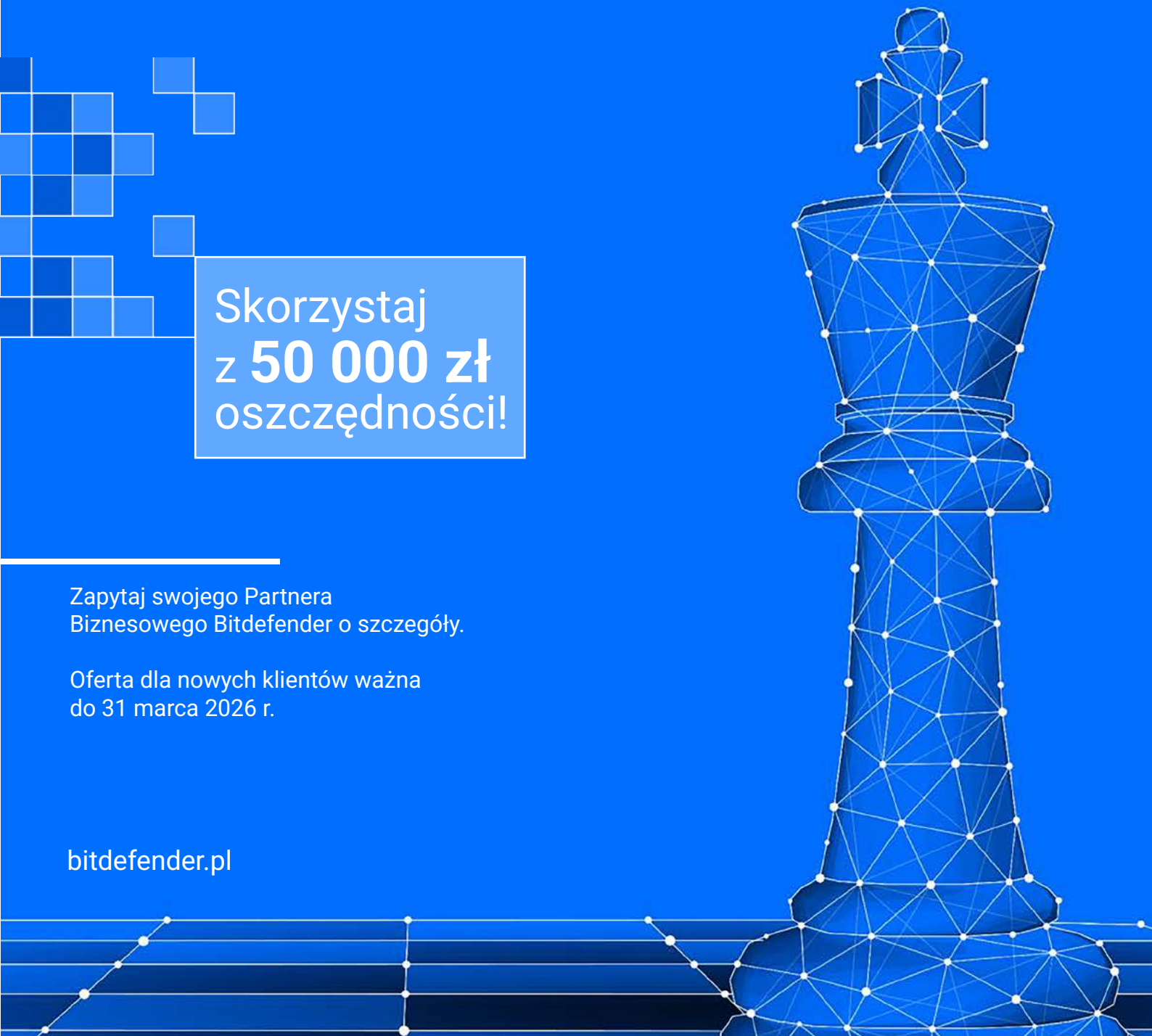
Bitdefender Global Leader In Cybersecurity

W 2026 wybierz cyberbezpieczeństwo klasy enterprise

Pakiety GravityZone Business Security Enterprise integrują **redukcję powierzchni ataku**, **zarządzanie** podatnościami, detekcję i reakcję, **ochronę danych** oraz **zgodność** regulacyjną.



Skorzystaj z **50 000 zł** oszczędności!

Zapytaj swojego Partnera Biznesowego Bitdefender o szczegóły.

Oferta dla nowych klientów ważna do 31 marca 2026 r.

bitdefender.pl

Pakiet Redukcja zawiera:

Przy rosnącej skali i dynamice cyberataków, przewidywanie i minimalizacja ryzyk stają się warunkiem koniecznym stabilnego prowadzenia biznesu.

