WYKRYWANIE ZAAWANSOWANYCH ZAGROŻEŃ,
PRECYZYJNA ANALIZA I SKUTECZNA OCHRONA

BITDEFENDER ENDPOINT DETECTION AND RESPONSE (EDR)

Bitdefender®

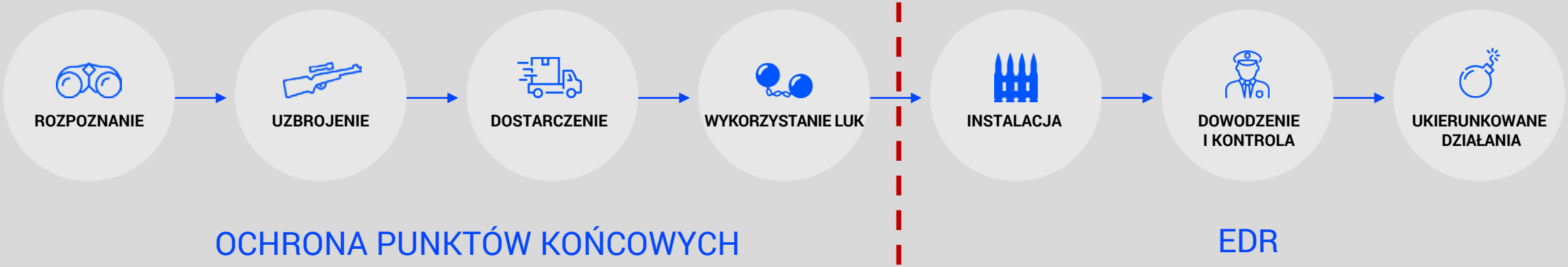
WWW.BITDEFENDER.PL

AGENDA

- Zaawansowane zagrożenia - wyzwania dla klientów
- Zalety Bitdefender EDR:
  - Zaawansowane wykrywanie i reagowanie na ataki
  - Niwelowanie braków w umiejętno-ściach z zakresu cyberbezpieczeństwa
  - Określenie ryzyka organizacyjnego
  - Zmniejszenie obciążenia operacyjnego
- Jak to działa?
- Dlaczego Bitdefender EDR?
- Podsumowanie
- Pakiety EDR

WYZWANIA ZWIĄZANE Z ZAAWANSOWANYMI ZAGROŻENIAMI

- Co się stanie, jeśli zapobieganie zawiedzie?
- Coraz trudniej wykryć cyberprzestępców
- Pojedyncze techniki ataków wyglądają jak rutynowe zachowania
- Rozwiązania EDR mogą być skomplikowane, a wykwalifikowany personel trudny do znalezienia
- Rozwiązania muszą minimalizować obciążenie zasobów, być elastyczne i łatwe do wdrożenia

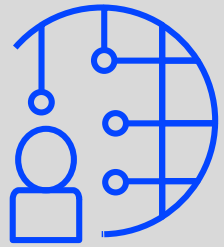


ZALETY BITDEFENDER EDR

JAKIE SĄ ZALETY ROZWIĄZANIA BITDEFENDER EDR?

