Poznajemy Defender for Business

Opowieść, licencje i porównanie z odpowiednikami.

- Defender for Business: EDR dla firmy, która nie ma zespołu bezpieczeństwa
- Licencje i porównanie: Defender for Business, Endpoint P1 i P2 oraz odpowiedniki

Defender for Business: EDR dla firmy, która nie ma zespołu bezpieczeństwa

Poziom: podstawy **Dotyczy: Microsoft Defender for Business (stan na październik 2026)**

Czas: ~15 min

Ta strona otwiera książkę o Microsoft Defender for Business: skąd wzięła się ochrona, która w 2022 roku trafiła do firm do 300 użytkowników, czym różni się od zwykłego antywirusa i dlaczego Zielona wdraża ją razem z Intune. Pojęcia EDR i XDR mają własną stronę: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia.

Skróty użyte na tej stronie (4)

Skrót	Co znaczy
ATP	Advanced Threat Protection: dawna nazwa usługi Microsoftu do wykrywania zaawansowanych ataków, dziś Microsoft Defender for Endpoint
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
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

W 2004 roku Microsoft kupił firmę GIANT Company Software i jej program GIANT AntiSpyware. Dwa lata później, w 2006 roku, ten program wyszedł jako Windows Defender: darmowe narzędzie przeciw oprogramowaniu szpiegującemu dla Windows XP i Windows Server 2003. Z Windowsem Vista zadomowił się w systemie, a w Windows 8 w 2012 roku stał się pełnym antywirusem wbudowanym w system, bez żadnej instalacji.

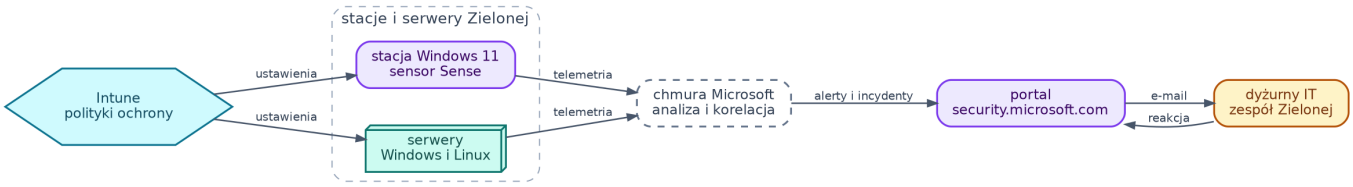
Antywirus pilnuje pojedynczego pliku, a po głośnych atakach ransomware potrzebny był ktoś, kto pamięta, co działo się na komputerze przed wykryciem. Pierwszego marca 2016 roku Microsoft ogłosił więc Windows Defender Advanced Threat Protection: czujniki wbudowane w Windows 10, które wysyłają obserwacje do chmury, gdzie analiza trwa bez obciążania stacji. To był początek EDR w wydaniu Microsoftu.

Potem zaczęła się seria zmian nazw. Pod koniec lutego 2019 roku produkt dostał nazwę Microsoft Defender ATP, bo obejmował już także Maca. Dwudziestego drugiego września 2020 roku został przemianowany na Microsoft Defender for Endpoint, razem z mobilnymi wersjami dla iOS i Androida. W listopadzie 2021 roku pojawiły się dwa plany: Plan 1 (ochrona i redukcja powierzchni ataku) i Plan 2 (pełny EDR i polowanie na zagrożenia).

Ciekawostka: Defender for Endpoint powstał dla dużych firm z własnym zespołem bezpieczeństwa, więc małe firmy dostawały albo za mało (Plan 1), albo za dużo i za drogo (Plan 2). Odpowiedzią był Defender for Business, zapowiedziany na Ignite w listopadzie 2021 roku. W marcu 2022 roku trafił do Microsoft 365 Business Premium, a w maju 2022 roku zaczął być sprzedawany osobno. Jest przeznaczony dla firm do 300 użytkowników.