Dlatego przygotowaliśmy pakiety GravityZone Business Security Enterprise, których komponenty tworzą, uzupełniają i integrują obszary bezpieczeństwa - od utwardzania procesów i redukcji powierzchni ataku (PHASR), przez rozszerzoną detekcję i reakcję (XDR), zarządzanie podatnościami (PM), po ochronę danych (FDE).

Platforma GravityZone Business Security Enterprise

Dodatkowe komponenty
+ Proactive Hardening and Attack Surface Reduction
+ Patch Management
+ Full Disk Encryption

Platforma GravityZone Business Security Enterprise

Zintegrowana platforma ochrony punktów końcowych z zaawansowaną prewencją, wykrywaniem i reakcją.

- **Skalowalność klasy enterprise**, dla środowisk hybrydowych, wielooddziałowych i wysoko regulowanych.
- Pełna widoczność incydentów dzięki telemetrycznym danym i analizie zachowań **w czasie rzeczywistym**.
- **EDR o wysokiej skuteczności**, umożliwiający szybkie dochodzenie, korelację i reakcję na zagrożenia.
- **Wielowarstwowa architektura ochrony**, obejmująca antymalware, exploit defense, sieć, pamięć i zachowania.
- **Pełna integracja** z PHASR i Patch Management, tworząca kompletny ekosystem bezpieczeństwa.

Proactive Hardening and Attack Surface Reduction (PHASR)

Ogranicza powierzchnię ataków typu Living off the Land o 95%

- **Redukcja powierzchni ataku o 95%** dzięki zaawansowanej AI do identyfikacji i blokowania niepotrzebnych lub ryzykownych narzędzi i operacji.
- Proaktywne **ograniczanie ataków** typu Living-Off-The-Land przez dynamiczne ograniczenie wykorzystywanie zaufanych, lecz rzadko używanych narzędzi jako wektorów ataku.
- Utwardzanie systemu i **dopasowanie zabezpieczeń do indywidualnego profilu użytkownika** i punktu końcowego, bez zakłócania pracy.
- Granularna kontrola i ograniczanie konkretnych, ryzykownych działań wewnątrz dozwolonych narzędzi.
- Raportowanie metryk powierzchni ataku i poziomu redukcji ryzyka do monitorowania stanu i uzasadniania inwestycji.
- **Komplementarny dla EDR** – przewiduje i ogranicza zagrożenia tam, gdzie EDR nie ma widoczności.

Patch Management (PM)

Eliminowanie podatności dzięki stałemu utrzymaniu środowiska w aktualnym stanie.

- **Automatyczna dystrybucja** poprawek na fizyczne i wirtualne stacje robocze oraz serwery.
- Centralne zarządzanie aktualizacjami w całej infrastrukturze – **jeden wygodny panel, pełna kontrola**.
- Obsługa poprawek systemowych i aplikacyjnych, w tym Microsoft, Linux i aplikacji firm trzecich.
- **Pełna widoczność stanu patchowania:** braków, opóźnień, zgodności i priorytetów.
- Pełne pokrycie systemów: Windows (od wersji 8), Linux (CentOS, RHEL, SLE), macOS oraz 100+ aplikacji trzecich (np. Adobe, Microsoft).

Full Disk Encryption (FDE)

W pełni szyfruje dysk twardy każdego punktu końcowego i zmniejsza ryzyko przypadkowej utraty lub kradzieży danych.

- **Automatyczna kontrola zgodności** z regulacjami, takimi jak RODO
- Wykorzystuje natywne mechanizmy szyfrowania w systemach Windows (BitLocker) i macOS (FileVault), co minimalizuje wpływ na wydajność.
- Nie wymaga dodatkowego agenta, **a wdrożenie jest szybkie**, **intuicyjne** i odbywa się z jednej konsoli zarządzania.

Pakiet Detekcja & Reakcja
zawiera:

Platforma GravityZone Business Security Enterprise
Dodatkowe komponenty
+ XDR
+ Patch Management
+ Full Disk Encryption

Sensory GravityZone XDR zapewniają ciągłe monitorowanie aplikacji, tożsamości, sieci oraz środowisk chmurowych, wykrywając anomalie i działania charakterystyczne dla pełnego cyklu ataku: nadużycia kont i eskalacji uprawnień, ruch lateralny i próby eksfiltracji danych.

Dzięki korelacji zdarzeń z Office 365, Active Directory, Atlassian Cloud, AWS, Azure, Google Cloud i sieci firmowej umożliwiają szybką reakcję zespołów bezpieczeństwa oraz skuteczne ograniczanie skutków incydentów.

Poznaj, jak sensory XDR chronią firmę:

Sensor chmury / GravityZone XDR Cloud Sensor

Monitoruje środowiska chmurowe, takie jak AWS, Microsoft Azure, Google Cloud wykrywając nietypowe działania i potencjalne zagrożenia.