ZAAWANSOWANE WYKRYWANIE I REAGOWANIE NA ATAKI

NIWELOWANIE BRAKU WIEDZY I UMIEJĘTNOŚCI Z ZAKRESU CYBERBEZPIECZEŃSTWA



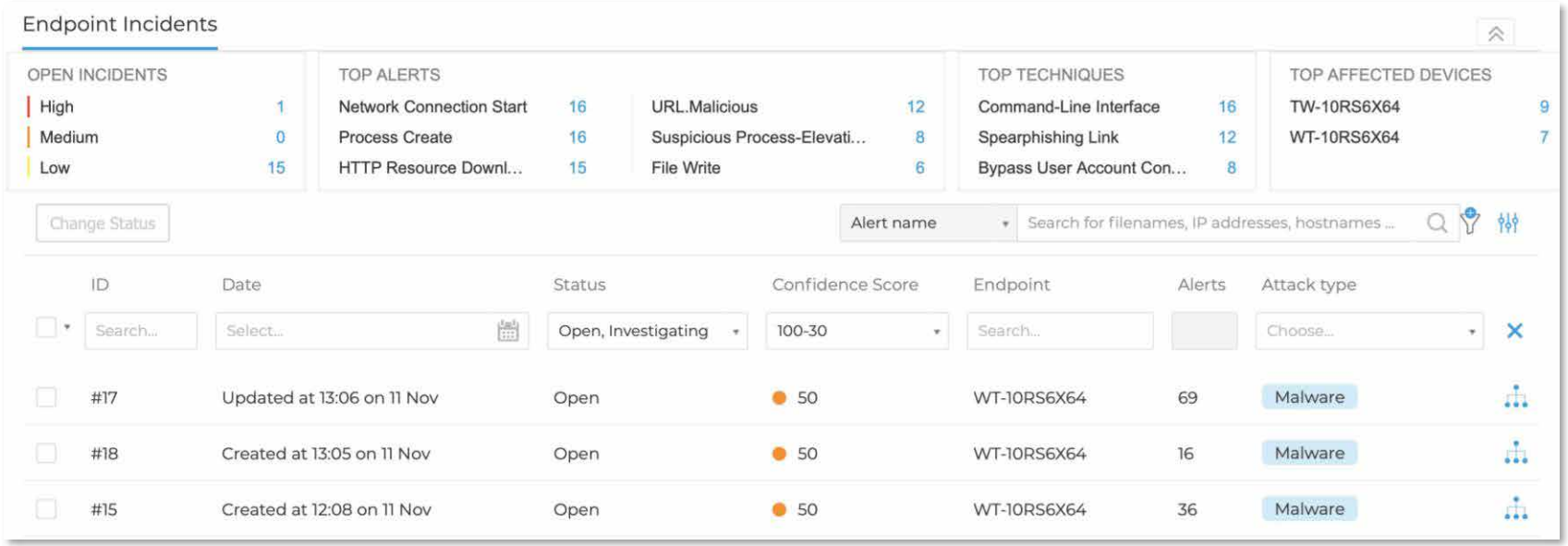
OKREŚLENIE RYZYKA ORGANIZACYJNEGO

ZMNIEJSZENIE OBCIĄŻENIA OPERACYJNEGO

Kiedy Twoje dotychczasowe zabezpieczenie punktów końcowych nie zapewnia zaawansowanej widoczności ataków i odpowiedniego reagowania, wdrożenie Bitdefender Endpoint Detection and Response (EDR) szybko i skutecznie wzmacnia Twój system bezpieczeństwa.