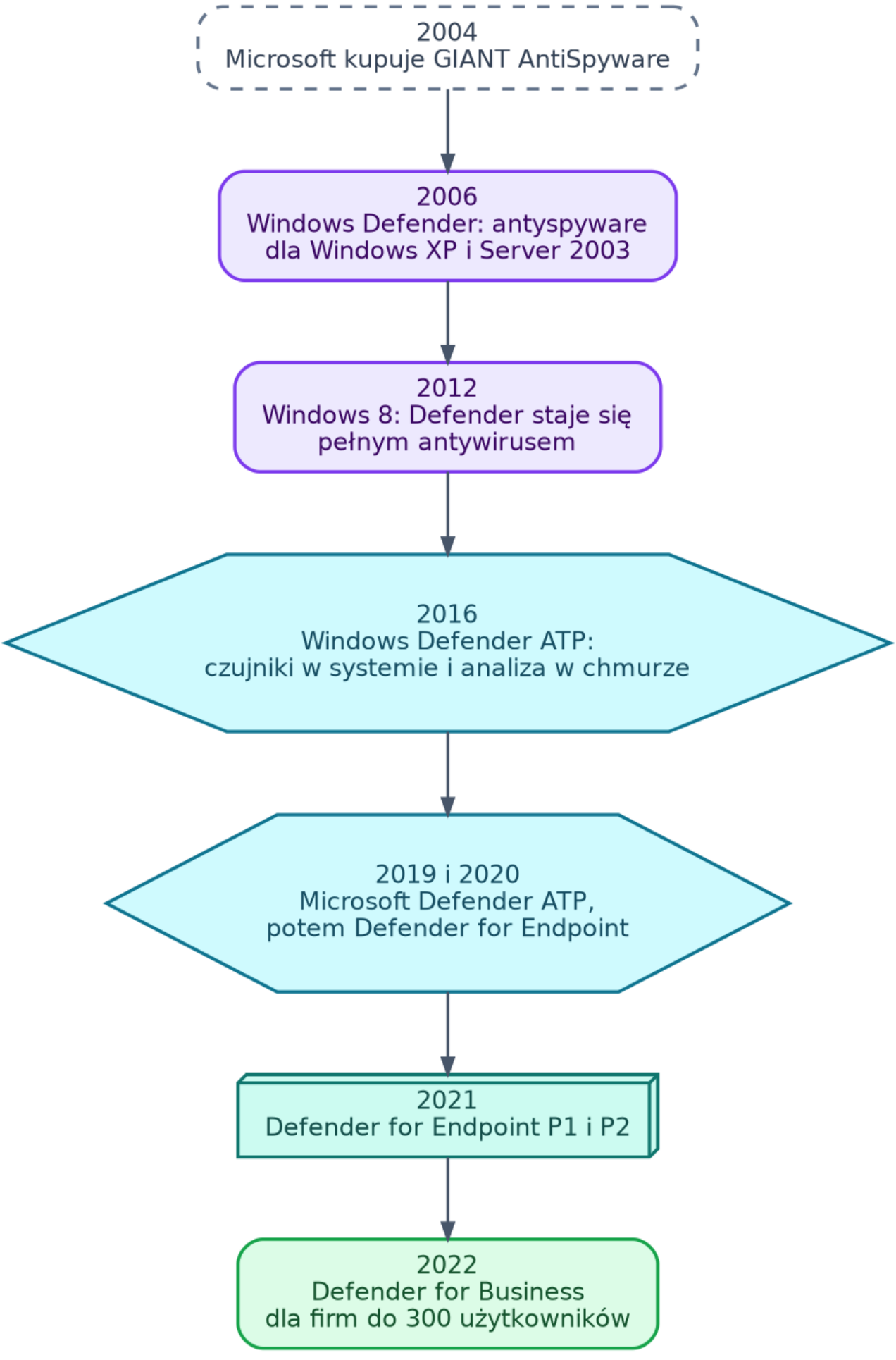
Jak to działa w jednym obrazku

Defender for Business to ten sam silnik co w Defender for Endpoint, z uproszczonym kreatorem, gotowymi politykami i prostszym portalem. Na stacji i na serwerze pracuje czujnik o nazwie Sense, który wysyła obserwacje do chmury Microsoftu. Alerty i incydenty trafiają do portalu `security.microsoft.com`, a dyżurny dostaje e-mail. Intune równolegle rozdaje stacjom ustawienia.



Stacje i serwery Zielonej wysyłają telemetrię do chmury Microsoft, alerty trafiają do portalu i do dyżurnego IT, a Intune rozdaje polityki (kliknięcie otwiera pełny rozmiar)

Rodowód nazw dobrze widać na osi czasu. Nazwa się zmieniała kilkakrotnie, ale idea jest ciągła: antywirus wbudowany w system, na nim czujnik EDR, a nad nimi chmura, która potrafi połączyć wiele drobnych sygnałów w jedną opowieść o ataku.


