

WYKRYWANIE ZAAWANSOWANYCH ZAGROŻEŃ,
PRECYZYJNA ANALIZA I SKUTECZNA OCHRONA

BITDEFENDER ENDPOINT DETECTION AND RESPONSE (EDR)

Bitdefender[®]

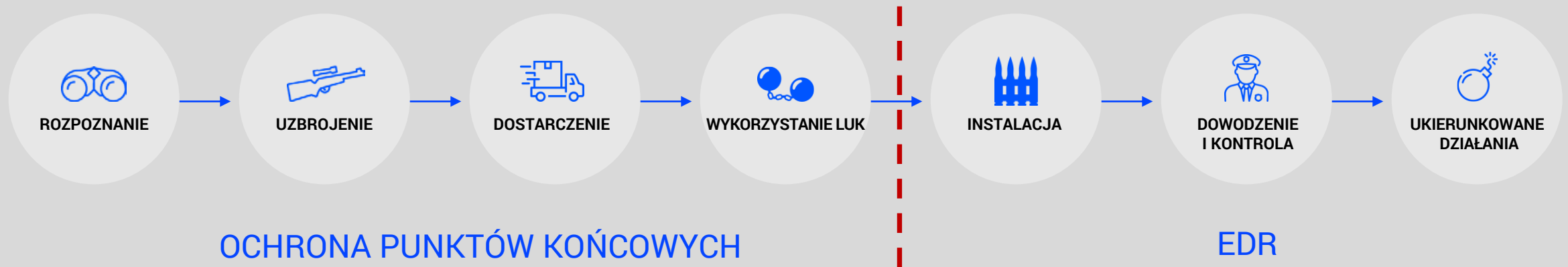
WWW.BITDEFENDER.PL

AGENDA

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

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

4

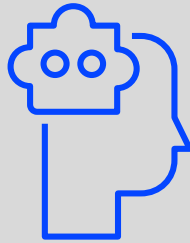
Bitdefender®

3 GRUDNIA 2020

JAKIE SĄ ZALETY ROZWIĄZANIA BITDEFENDER EDR?



ZAAWANSOWANE WYKRYWANIE
I REAGOWANIE NA ATAKI



NIWELOWANIE BRAKU WIEDZY
I UMIEJĘTNOŚCI Z ZAKRESU
CYBERBEZPIECZEŃSTWA



OKREŚLENIE RYZYKA
ORGANIZACYJNEGO



ZMNIJSZENIE 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

Endpoint Incidents

OPEN INCIDENTS

High	1
Medium	0
Low	15

TOP ALERTS

Network Connection Start	16
Process Create	16
HTTP Resource Downl...	15
URL.Malicious	12
Suspicious Process-Elevati...	8
File Write	6