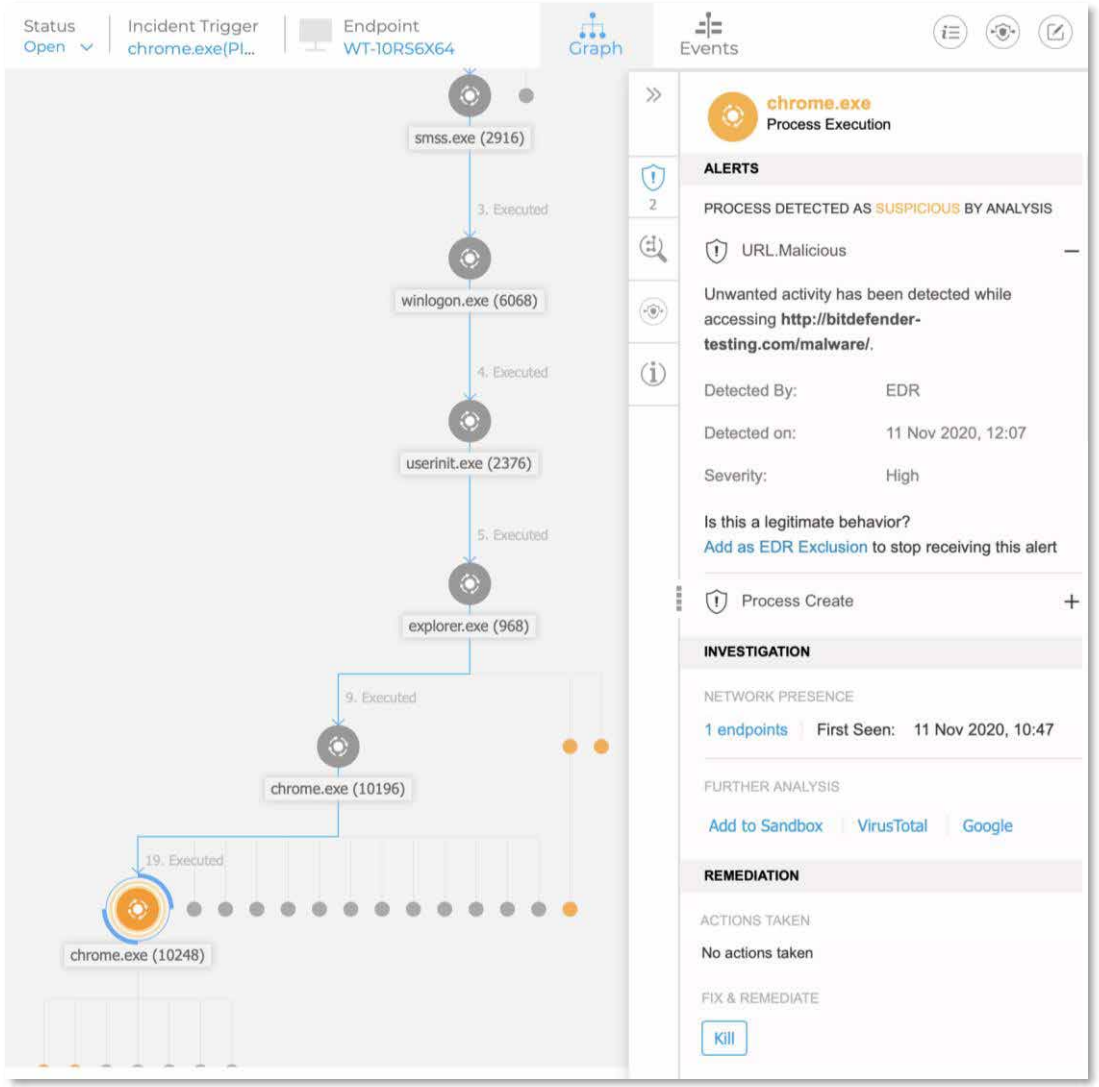
ZAAWANSOWANE WYKRYWANIE I REAGOWANIE NA ATAKI

- Wykrywanie podejrzanej aktywności
- Uczenie maszynowe, skanowanie w chmurze i sandbox
- MITRE ATT&CK i wyszukiwanie IoC
- Reagowanie na incydenty
  - Zamknięcie lub blokowanie procesu
  - Izolowanie
  - Rozpoczęcie analizy sandbox
  - Blokowanie hashów
  - Łączenie się zdalnie