2004
Microsoft kupuje GIANT AntiSpyware
2006
Windows Defender: antyspyware
dla Windows XP i Server 2003
2012
Windows 8: Defender staje się
pełnym antywirusem
2016
Windows Defender ATP:
czujniki w systemie i analiza w chmurze
2019 i 2020
Microsoft Defender ATP,
potem Defender for Endpoint
2021
Defender for Endpoint P1 i P2
2022
Defender for Business
dla firm do 300 użytkowników

Od przejęcia GIANT AntiSpyware w 2004 roku do Defender for Business w 2022 roku (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Poniedziałek, 9:00. Pan Zbigniew kładzie na biurku Tomka wydruk artykułu o tym, że „każda firma powinna mieć EDR", i pyta: kto w Zielonej będzie patrzył w alerty, skoro IT to dwie osoby, a w nocy nikt nie siedzi w serwerowni? Tomek odpowiada, że narzędzie same naprawia większość spraw, a resztę zgłasza e-mailem do dyżurnego. Pan Zbigniew dopytuje jeszcze, czy to kolejny wydatek. Okazuje się, że Defender for Business jest już w licencji Microsoft 365 Business Premium, którą firma ma dla 180 osób.

Trzy powody składają się na wybór. Zielona ma 180 użytkowników, więc mieści się w limicie 300. Licencja Microsoft 365 Business Premium zawiera Defender for Business, więc nie dokupujemy osobnego produktu. A Intune, który i tak wdrażamy, rozdaje ustawienia ochrony tym samym kanałem co resztę polityk.

Są też ograniczenia, o których mówimy od początku. Defender for Business nie ma polowania na zagrożenia (advanced hunting) ani zdalnej powłoki (live response), a od września 2026 roku automatyczne dochodzenie działa wewnątrz antywirusa i nie da się go uruchomić ręcznie. Dla Zielonej to wystarczy: dyżurny działa według prostej procedury, a nie jak analityk w centrum operacyjnym.

Starsze stacje nadal mają agenta McAfee/Trellix zarządzanego z ePO, o czym mówi strona Ochrona stacji: od wirusa Brain do EDR. Defender for Business przejmuje je stopniowo, a okres współistnienia opisujemy w książce osobno.

Mapa tej książki

Strona	Na jakie pytanie odpowiada
Opowieść (ta strona)	Skąd wziął się Defender for Business i dlaczego Zielona go wybrała
Licencje i porównanie: Defender for Business, Endpoint P1 i P2 oraz odpowiedniki	Co dostajemy w której licencji, jak liczą się serwery i czym są konkurenci
Onboarding urządzeń: Intune, skrypt lokalny, GPO, serwery i Linux	Jak dołączamy stacje i serwery, sprawdzamy to i wychodzimy z innego antywirusa

Strona	Na jakie pytanie odpowiada
Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów	Jak ustawiamy ochronę, żeby nie zatrzymać Optimy
Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie	Co robi dyżurny, gdy przychodzi alert
Zarządzanie podatnościami i raporty: co łatać najpierw	Co łatamy najpierw i co mówimy panu Zbigniewowi co miesiąc

Plan wdrożenia Intune opisuje strona Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy, a rejestrację urządzeń strona Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot. Książka o Intune zaczyna się od Intune: zarządzanie komputerami, które nie wracają do biura. Tu zostają tylko miejsca, w których oba produkty się stykają.

Powiązane: Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia · Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM · Intune obok domeny: audyt GPO i plan migracji

Źródła: Microsoft Learn, „What is Microsoft Defender for Business?" i „What's new in Microsoft Defender for Business?" (learn.microsoft.com/defender-business) · Microsoft Windows Experience Blog, „Announcing Windows Defender Advanced Threat Protection" (1 marca 2016) · Microsoft Security Blog, „Announcing Microsoft Defender ATP for Mac and new Threat and Vulnerability Management capabilities" (28 lutego 2019) · Windows Central, „Microsoft plays the name game with Microsoft Defender services" (22 września 2020) · Redmond Magazine, „Microsoft Defender for Endpoint Plan 1 Commercially Released" (16 listopada 2021) i „Microsoft Defender for Business Ignite" (3 listopada 2021) · TechRepublic, „Windows Defender: Past, present, and future"

Licencje i porównanie: Defender for Business, Endpoint P1 i P2 oraz odpowiedniki

Poziom: podstawy

Dotyczy: Microsoft Defender for Business, Defender for Endpoint Plan 1 i Plan 2, Defender for Business servers, Defender for Servers (stan na październik 2026)

Czas: ~25 min

Pod nazwą Defender kryje się kilka licencji, które różnią się tym, czy dostajemy tylko ochronę, czy także EDR, i czy chronią stacje, czy też serwery. Ta strona pokazuje, co jest w Defender for Business, czego w nim brakuje w porównaniu z Planem 1 i Planem 2, jak liczymy serwery i jak wybieramy między Microsoftem a innymi producentami. Ceny pomijamy, bo zmieniają się częściej niż ta baza wiedzy.