TOP TECHNIQUES

Command-Line Interface	16
Spearphishing Link	12
Bypass User Account Con...	8

TOP AFFECTED DEVICES

TW-10RS6X64	9
WT-10RS6X64	7

Change Status

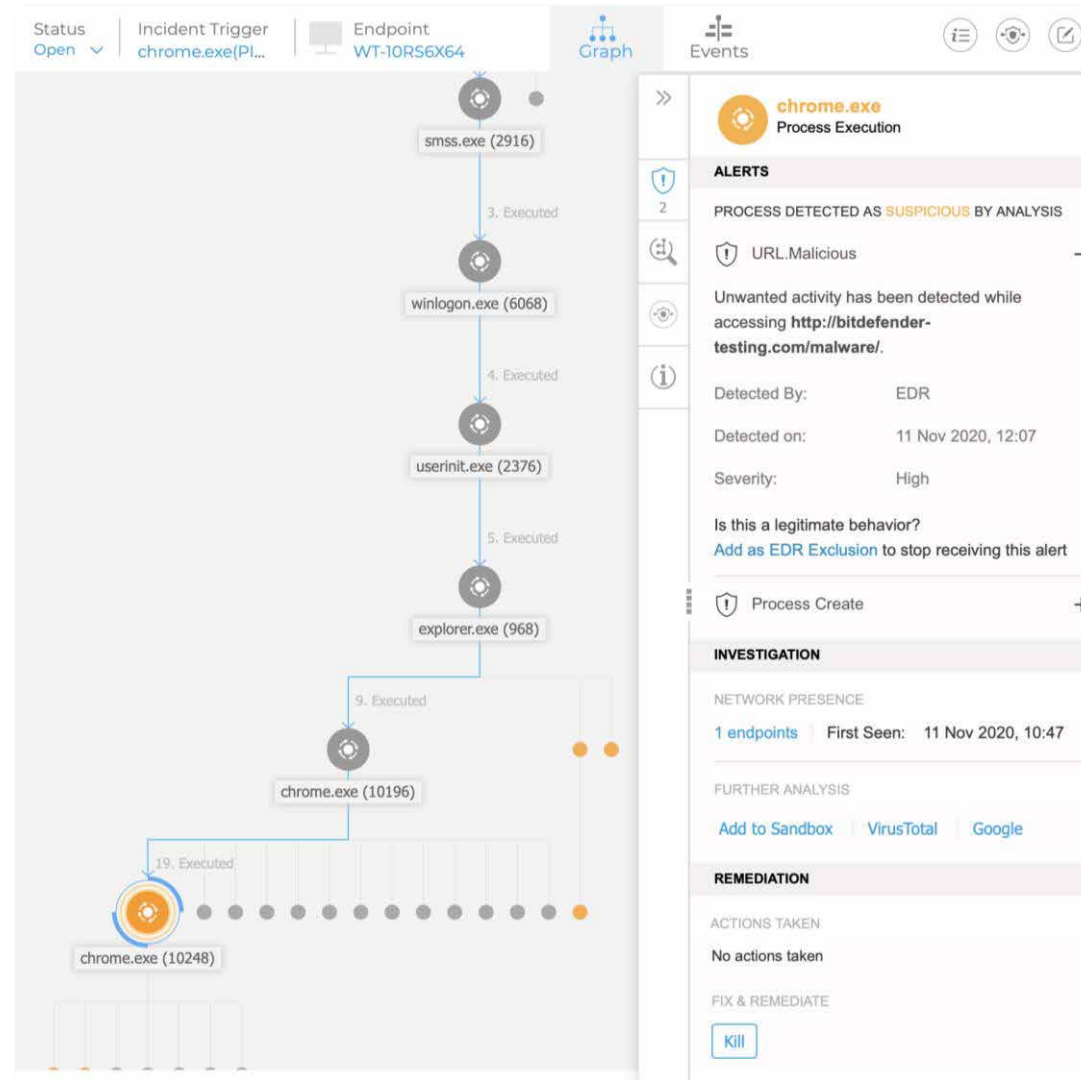
Alert name Search for filenames, IP addresses, hostnames ...

ID	Date	Status	Confidence Score	Endpoint	Alerts	Attack type
<input type="checkbox"/> Search...	Select...	Open, Investigating	100-30	Search...		Choose...
<input type="checkbox"/> #17	Updated at 13:06 on 11 Nov	Open	50	WT-10RS6X64	69	Malware
<input type="checkbox"/> #18	Created at 13:05 on 11 Nov	Open	50	WT-10RS6X64	16	Malware
<input type="checkbox"/> #15	Created at 12:08 on 11 Nov	Open	50	WT-10RS6X64	36	Malware



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

Risk Management Dashboards

User Monitoring

Allow GravityZone to track suspicious user activity. The system will notify you of any suspicious activity. To disable this feature, use the configuration button:

USER MONITORING

Company Risk Score



Lower the configuration score by addressing what needs to be remediated. [How is it calculated?](#)

