PRZEWODNIK

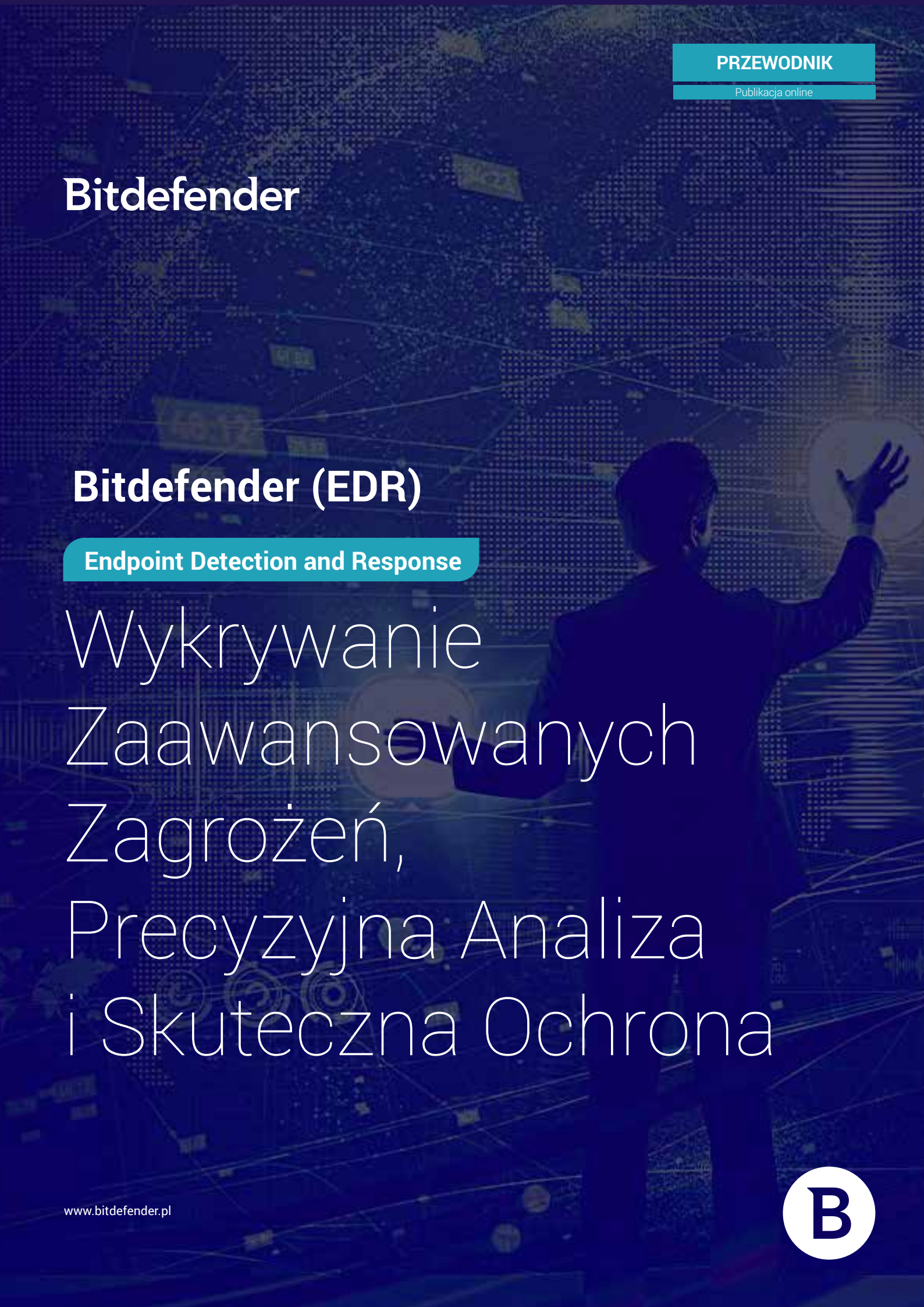
Publikacja online

Bitdefender

Bitdefender (EDR)

Endpoint Detection and Response

Wykrywanie Zaawansowanych Zagrożeń, Precyzyjna Analiza i Skuteczna Ochrona



www.bitdefender.pl

Zaawansowane zagrożenia są wyzwaniem dla firm

W dzisiejszych czasach cyberprzestępcy stają się coraz bardziej wyrafinowani, a dokonywane przez nich ataki są coraz bardziej zaawansowane i trudniejsze do wykrycia.
Korzystając z technik, które osobno sprawiają wrażenie rutynowego zachowania, atakujący może uzyskać dostęp do Twojej infrastruktury i pozostać niewykryty przez wiele miesięcy, co znacznie zwiększa ryzyko finansowe związane z naruszeniem bezpieczeństwa danych.

