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"

Revision #37
Created 2026-09-25 07:40:42 UTC by Tomasz Konieczny
Updated 2026-10-26 14:14:20 UTC by Tomasz Konieczny