Health i

Dynam
compar
CVEs d
enviro
already
in

Se

Risk Score Breakdown

Misconfigurations

100%



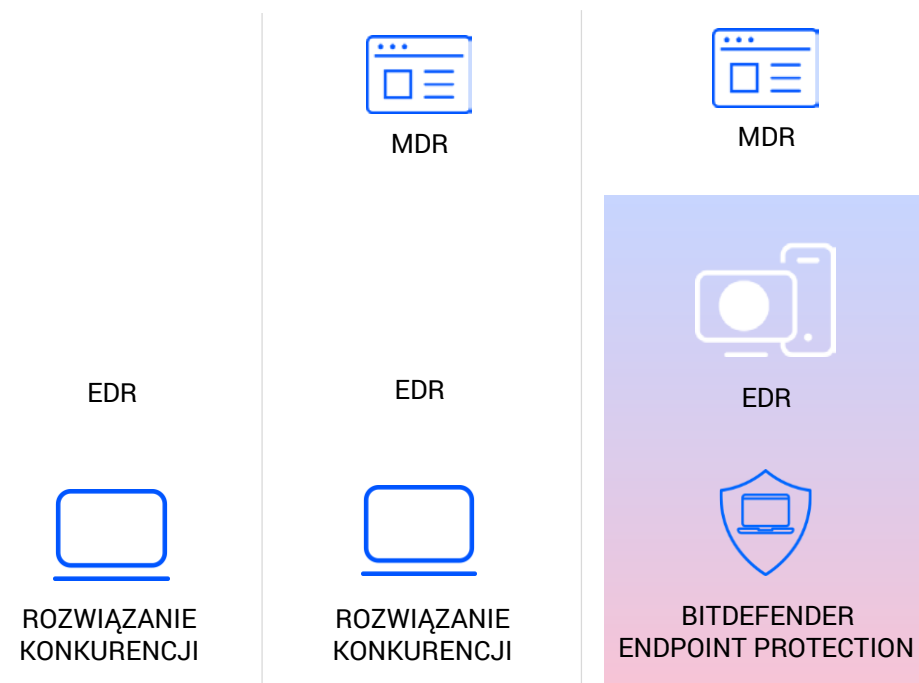
Bitdefender®

3 GRUDNIA 2020



ZMNIĘSZENIE OBCIĄŻENIA OPERACYJNEGO

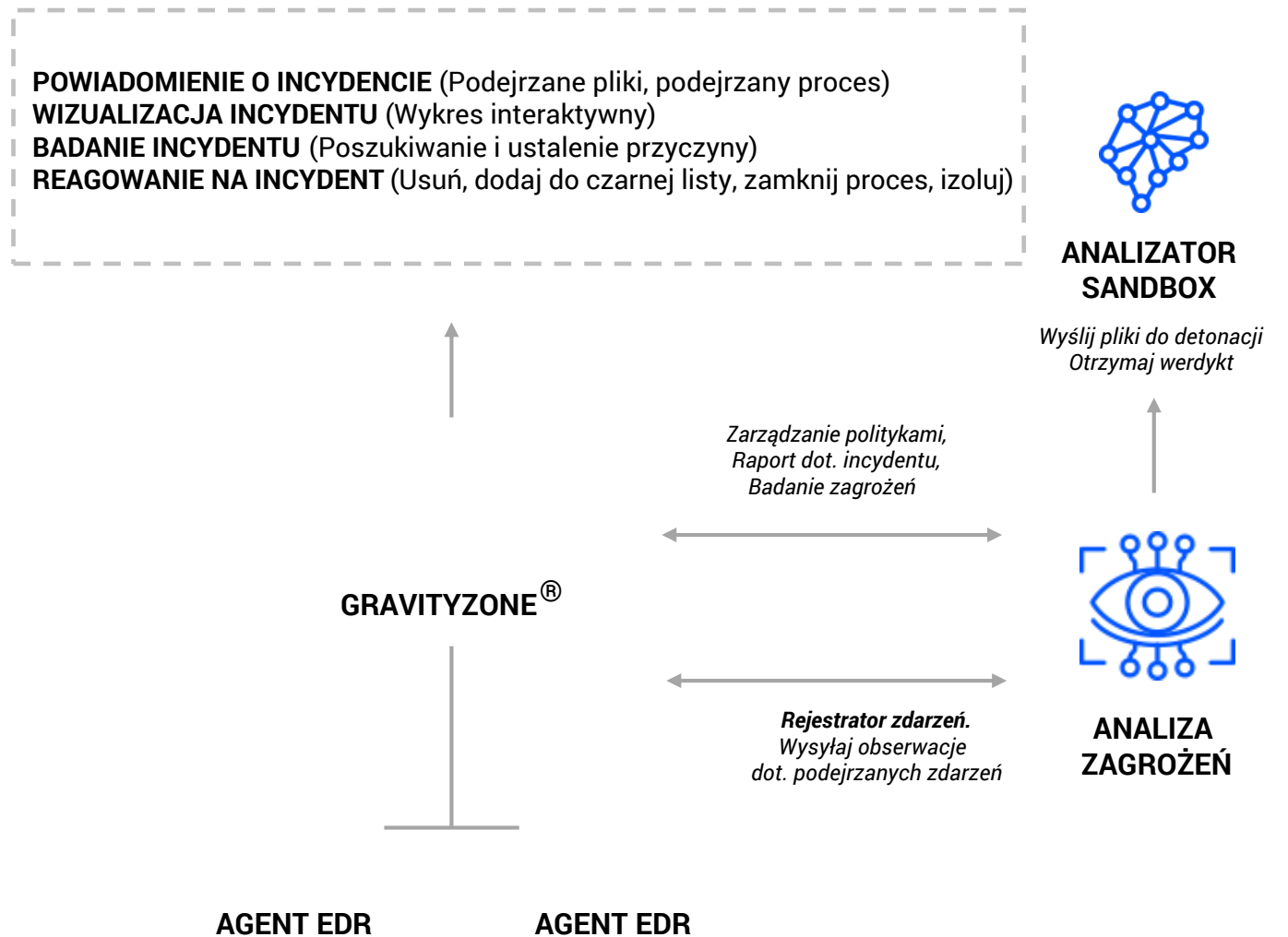
- Rozwiązanie chmurowe z niskimi kosztami utrzymania
- Proste wdrożenie
- Lekki agent
- Pełna kompatybilność z systemami antywirusowymi innych firm
- Elastyczność i możliwość rozbudowy