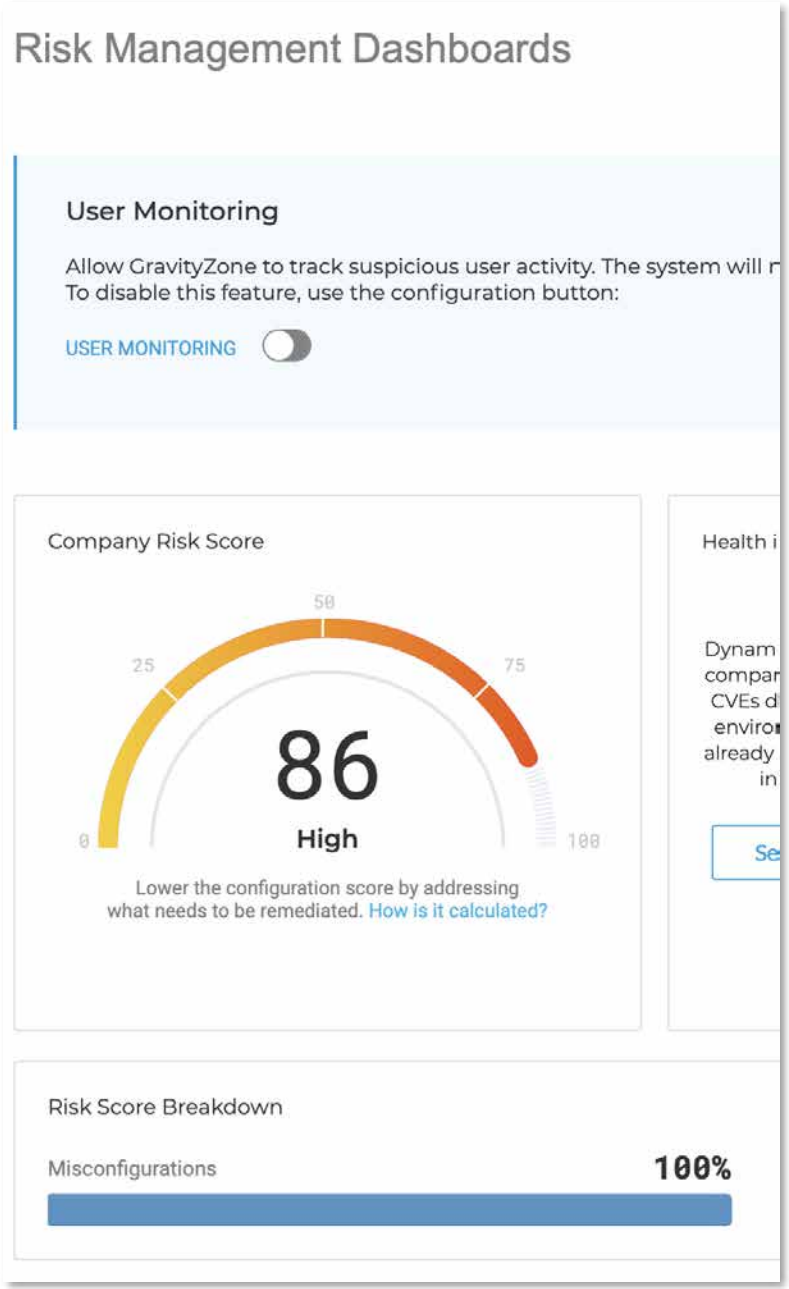
NIWELOWANIE LUKI W UMIEJĘTNOŚCIACH Z ZAKRESU CYBERBEZPIECZEŃSTWA

- Reagowanie, ograniczanie rozprzestrzeniania się, powstrzymanie ataku
- Wizualizacja zagrożeń
- Złożone ataki łatwe do zrozumienia
- Identyfikacja pierwotnej przyczyny
- Automatyczna priorytetyzacja alertów
- Reagowanie jednym kliknięciem



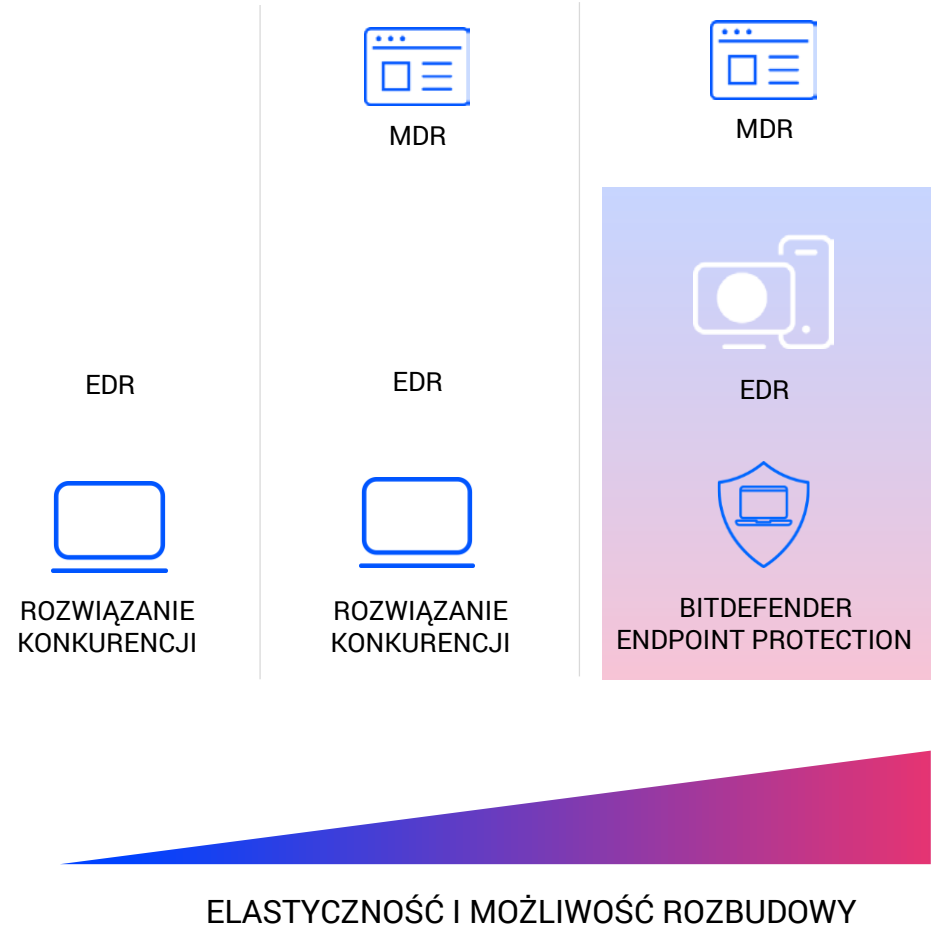
OKREŚLENIE RYZYKA ORGANIZACYJNEGO

- Zidentyfikujesz ryzyko na podstawie setek czynników
- Wskazówki dotyczące ograniczania ryzyka związanego z użytkownikami, siecią i systemem operacyjnym