Jak przeciwdziała im Bitdefender Endpoint Detection and Response (EDR)?

Kiedy istniejące zabezpieczenia punktów końcowych nie zapewniają zaawansowanej widoczności ataków i odpowiedniej możliwości reakcji - dodanie łatwego w użyciu Bitdefender Endpoint Detection and Response (EDR) szybko i skutecznie wzmacnia Twoje procedury bezpieczeństwa.

Zaawansowane wykrywanie i reagowanie na ataki

Bitdefender EDR monitoruje Twoją sieć, aby wcześnie wykryć podejrzaną aktywność i dostarcza narzędzi, które pozwolą Ci odeprzeć cyberataki.

- EDR integruje nagradzaną technologię uczenia maszynowego, skanowanie w chmurze i Analizator Sandbox Bitdefender w celu wykrywania aktywności, która wymyka się tradycyjnym mechanizmom ochrony punktów końcowych.
- Pełna widoczność technik, taktyk i procedur (TTP) wykorzystywanych do ataków na Twoje systemy.
- Zaawansowane możliwości wyszukiwania określonych wskaźników naruszenia bezpieczeństwa (IoC), technik MITRE ATT&CK oraz innych incydentów w celu wykrycia ataków na wczesnym etapie.
  W ewaluacji MITRE ATT&CK z kwietnia 2020 r. Bitdefender osiągnął najlepszy wynik pod względem wykrywania i alertów umożliwiających podjęcie działań na każdym etapie przebiegu ataku.
- Podejmowanie działań zaradczych w celu usunięcią luk i wyeliminowania ryzyka ponownych ataków.

Niwelowanie luki w umiejętnościach z zakresu cyberbezpieczeństwa

- Łatwa do opanowania, wbudowana kontrola mechanizmów reagowania umożliwiająca Twoim pracownikom skuteczną reakcję, ograniczenie rozprzestrzeniania się zagrożeń i powstrzymanie zainicjowanych ataków.
- Wizualizacja zagrożeń pozwala ukierunkować działania rozpoznawcze, zrozumieć zaawansowane wykrywanie, zidentyfikować pierwotną przyczynę ataku i maksymalizować możliwość bezpośredniego reagowania.
- Zautomatyzowana priorytetyzacja alertów daje możliwość rozwiązywania problemów jednym kliknięciem.