Skróty użyte na tej stronie (5)

Skrót	Co znaczy
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
FAQ	Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami
MDR	Managed Detection and Response: usługa, w której zewnętrzny zespół specjalistów przez całą dobę pilnuje alertów w imieniu firmy i reaguje na ataki
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SUSE	nazwa niemieckiej firmy i jej dystrybucji Linuksa, od niemieckiego skrótu Software und System Entwicklung

Fiszka

Nazwy menu w portalach Microsoftu bywają zmieniane, a opisy poniżej odpowiadają stanowi z października 2026. Gdy ścieżka się nie zgadza, szukamy pozycji o tej samej nazwie w pobliżu albo korzystamy z wyszukiwarki w portalu.

KLIKAMY W INTERFEJSIE

Sprawdzenie licencji Defender for Business w portalu

```
security.microsoft.com → Settings → Endpoints → Licenses
```

Raport pokazuje kupione i użyte licencje. Dokumentacja zaznacza, że jest szacowany na podstawie logowań i odświeża się nawet do 24 godzin.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Settings → Endpoints → Licenses w portalu Defender, widoczny wiersz Microsoft Defender for Business z liczbą kupionych i użytych licencji oraz osobny wiersz dla serwerów, jeżeli licencja Defender for Business servers jest kupiona.

KLIKAMY W INTERFEJSIE

Przypisanie licencji użytkownikowi

```
admin.microsoft.com → Users → Active users → wybieramy konto → Licenses and apps
→ zaznaczamy Microsoft 365 Business Premium (albo Microsoft Defender for Business) →
Save changes
```

Licencja jest licencją użytkownika, a nie urządzenia. Na jednej licencji użytkownika zabezpieczamy do pięciu urządzeń klienckich.

KLIKAMY W INTERFEJSIE

Zakup licencji Defender for Business servers

```
admin.microsoft.com → Billing → Purchase services → Microsoft Defender for Business
servers
```

Jedna licencja przypada na jedną instancję serwera, nie na użytkownika. Warunek wstępny: w subskrypcji jest co najmniej jedna płatna licencja Defender for Business albo Microsoft 365 Business Premium.

KLIKAMY W INTERFEJSIE

Sprawdzenie ustawień zaawansowanych wariantu Business

```
security.microsoft.com → Settings → Endpoints → General → Advanced features
```

Dokumentacja Business wymienia na tej liście dwa przełączniki, Live response for servers i Live response unsigned script execution, jako niedostępne w Defender for Business. Gdy w naszym portalu je widzimy i działają, mamy już doświadczenie Plan 2, a przełączenie na nie wymaga licencji Plan 2 dla wszystkich użytkowników i zgłoszenia do wsparcia Microsoftu.

Z życia wzięte

Z ŻYCIA WZIĘTE

Piątek, 15:50. Pan Zbigniew przekazuje Tomkowi ofertę innego producenta antywirusa z dopiskiem „tańszy, a ma dwadzieścia funkcji więcej" i pyta, czy nie płacimy dwa razy za to samo. Tomek otwiera raport licencji i pokazuje, że Defender for Business wchodzi w skład Microsoft 365 Business Premium, więc osobnej opłaty za niego nie ma. Potem zestawia obie oferty w tabeli i okazuje się, że dwadzieścia funkcji więcej to głównie pakiet usług 24 godziny na dobę, którego Zielona i tak nie planuje kupować.

