bakotech®

W/TH® secure

Stop atakom **ukierunkowanym**

WithSecure™ Elements Endpoint Detection and Response

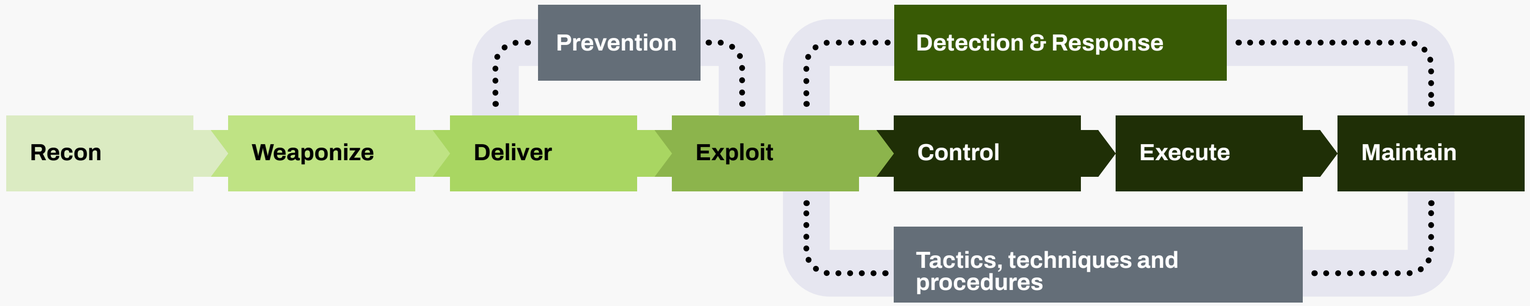
Chroń swój biznes i dane przed zaawansowanymi cyberatakami

Skuteczne zapobieganie zagrożeniom jest podstawą cyberbezpieczeństwa, ale aby zabezpieczyć firmę i jej dane przed taktykami, technikami i procedurami stosowanymi w atakach ukierunkowanych, potrzebne jest o wiele więcej.

Nieustannie ewoluujący krajobraz zagrożeń oraz wymogi regulacyjne, takie jak RODO, wymagają od firm przygotowania się na wykrywanie naruszeń po wystąpieniu sytuacji kryzysowej. Oznacza to, że firma musi być w stanie szybko reagować na zaawansowane ataki.

Rozwiązanie WithSecure Elements Endpoint Detection and Response, które zostało stworzone przez doświadczony zespół threat hunterów, umożliwia zespołowi IT lub certyfikowanemu dostawcy usług ochronę organizacji przed zaawansowanymi zagrożeniami.

Twoi specjaliści IT będą mogli szybko i skutecznie reagować na incydenty zezwalając usługodawcy na zarządzanie operacjami wykrywania i reagowania, dzięki czemu będziesz mógł skupić się na swojej podstawowej działalności i polegać na wskazówkach ekspertów w razie ataku.