AWS
Analizuje wzorce zachowań, wychwytuje podejrzane operacje w funkcjach Lambda, zmiany w grupach zabezpieczeń, manipulacje w S3 oraz nietypowe logowania. Dzięki temu zespoły bezpieczeństwa mogą szybko reagować i chronić chmurę przed atakami. Sensor ponadto wykrywa także podejrzane działania, takie jak usunięcie domyślnego szyfrowania zasobów S3 przez nieznanego użytkownika lub hosta.

Microsoft Azure
Monitoruje aktywność wskazującą na potencjalne naruszenia bezpieczeństwa środowiska Microsoft Azure i wykrywa incydenty na dowolnym etapie cyklu życia ataku. Sensor umożliwia wykrywanie np. usuwania dzienników zdarzeń, anomalii w zachowaniu, tworzenie kont Azure automation oraz próby utworzenia publicznego anonimowego dostępu do zasobów.

Google Cloud
Monitoruje aktywność pod kątem naruszeń bezpieczeństwa wykrywając np. takie działania jak usunięcie dziennika audytu, próby ukrycia działań wykonywanych przez cyberprzestępców, usunięcie kopii zapasowej magazynu oraz identyfikowanie modyfikacji tras i zapory sieciowej VPC. Sensor rozpoznaje również modyfikacje konfiguracji IAM.

Sensor sieci / GravityZone XDR Network Sensor

Monitoruje ruch sieciowy w poszukiwaniu oznak ataku. Pomaga wykrywać próby poruszania się atakującego po sieci firmowej oraz próby eksfiltracji danych poza organizację. Sensor rozpoznaje także skanowanie portów i ataki sieciowe typu brute-force, wspierając szybką reakcję zespołów bezpieczeństwa.

Business Applications

Sensor aplikacji biznesowych Atlassian Cloud stale monitorują platformy takie jak Confluence, Jira i Bitbucket, pomagając chronić wrażliwe dane, wykrywać podejrzane działania i zapobiegać nieautoryzowanemu dostępowi. Czujnik pobiera dzienniki audytów i logi z Atlassian Admin.

Sensor tożsamości / Bitdefender XDR Identity Sensor

IMonitorują i analizują aktywność, tożsamości użytkowników, kontrolę dostępów i uwierzytelnienie w sieci lub środowisku chmurowym organizacji.

Active Directory
Zbiera i analizuje aktywność logowania użytkowników, zmiany konfiguracji oraz inne zdarzenia związane z tożsamością. Monitoruje zdarzenia w Active Directory wykrywając próby użycia skompromitowanych kont, podejrzane logowania, ataki typu brute-force, nietypowe działania w protokole Kerberos oraz podejrzane operacje w zdalnych systemach i obiektach Active Directory. Dzięki temu pomaga zespołom bezpieczeństwa szybko reagować, np. blokując konto lub wymuszając reset hasła, aby zapobiec dalszym naruszeniom bezpieczeństwa.

Azure AD
Sensor gromadzi i przetwarza aktywności i konfiguracje logowania wykrywając naruszenia na całej długości łańcucha ataku. Czujnik analizuje logowania użytkowników pod kątem znaczników czasu, geolokalizacji, adresów IP. Umożliwia wykrywanie ataków Brute Force lub nieudane logowania z jednej lokalizacji.

Sensor aplikacji / Bitdefender XDR Productivity

Identyfikuje szczególne aspekty kont Office 365, które mogą wskazywać na aktywność cyberprzestępczą. Sensor wykrywa następujące działania:

- wyłączanie ochrony antyphishingowej w Office 365
- podejrzane działanie dotyczące tworzenia użytkowników, np. wykrywa utworzenie użytkownika z wyłączonym 2fa
- dodawanie dokumentów z podejrzanymi makrami do SharePoint i OneDrive
- przesyłanie plików wykonywalnych na skrzynki pocztowe kont Office 365
- Monitorowanie usług poczty Microsoft Exchange Online aby zidentyfikować i powstrzymywać próby kradzieży danych.

