia deinstalacyjnego kończy się zwykle koniecznością trybu awaryjnego do dokończenia usuwania sterowników jądra.

□□ Ćwiczenia

> Zadania sprawdzające.

Ćwiczenie 1 — diagnoza objawu

Dziesięć stacji roboczych w jednym dziale zgłasza w tym samym dniu wykrycie tego samego pliku aplikacji księgowej jako zagrożenie. Wskazujemy najbardziej prawdopodobną przyczynę i pierwszy krok reakcji.

Odpowiedź

Skala i jednoczesność zgłoszeń wskazują na fałszywy alarm wywołany świeżo pobraną aktualizacją definicji albo regułą behawioralną, a nie na faktyczne zagrożenie w legalnej, wcześniej działającej bez zastrzeżeń aplikacji. Pierwszym krokiem jest sprawdzenie w konsoli, czy identyczne wykrycie dotyczy tego samego pliku i tej samej wersji definicji na wszystkich zgłaszających stacjach, a nie osobne rozpatrywanie każdego zgłoszenia z osobna.

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · ePolicy Orchestrator: konsola zarządzania

Źródła: dokumentacja Trellix ePolicy Orchestrator, rozdział „Troubleshooting agent communication" · Microsoft Docs, „Microsoft Defender Antivirus compatibility"