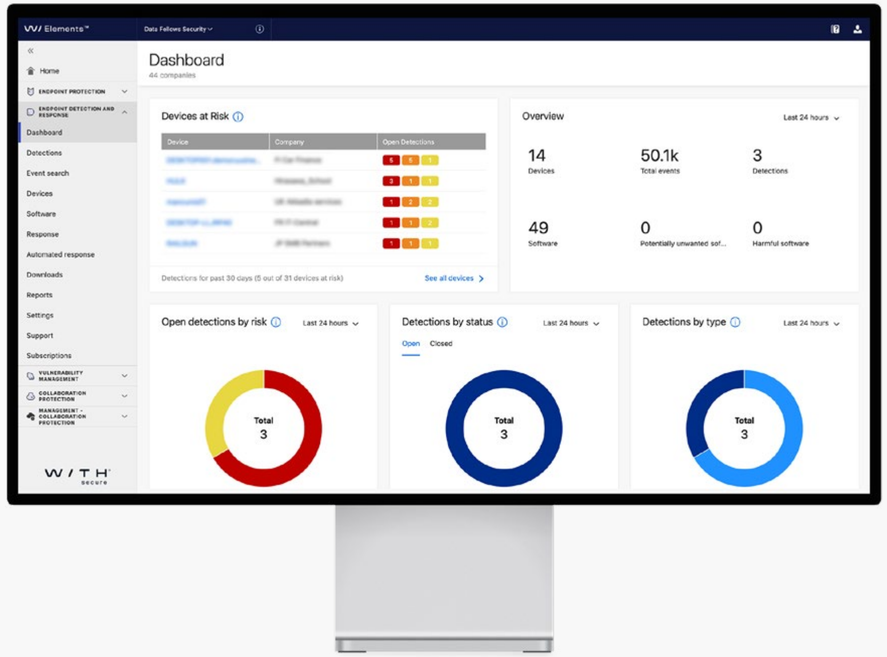
Przegląd rozwiązania

Szybkie powstrzymywanie ataków ukierunkowanych dzięki wskazówkom i automatyzacji

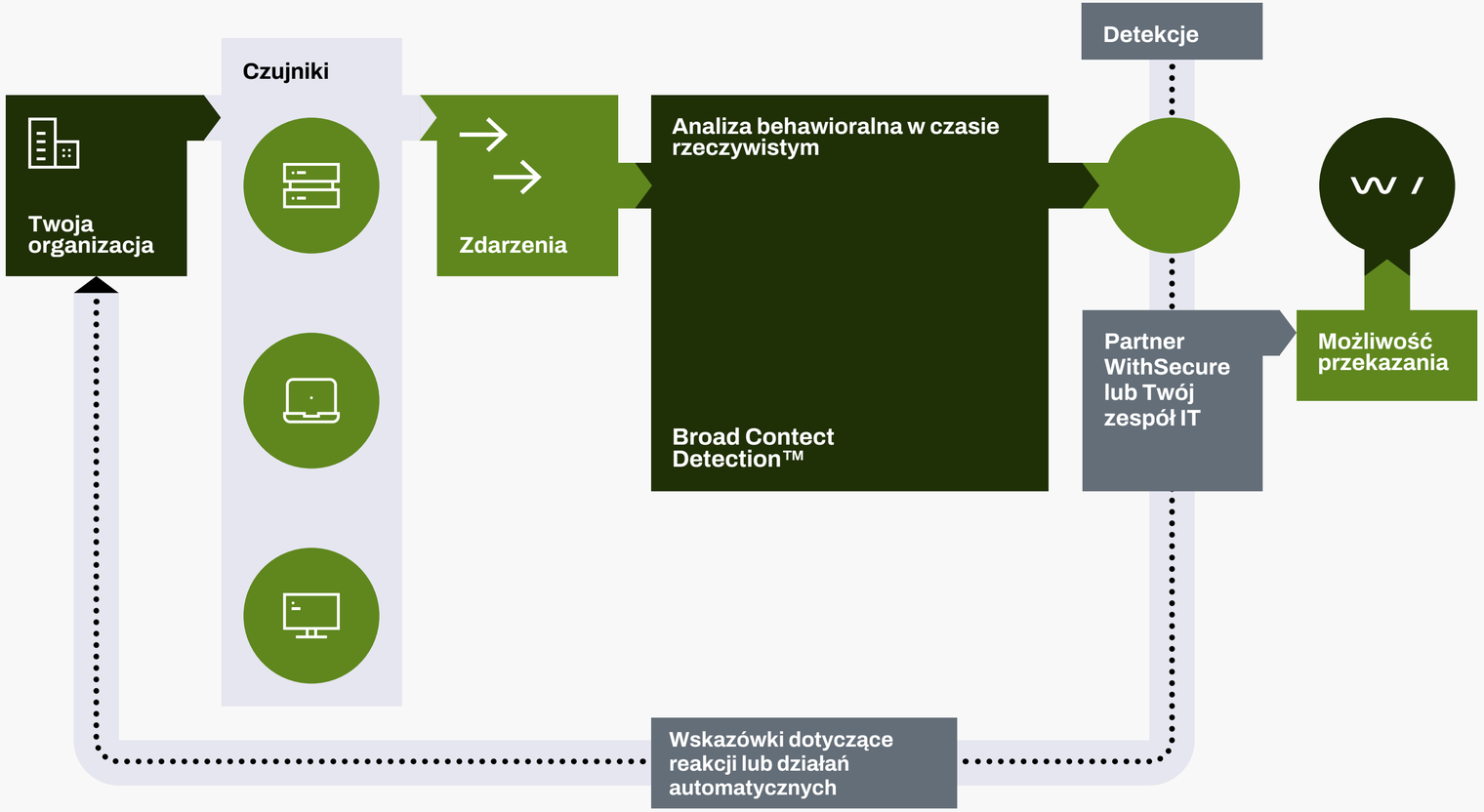
W jaki sposób wykryć nawet najbardziej wyszukany atak? Dzięki wykorzystaniu zaawansowanej analityki i technologii uczenia maszynowego, co umożliwia ochronę organizacji przed zaawansowanymi cyberzagrożeniami i naruszeniami.