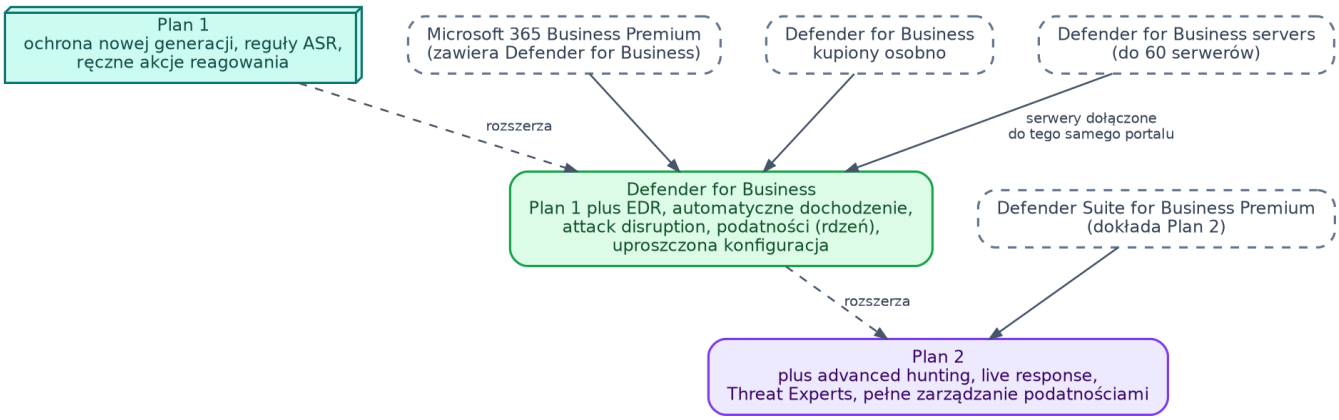
Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: Defender for Business. Rozwiązanie do ochrony stacji i serwerów dla firm do 300 użytkowników, oparte na silniku Microsoft Defender for Endpoint, z kreatorem konfiguracji i domyślnymi politykami. Dostępne osobno albo jako część Microsoft 365 Business Premium.

> **Pojęcie: Plan 1 i Plan 2.** Dwie licencje Defender for Endpoint dla dużych organizacji, w sprzedaży od listopada 2021 roku. Plan 1 to ochrona nowej generacji, redukcja powierzchni ataku i ręczne akcje reagowania. Plan 2 dokłada EDR, automatyczne dochodzenie, polowanie na zagrożenia i usługę Threat Experts.

Defender for Business leży pomiędzy nimi: zawiera Plan 1 i wybrane elementy Planu 2, zoptymalizowane pod małe firmy.



Defender for Business rozszerza Plan 1 i jest rozszerzany przez Plan 2, a kupuje się go w Business Premium, osobno albo z dodatkiem dla serwerów (kliknięcie otwiera pełny rozmiar)

Co jest w Business, a czego nie

Możliwość	Defender for Business	Plan 1	Plan 2
Ochrona nowej generacji (antywirus)	tak	tak	tak
Redukcja powierzchni ataku (reguły ASR)	tak	tak	tak
Ręczne akcje: skan, izolacja, wskaźniki blokowania	tak	tak	tak
EDR (czujnik i telemetria)	tak, w wersji dla małych firm	nie	tak
Automatyczne dochodzenie i naprawa	tak	nie	tak
Automatic attack disruption	tak	nie	tak

Możliwość	Defender for Business	Plan 1	Plan 2
Zarządzanie podatnościami	podstawowe	nie	podstawowe, z dodatkiem rozszerzone
Analiza zagrożeń (threat analytics)	tak, w wersji dla małych firm	nie	tak
Advanced hunting (polowanie na zagrożenia)	nie	nie	tak
Live response (zdalna powłoka na urządzeniu)	nie	nie	tak
Usługa Threat Experts	nie	nie	tak
Kreator i uproszczona konfiguracja w portalu	tak	nie	nie
Limit użytkowników	do 300	brak limitu	brak limitu
Interfejsy programistyczne (API)	tak	tak	tak

Tabela wynika z dokumentacji Microsoftu: strony „What is Microsoft Defender for Business?", „Microsoft Defender for Business FAQ" i „Take response actions on a device". Dwa miejsca wymagają dopowiedzenia.

Po pierwsze, ręczne akcje. Strona o ustawieniach zaawansowanych Business wymienia cztery: skan, izolacja, zatrzymanie i kwarantanna pliku oraz wskaźniki. Strona o akcjach na urządzeniu mówi, że Business nie ma akcji zatrzymania i kwarantanny pliku. Dlatego w tabeli stoją trzy akcje, a czwartą sprawdzamy w swoim portalu na stronie urządzenia.

Po drugie, automatyczne dochodzenie. Od 1 września 2026 roku zostało włączone do antywirusa i nie ma już ręcznego przycisku „Initiate Automated Investigation". Naprawa nadal działa i nadal widać ją w Action center.

Licencje a mieszanie planów

Defender for Business nie obsługuje mieszanych subskrypcji. Gdy w jednym tenancie są licencje Business i Plan 2, domyślnie obowiązuje doświadczenie Business. Przejście na Plan 2 wymaga licencji Plan 2 dla wszystkich użytkowników i zgłoszenia do wsparcia Microsoftu. Po przekroczeniu 300 użytkowników Business przestaje być dostępny i trzeba wybrać plany dla dużych organizacji.