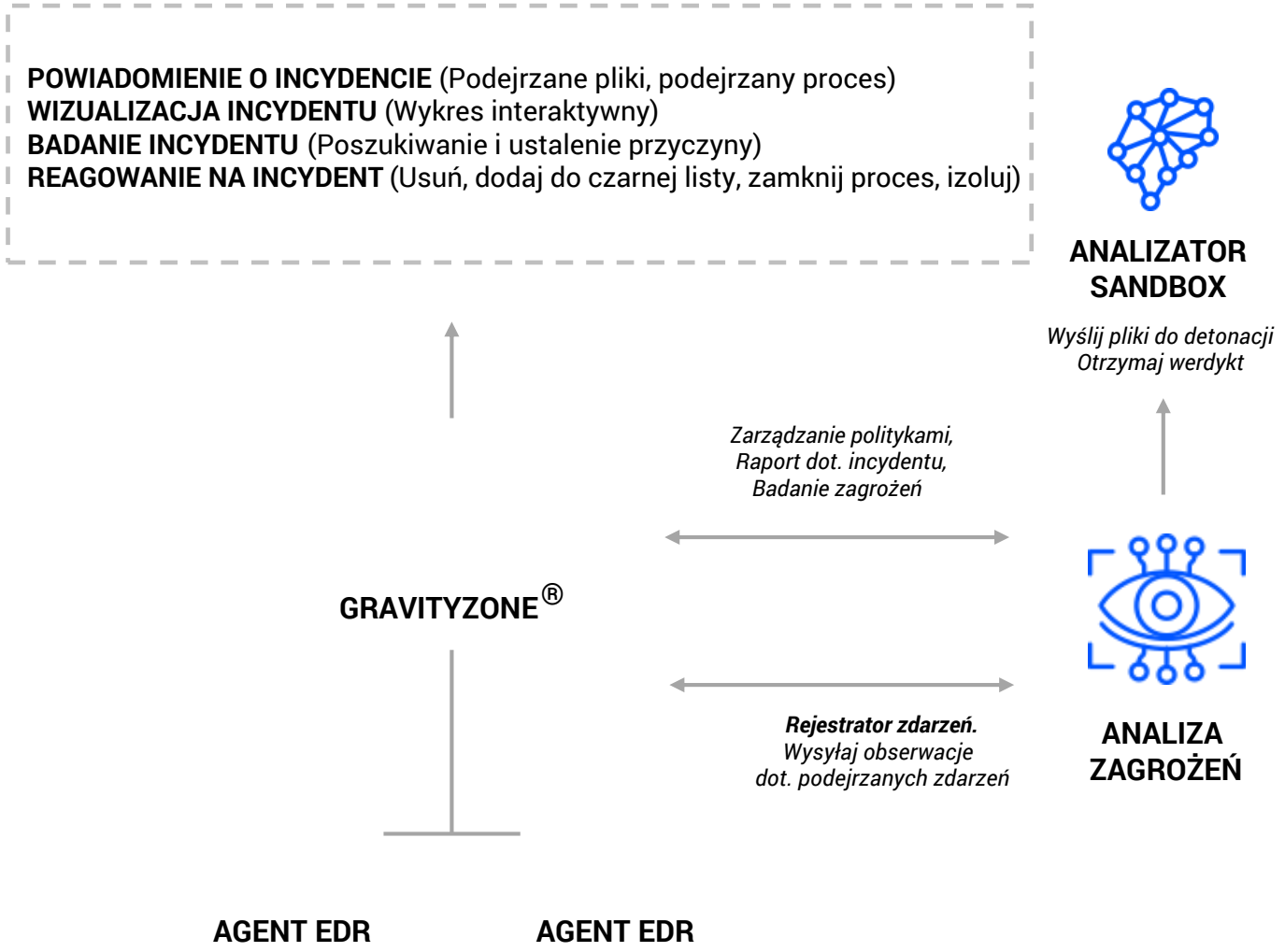
ZMNIEJSZENIE OBCIĄŻENIA OPERACYJNEGO

- Rozwiązanie chmurowe z niskimi kosztami utrzymania
- Proste wdrożenie
- Lekki agent
- Pełna kompatybilność z systemami antywirusowymi innych firm
- Elastyczność i możliwość rozbudowy



JAK TO DZIAŁA?