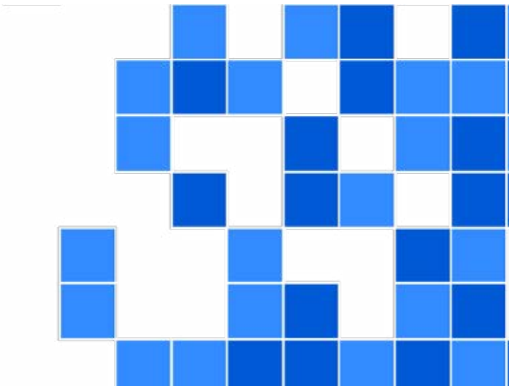
Wybrane przedziały cenowe i oszczędności

Pakiet Redukcja:		50-99	100 - 149	150-249	powyżej 250
Platforma GravityZone Business Security Enterprise, PHASR, PM, FDE	**Cena w tej ofercie dla 1 licencji**	233,20 zł	209,00 zł	188,62 zł	warunki ustalane indywidualnie
	Cena w tej ofercie dla minimalnej liczby licencji	11 660,00 zł	20 900,00 zł	47 155,63 zł	
	Cena standardowa dla 1 licencji	470,35 zł	436,69 zł	394,12 zł	
	Cena standardowa dla minimalnej liczby licencji	23 517,50 zł	43 669,00 zł	98 530,00 zł	
Łączna oszczędność dla Twojej organizacji	**Oszczędność z różnicy cen dla 1 licencji**	237,15 zł	227,69 zł	205,50 zł	
	Oszczędność z różnicy cen dla minimalnej liczby licencji	**11 857,34 zł**	**22 769,30 zł**	**51 374,40 zł**	

Powyższe wartości dotyczą licencji jednorocznych.
Regulamin oferty dostępny u Partnera Biznesowego Bitdefender oraz na www.bitdefender.pl

Pakiet Detekcja & Reakcja:		50-99	100-149	150-250	powyżej 250
Platforma GravityZone Business Security Enterprise, Sensor XDR, PM, FDE	**Cena w tej ofercie dla 1 licencji**	233,20 zł	209,00 zł	188,62 zł	warunki ustalane indywidualnie
	Cena w tej ofercie dla minimalnej liczby licencji	11 660,00 zł	20 900,00 zł	47 155,63 zł	
	Cena standardowa dla 1 licencji	472,06 zł	436,42 zł	392,28 zł	
	Cena standardowa dla minimalnej liczby licencji	23 603,00 zł	43 642,00 zł	98 070,00 zł	
Łączna oszczędność dla Twojej organizacji	**Oszczędność z różnicy cen dla 1 licencji**	238,86 zł	227,42 zł	203,65 zł	
	Oszczędność z różnicy cen dla minimalnej liczby licencji	**11 942,84 zł**	**22 742,30 zł**	**50 913,15 zł**	

Powyższe wartości dotyczą licencji jednorocznych.
Regulamin oferty dostępny u Partnera Biznesowego Bitdefender oraz na www.bitdefender.pl



O Bitdefender

Bitdefender to globalny dostawca technologii cyberbezpieczeństwa, działający od 2001 roku. Rozwiązania firmy są wykorzystywane w ponad 170 krajach przez przedsiębiorstwa, instytucje publiczne oraz użytkowników indywidualnych. Bitdefender rozwija własne, opatentowane technologie ochrony i prowadzi zaawansowane prace badawczo-rozwojowe w obszarze analizy zagrożeń, ochrony danych oraz automatyzacji bezpieczeństwa.

NAGRODY

Skuteczność i dojrzałość rozwiązań Bitdefender potwierdzają liczne, niezależne wyróżnienia. W Polsce platforma GravityZone PHASR została nagrodzona przez redakcję IT Professional tytułem „Produkt Roku 2025" w kategorii ochrony punktów końcowych za innowacyjne podejście do dynamicznej redukcji powierzchni ataku, w szczególności wobec technik typu Living off the Land.

Na poziomie globalnym Bitdefender po raz czwarty z rzędu został wskazany przez Gartnera jako Representative Vendor w raporcie 2025 Gartner Market Guide for MDR, co potwierdza jego pozycję w obszarze usług Managed Detection and Response.

Gartner

Bitdefender osiągnął również niemal idealny wynik 99,8% skuteczności ochrony w najnowszym teście AV-Comparatives Business Security Test, blokując 437 z 438 scenariuszy ataków przy jednoczesnych najwyższych ocenach wydajności („Very Fast"). Otrzymał certyfikację AV Comparatives EPR jako najlepsze ogólne rozwiązanie Endpoint Prevention and Response.

Bitdefender otrzymał wyróżnienie Gartner Peer Insights Customers' Choice 2025 za wysokie oceny i rekomendacje użytkowników swojej platformy Bitdefender GravityZone Business Security w raporcie Voice of the Customer for Endpoint Protection Platforms (EPP). Co więcej Bitdefender został jedyną firmą określoną jako Visionary w Gartner Magic Quadrant 2025 dla EPP.

W Polsce produkty Bitdefender są oficjalnie dystrybuowane od 2012 roku, wspierając organizacje w budowaniu odporności na zaawansowane cyberzagrożenia.

Zapraszamy do kontaktu z Twoim Partnerem Biznesowym Bitdefender.

bitdefender.pl