W Microsoft 365 Business Premium istnieje też dodatek Defender Suite for Business Premium, w sprzedaży od września 2025 roku przez partnerów. Dokłada Defender for Endpoint Plan 2, Defender for Office 365 Plan 2, Defender for Identity, Defender for Cloud Apps i Entra ID P2.

Warunki sprzedaży zmieniają się, więc przed zakupem sprawdzamy je u partnera.

Serwery

Defender for Business obejmuje serwery tylko z osobną licencją.

Licencja	Dla kogo	Gdzie zarządzamy	Zasady
Defender for Business servers	firmy do 300 użytkowników, serwery Windows i Linux	portal Defender, `security.microsoft.com`	jedna licencja na instancję serwera, do 60 licencji w subskrypcji
Defender for Servers Plan 1 i Plan 2	większe środowiska, serwery także w chmurze	portal Azure, przez Defender for Cloud	Plan 2 dokłada polowanie na zagrożenia (retencja sześć miesięcy) i Threat Experts
Defender for Endpoint for servers	pojedyncze serwery w środowisku Defender for Endpoint	portal Defender	osobna licencja serwerowa

Wybór ma jeszcze jedną konsekwencję. Gdy do tenanta Business dołożymy Defender for Cloud, uproszczone doświadczenie Business się nie zmienia.

W Zielonej stoi 26 serwerów: 8 z Windows (`dc01`, `dc02`, `fs01`, `rds01`, `wsus01`, `hv01`, `hv02`, `sql01`) i 18 z Linuksem. To mieści się w limicie 60, więc wystarcza Defender for Business servers. Wymagania systemowe sprawdzamy osobno: Windows Server 2012 R2 i 2016 wymagają zunifikowanego agenta, a Linux musi być na liście obsługiwanych dystrybucji (Rocky Linux od 8.7 i 9.2, RHEL do 10, SUSE Linux Enterprise 15). Szczegóły są na stronie Onboarding urządzeń: Intune, skrypt lokalny, GPO, serwery i Linux.

Odpowiedniki innych producentów

Poniższa tabela porównuje podejście producentów, a nie ich jakość. Opiera się na stronach producentów z października 2026. Nazwy pakietów zmieniają się często: strony ESET z różnych okresów pokazują na przykład układy Entry, Advanced, Complete i Elite oraz Core, Premium i Ultimate. Każdą pozycję sprawdzamy u producenta w dniu zakupu.