SPOSÓB DZIAŁANIA



DLACZEGO BITDEFENDER EDR?

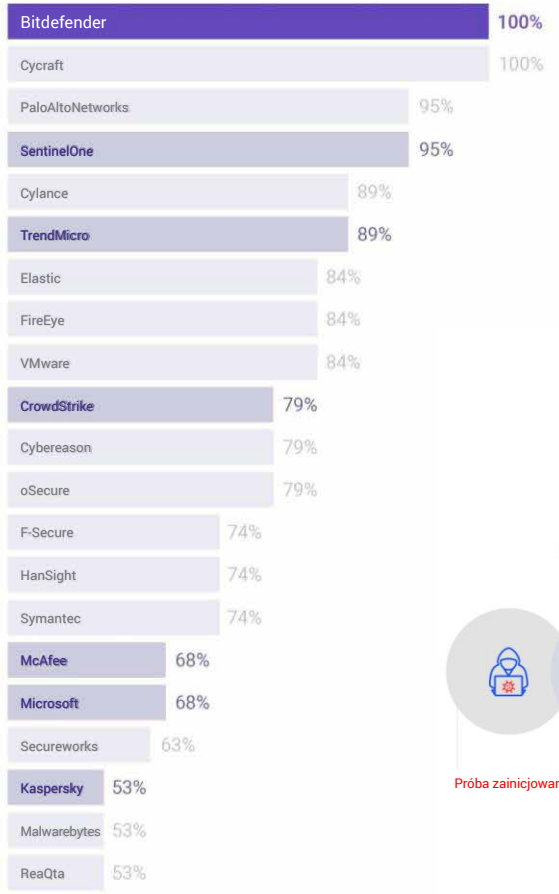
“Największy dostawca usług EDR, którego nie brałeś pod uwagę, choć powinieneś”

The Forrester Wave™ : Enterprise Detection and Response, 1. kwartał 2020 r.

https://businessinsights.bitdefender.com/forrester-names-bitdefender-the-biggest-edr-vendor-you-havent-considered-but-should-have-in-2020-wave-for-edr

Zabezpieczenie przed wszystkimi znanymi atakami w bazie MITRE ATT&CK

dla średnich firm i MSP



https://businessinsights.bitdefender.com/mitre-attack-evaluation-results

PRZEBIEG ATAKU

https://businessinsights.bitdefender.com/apt-mercenary-groups-pose-real-threat-to-companies-but-detecting-tactics-and-techniques-is-within-reach

PODSUMOWANIE

BITDEFENDER EDR - PODSUMOWANIE

“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
- Niwelowanie braków w umiejętnościach z zakresu cyberbezpieczeństwa
- Określenie ryzyka organizacyjnego
- Zmniejszenie obciążenia operacyjnego

PAKIETY EDR

OPCJE BITDEFENDER EDR

NAJWAŻNIEJSZE NAGRADZANE FUNKCJONALNOŚCI BITDEFENDER EDR	BITDEFENDER EDR	EPP + EDR GRAVITYZONE ULTRA	MANAGED DETECTION AND RESPONSE		
			MDR Core	MDR Advanced	MDR Enterprise
Anty - Malware	Tryb raportowania	X	X	X	X
Przeciwdziałanie i łagodzenie skutków malware	Tryb raportowania	X	X	X	X
Wsparcie systemów Windows, Mac i Linux	Tylko Windows	X	X	X	X
Ochrona środowisk fizycznych i wirtualnych	X	X	X	X	X
Lekki agent	X	X	X	X	X
Konsola zarządzania oparta na chmurze	X	X	X	X	X
Automatyczna naprawa		X	X	X	X
Kontrola aplikacji i urządzenia		X	X	X	X
Zapora sieciowa na hoście i Ochrona przed Atakiem Sieciowym		X	X	X	X
Analiza ryzyka dla urządzenia i aplikacji	X	X	X	X	X
Analiza przebiegu ataku	X	X	X	X	X
Pełne szyfrowanie dysku (dodatek)		X	X	X	X
Naprawa luk (dodatek)		X	X	X	X
Analiza ryzyka ludzkiego	X	X		X	X
Endpoint Detection and Response (EDR)	X	X	X	X	X
Network Traffic Security Analytics NTSA (dodatek)		X		X	X


Bitdefender®
WWW.BITDEFENDER.PL