ELASTYCZNOŚĆ I MOŻLIWOŚĆ ROZBUDOWY

JAK TO DZIAŁA?

SPOSÓB DZIAŁANIA

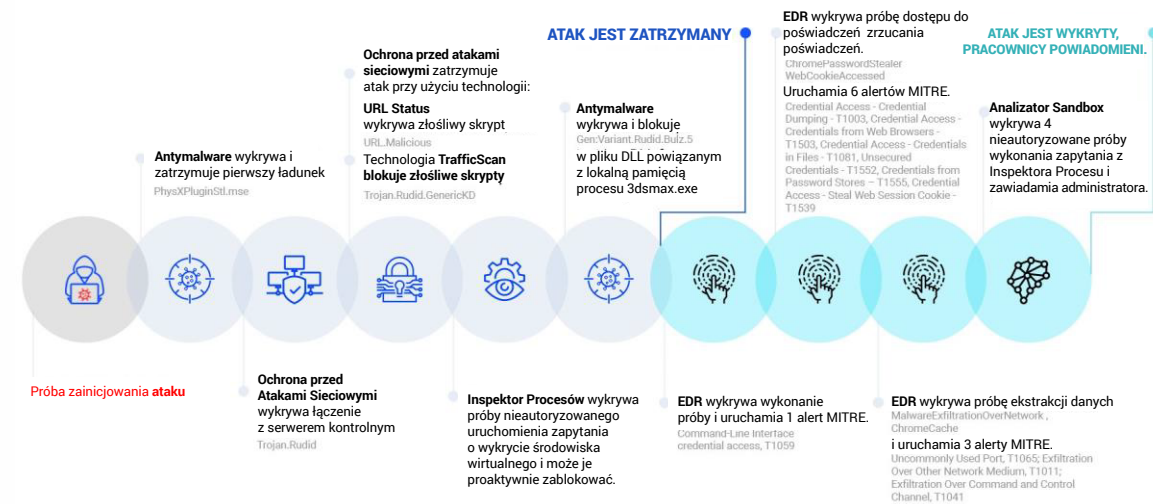


DLACZEGO BITDEFENDER EDR?

Zabezpieczenie przed wszystkimi znanymi atakami w bazie MITRE ATT&CK dla średnich firm i MSP



PRZEBIEG ATAKU



“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>

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

<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