Produkt	Model chmury	EDR	Linux i serwery	Zarządzanie	Mocne strony	Słabe strony

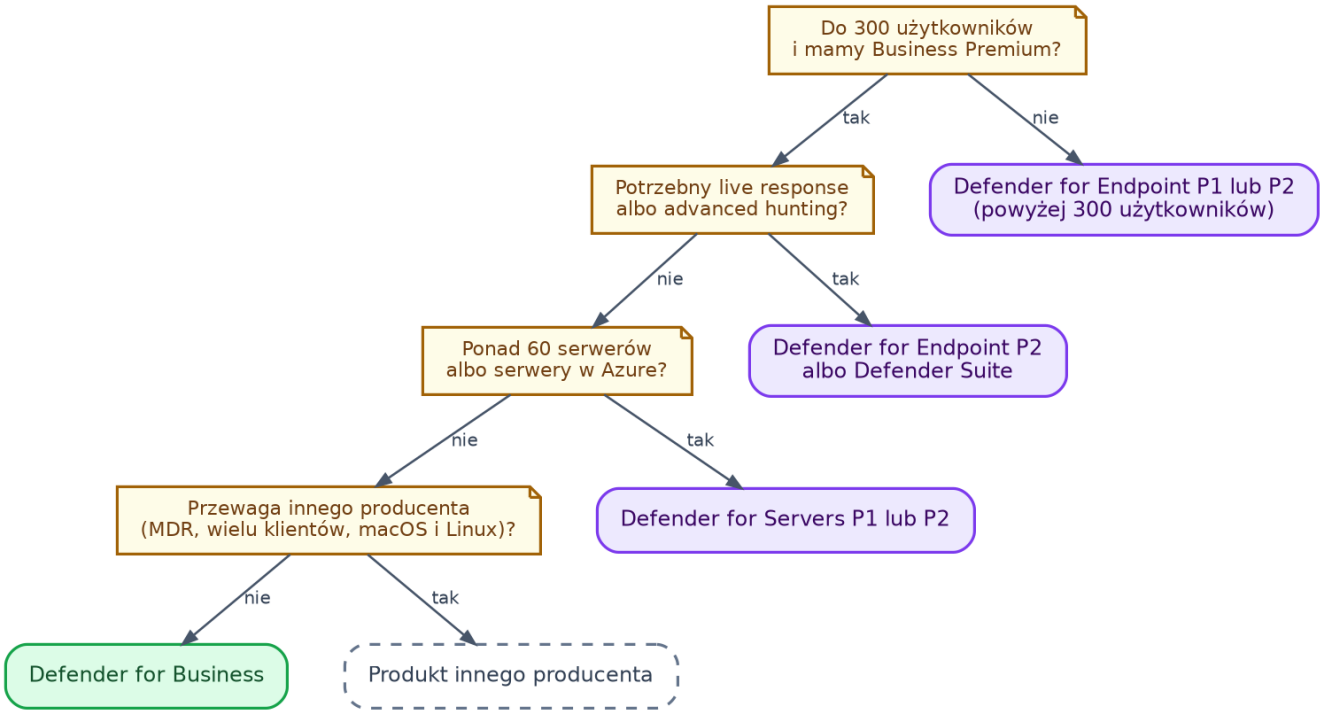
Microsoft Defender for Business	chmura Microsoftu, czujnik w systemie	w pakiecie, w wersji dla małych firm	serwery Windows i Linux z osobną licencją	portal Defender, opcjonalnie Intune	wbudowany w Windows, część Business Premium, wspólny portal z pocztą i tożsamością	brak advanced hunting i live response, brak usługi 24 godziny na dobę w pakiecie
ESET PROTECT	konsola w chmurze albo lokalna	ESET Inspect jako moduł wyższych pakietów	agenty dla serwerów, w tym ESET Server Security for Linux	konsola ESET PROTECT	usługa MDR w wyższych pakietach, europejski producent	EDR zależy od pakietu, zmieniające się nazwy pakietów
Bitdefender GravityZone	konsola w chmurze albo lokalna	w wyższych wydaniach, także oferta XDR	Windows, Linux, macOS, serwery fizyczne i wirtualne	GravityZone Control Center	ochrona przed ransomware z odtwarzaniem plików, Network Attack Defense	wiele wydań i dodatków, trzeba dobrać właściwe
Sophos Intercept X	chmura Sophos Central	EDR, XDR i MDR w kolejnych poziomach	Windows, macOS, Linux, serwery	Sophos Central	CryptoGuard cofa szyfrowanie plików, wspólna konsola z produktami Sophos	największy sens w całym ekosystemie Sophos
SentinelOne Singularity	platforma chmurowa, jeden agent	EDR i XDR w pakietach (Complete, Commercial)	Windows, macOS, Linux i środowiska chmurowe	jedna konsola, role i obsługa wielu dzierżaw	autonomiczne wykrywanie i reagowanie, ujednolicona konsola	wymaga osoby, która czyta konsolę, albo usługi MDR
CrowdStrike Falcon Go	platforma chmurowa, jeden agent	nie w Falcon Go, EDR dopiero w Falcon Enterprise	strona Falcon Go wymienia stacje Windows i urządzenia mobilne, Linux i serwery sprawdzamy przed zakupem	konsola Falcon	prosty start, ochrona nowej generacji i kontrola urządzeń USB	pakiet Go jest ochroną bez EDR

> Kolumna „Mocne strony" opisuje to, co producent sam podkreśla na swoich stronach, uzupełnione o cechy architektury. Opinie o skuteczności zostawiamy niezależnym testom, a nie tej bazie wiedzy.

Jak wybieramy

Decyzję podejmujemy według kilku pytań, w tej kolejności:

1. Czy już płacimy za Microsoft 365 Business Premium. Jeżeli tak, Defender for Business jest w cenie licencji i nie dokupujemy nic.
2. Czy mieścimy się w 300 użytkownikach. Jeżeli nie, wybieramy Plan 1 lub Plan 2.
3. Czy potrzebujemy live response albo advanced hunting. Jeżeli tak, potrzebny jest Plan 2 albo dodatek Defender Suite.
4. Czy mamy więcej niż 60 serwerów albo serwery w Azure. Wtedy Defender for Servers.
5. Czy potrzebujemy usługi 24 godziny na dobę, bo nikt w firmie nie patrzy na alerty w nocy. Wtedy porównujemy oferty MDR producentów albo partnerów.
6. Jaki mamy mix systemów. Przy wielu Linuksach i macOS zestawiamy listy obsługiwanych dystrybucji i dostępnych polityk.