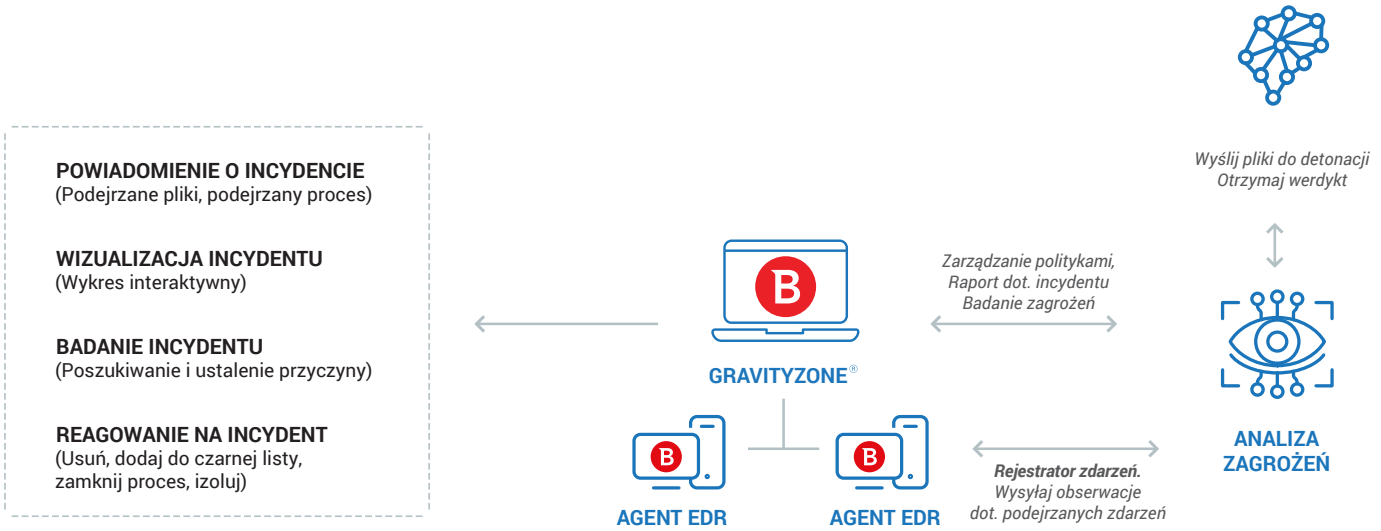
Redukcja ryzyka organizacyjnego

- EDR stale analizuje Twoją organizację, korzystając z unikalnych możliwości identyfikowania setek czynników ryzyka. Zawiera jasne wskazówki, które pomogą Ci zmniejszyć niebezpieczeństwa związane z użytkownikiem, siecią i systemem operacyjnym.

Minimalizacja obciążeń operacyjnych

- Dostarczany w chmurze, nie wymagający wysokich nakładów, EDR jest łatwy do wdrożenia i integracji z istniejącą architekturą bezpieczeństwa oraz w pełni kompatybilny z oprogramowaniem antywirusowym dla punktów końcowych.
- Lekki agent zużywa mało zasobów dyskowych, pamięci, łącza i procesora.
- Elastyczna, skalowalna platforma z możliwością rozszerzenia dla zaawansowanej ochrony punktów końcowych Bitdefender oraz dla zarządzanego wykrywania i reagowania (MDR).

Sposób działania



Powyżej: Bitdefender Endpoint Detection and Response

Bitdefender EDR to rozwiązanie dostarczane w chmurze, zbudowane na platformie chmurowej Bitdefender GravityZone. Agenci EDR są rozmieszczeni w punktach końcowych organizacji. Każdy agent EDR posiada rejestrator zdarzeń, który stale monitoruje punkt końcowy i bezpiecznie wysyła informację zwrotną o podejrzanych zdarzeniach do chmury GravityZone.

W GravityZone moduł Analizy Zagrożeń zbiera i przetwarza zdarzenia w punktach końcowych w formie listy incydentów z określeniem ich priorytetu w celu dodatkowego zbadania i reakcji. Wysyła podejrzane pliki do detonacji w Analizatorze Sandbox, a następnie wykorzystuje werdykt analizatora w raportach incydentów w EDR. Panel Nawigacyjny EDR, wyświetlający informacje dotyczące ochrony w czasie rzeczywistym, jest dostępny z dowolnego urządzenia. Umożliwia to administratorom wyświetlanie alertów i wizualizacji, a następnie badanie i skuteczne reagowanie na zagrożenia.

Funkcje Bitdefender Endpoint Detection and Response

Analiza ryzyka

Analityka ryzyka ludzkiego i ryzyka punktów końcowych

Stale analizuje ryzyko organizacyjne przy użyciu setek czynników, aby identyfikować zagrożenia, ustalać priorytety i dostarczać wskazówek dotyczących ograniczania ryzyka związanego z użytkownikami, siecią i punktami końcowymi.

Wykrywanie

Wiodąca technologia wykrywania zagrożeń

Wykrywa w czasie rzeczywistym zaawansowane zagrożenia, w tym ataki bezplikowe, oprogramowanie ransomware i inne zagrożenia 0-day. Uzupełnia i wzmacnia stosowaną ochronę punktów końcowych dla ulepszonego wykrywania.

Analiza zagrożeń

Oparty na chmurze kolektor w sposób ciągły przetwarza zdarzenia w punktach końcowych w formie incydentów z określeniem ich priorytetu w celu dodatkowego zbadania i reakcji.

Rejestrator zdarzeń

Stałe monitorowanie zdarzeń w punktach końcowych, w ramach którego przekazywane są one do analizy w celu stworzenia wizualizacji etapów przebiegu ataku.

Analizator Sandbox

Automatycznie detonuje podejrzane pliki w zamkniętym środowisku wirtualnym. Moduł wykorzystuje następnie przeprowadzoną analizę do podejmowania decyzji dotyczących podejrzanych plików.

Badanie i reagowanie

Wyszukiwanie IoC

Przeszukuj bazę danych zdarzeń, aby wykryć zagrożenia. Odkryj techniki MITRE ATT&CK i wskaźniki ataku. Wgląd w aktualne zagrożenia i złośliwe oprogramowanie, które może być z nimi związane.

Wizualizacja

Łatwe do zrozumienia przewodniki wizualne, wzbogacone o kontekst i informacje o zagrożeniach, podkreślają kluczowe ścieżki ataku, odciążając personel IT. Pomocne dla identyfikacji luk w ochronie i określenia wagi incydentów w celu zapewnienia przestrzegania procedur bezpieczeństwa.

Detonacja

Badanie w Analizatorze Sandbox inicjowane przez operatora pomaga podejmować świadome decyzje dotyczące podejrzanych plików.

Czarna lista

Zatrzymaj rozprzestrzenianie się podejrzanych plików lub procesów wykrytych przez EDR na inne komputery.

Zamykanie procesów
Natychmiast zakończ podejrzane procesy, aby powstrzymywać potencjalne aktywne incydenty.

Izolacja sieci
Blokuj połączenia do i z punktu końcowego w celu zatrzymania ruchu bocznego i dalszych naruszeń podczas badania incydentów.

Zdalna powłoka
Wykonuj polecenia zdalne na dowolnej stacji roboczej w celu natychmiastowej reakcji na bieżące incydenty.

Raportowanie i ostrzeganie

Pulpity nawigacyjne i raporty
Konfigurowalne pulpity nawigacyjne oraz wszechstronne możliwości natychmiastowego i zaplanowanego raportowania.

Powiadomienia
Konfigurowalny pulpit nawigacyjny i powiadomienia e-mail.

Integracja SIEM i obsługa API
Obsługuje dalszą integrację z narzędziami innych firm.

Wydajność i zarządzanie

Zoptymalizowany agent EDR
Niskie zużycie procesora, pamięci RAM i miejsca na dysku.

Konsola internetowa
Łatwe w użyciu zarządzanie w chmurze.

DLACZEGO BITDEFENDER?

NIEZRÓWNANY LIDER INNOWACJI.

38% wszystkich dostawców rozwiązań z zakresu cyberbezpieczeństwa na całym świecie wdrożyło co najmniej jedno rozwiązanie Bitdefender. Obecny w 150 państwach.

ŚWIATOWY LIDER W ZAKRESIE KOMPLEKSOWEJ OCHRONY

Wiodące rozwiązanie zabezpieczające, które integruje funkcje wzmocnionej ochrony, zapobiegania zagrożeniom, wykrywania i reagowania na incydenty w punktach końcowych, sieci i chmurze.

Numer 1 w rankingach oprogramowania zabezpieczającego

Bitdefender

www.bitdefender.pl

Oficjalny dystrybutor produktów Bitdefender w Polsce:
Marken Systemy Antywirusowe
ul. Armii Krajowej 23/13, 81-366 Gdynia
tel: 58 667 49 49
www.marken.com.pl

OCHRONA SPOD ZNAKU WILKA

Bezpieczeństwo danych, będące dziedziną genialnych innowacji, a zarazem branżą, w której kluczem do skutecznego stawiania czoła wyzwaniom jest najwyższy poziom spostrzegawczości, inteligencji i wnikliwości - to gra z zerowym marginesem błędu. Naszym zadaniem jest zwyciężać za każdym razem, tysiąc razy na tysiąc i milion razy na milion.

To właśnie robimy. Jesteśmy liderami branży nie tylko dzięki spostrzegawczości, inteligencji i wnikliwości naszych specjalistów, ale także dzięki temu, że jesteśmy o krok przed wszystkimi, zarówno tzw. "czarnymi kapeluszami", jak i innymi ekspertami w dziedzinie bezpieczeństwa. Błyskotliwe dzieło pracy naszego zespołu ekspertów jest po Twojej stronie niczym legendarny ałunowy "Dacki smok", napędzany inżynierską intuicją, stworzony by chronić Cię przed wszelkimi niebezpieczeństwami kryjącymi się w tajemnych zawiłościach cyfrowego królestwa.