Drzewo wyboru produktu: limit 300 użytkowników, live response, liczba serwerów i potrzeba usługi MDR prowadzą do Business, planów Defender for Endpoint, Defender for Servers albo innego producenta (kliknięcie otwiera pełny rozmiar)

Zielona kończy na pierwszej gałęzi: ma Business Premium, mieści się w limicie, nie potrzebuje live response i ma 26 serwerów. Brak usługi nocnej rekompensujemy procedurą dyżurnego ze strony Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie.

Częste błędy

Objaw	Przyczyna	Co robimy
W portalu brak możliwości onboardingu serwera	brak licencji Defender for Business servers albo brak płatnej licencji Business w subskrypcji	kupujemy licencję serwerową w Billing → Purchase services, albo odłączamy serwery od Defender for Business
Przycisk live response albo advanced hunting nie istnieje	to funkcje Planu 2, w Business ich nie ma	decydujemy, czy dokupujemy Plan 2 albo Defender Suite, pamiętając o zgłoszeniu do wsparcia przy przełączeniu doświadczenia
Szósty komputer jednego użytkownika nie dostaje ochrony	jedna licencja użytkownika obejmuje do pięciu urządzeń klienckich	przypisujemy dodatkową licencję albo ograniczamy liczbę urządzeń na konto
Po dokupieniu Planu 2 dla części osób nic się nie zmienia	mieszane licencje dają domyślnie doświadczenie Business	licencjonujemy wszystkich użytkowników na Plan 2 i zgłaszamy zmianę do wsparcia Microsoftu
Firma przekracza 300 użytkowników	Business jest ograniczony do 300	przy odnowieniu wybieramy plany dla dużych organizacji
Oferta konkurenta wygląda na „więcej funkcji"	pakiet zawiera usługę MDR albo moduły, których nie potrzebujemy	zestawiamy te same wiersze tabeli i pytamy, kto realnie będzie z nich korzystał

Ćwiczenia

1. Zielona dokupuje drugi oddział z 150 użytkownikami. Co sprawdzamy w licencjach Defender for Business?

Odpowiedź

Łączna liczba użytkowników byłaby 330, a limit Business to 300. Musimy wtedy przy odnowieniu wybrać plany dla dużych organizacji, na przykład Defender for Endpoint Plan 1 lub Plan 2, albo nie licencjonować części nowych osób w Defender for Business.

1. Dlaczego w tabeli porównawczej przy EDR w Falcon Go stoi „nie", skoro CrowdStrike jest znanym producentem EDR?

Odpowiedź

Według strony producenta Falcon Go zawiera ochronę nowej generacji, kontrolę urządzeń, ochronę mobilną i wsparcie, a EDR dochodzi dopiero w Falcon Enterprise. Nazwa producenta nie mówi nic o tym, co zawiera konkretny pakiet, więc porównujemy pakiety, nie marki.

1. Zielona ma 26 serwerów. Czy potrzebuje Defender for Servers?

Odpowiedź

Nie, jeżeli nie ma serwerów w Azure i nie potrzebuje funkcji Planu 2 dla serwerów. Defender for Business servers pozwala objąć do 60 serwerów w portalu Defender, więc 26 się mieści.

Powiązane: Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy · Defender for Business: EDR dla firmy, która nie ma zespołu bezpieczeństwa · Onboarding urządzeń: Intune, skrypt lokalny, GPO, serwery i Linux · Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia

Źródła: Microsoft Learn, „What is Microsoft Defender for Business?" · Microsoft Learn, „Microsoft Defender for Business FAQ" · Microsoft Learn, „Get Microsoft Defender for Business" · Microsoft Learn, „Microsoft Defender for Business requirements" · Microsoft Learn, „Manage your endpoint security subscription settings" · Microsoft Learn, „Take response actions on a device" · Microsoft Learn, „Onboard Windows servers to Microsoft Defender for Endpoint" · Microsoft Learn, „Microsoft Defender for Endpoint on Linux: prerequisites" · ESET, „ESET PROTECT subscription plans" (eset.com) · Bitdefender, „GravityZone Business Security" (bitdefender.com) · Sophos, „Sophos Endpoint" (sophos.com) · SentinelOne, „Platform packages" (sentinelone.com) · CrowdStrike, „Falcon Go" (crowdstrike.com)