Wiodące w branży rozwiązanie firmy WithSecure Elements Endpoint Detection and Response zapewnia kontekstowy wgląd w zaawansowane zagrożenia, umożliwiając wykrywanie ataków ukierunkowanych i reagowanie na nie za pomocą automatyzacji i wskazówek.

Kiedy dochodzi do naruszenia, potrzebujesz czegoś więcej niż tylko alertu.
Aby zaplanować najlepszą możliwą reakcję, należy zrozumieć specyfikę ataku.
Mechanizmy Broad Context Detection™, wraz z certyfikowanymi dostawcami usług i wbudowaną automatyzacją, szybko powstrzymają atak i dostarczą użytecznych wskazówek dotyczących dalszych działań naprawczych.



Jak to działa?



Wiodąca w branży technologia firmy WithSecure i eksperci ds. cyberbezpieczeństwa do Twoich usług

1. Lekkie czujniki rozmieszczone na punktach końcowych monitorują zdarzenia behawioralne generowane przez użytkowników i przesyłają je do analizy danych w czasie rzeczywistym oraz mechanizmów Broad Context Detection™ w celu odróżnienia wzorców złośliwego zachowania od normalnego zachowania użytkownika.
2. Alerty z oceną ryzyka i wizualizacją szerokiego kontekstu wszystkich dotkniętych hostów ułatwiają potwierdzenie wykrycia przez partnera firmy WithSecure lub własny zespół IT, z opcją przekazania trudnych dochodzeń do firmy WithSecure lub zautomatyzowania działań naprawczych.
3. Po potwierdzeniu wykrycia ataku rozwiązanie zapewnia porady i zalecane działania, które prowadzą użytkownika przez niezbędne kroki w celu szybkiego powstrzymania i zlikwidowania ataku.

Jak to działa?

Szukanie igły w stogu siana - przykład ze świata rzeczywistego

Wykrywanie zaawansowanych zagrożeń poprzez dostrzeganie drobnych, pojedynczych zdarzeń wywoływanych przez atakujących jest jak próba znalezienia igły w stogu siana.

W instalacji klienta, składającej się z 325 urządzeń, czujniki EDR zebrały około 500 milionów zdarzeń w ciągu jednego miesiąca. Analiza surowych danych w systemach back-end odfiltrowała tę liczbę do 225 000 zdarzeń.

Podejrzane zdarzenia były dalej analizowane przez mechanizmy Broad Context Detection™, aby zawęzić liczbę wykryć do zaledwie 24. Wreszcie, te 24 wykrycia zostały szczegółowo przeanalizowane, z czego tylko 7 zostało zostało potwierdzonych jako prawdziwe zagrożenia.

Kiedy zespoły IT mogą skupić się na mniejszej liczbie wykryć, mogą o wiele szybciej i skuteczniej reagować w przypadku rzeczywistego cyberataku - pozwól im na to!

500 milionów
zdarzeń dziennych / miesiąc zbierane przez 325 czujników punktów końcowych

225 000
zdarzeń dziennych / miesiąc
po analizie behawioralnej w czasie rzeczywistym

24
wykrycia po dodaniu szerszego kontekstu do podejrzanych zdarzeń

7
prawdziwych zagrożeń po potwierdzeniu, że wykryte zdarzenia są prawdziwymi zagrożeniami

Dlaczego warto?

Widoczność

Uzyskaj natychmiastowy wgląd w środowisko IT i stan zabezpieczeń

- Poprawia widoczność środowiska IT i stanu bezpieczeństwa poprzez inwentaryzację aplikacji i punktów końcowych
- Identyfikuje podejrzaną aktywność poprzez zbieranie i korelowanie zdarzeń behawioralnych, wykraczających poza zwykłe złośliwe oprogramowanie
- Dostarcza alerty z informacjami o szerokim kontekście i krytyczności zasobów, ułatwiając reagowanie na incydenty

Wykrywanie

Chroń swoją firmę i jej wrażliwe dane poprzez szybkie wykrywanie naruszeń

- Szybkie wykrywanie i powstrzymywanie ataków ukierunkowanych, aby zminimalizować przerwy w działalności i negatywny wpływ na markę
- Konfiguracja rozwiązania w ciągu kilku godzin, co pozwala na natychmiastową gotowość do reagowania na naruszenia
- Spełnienie wymogów regulacyjnych PCI, HIPAA i RODO, które wymagają zgłaszania naruszeń w ciągu 72 godzin

Odpowiedź

Szybka reakcja dzięki wskazówkom i automatyzacji w przypadku ataku

- Wbudowana automatyzacja i inteligencja pomagają Twojemu zespołowi skupić się tylko na prawdziwych atakach
- Alerty zawierają odpowiednie wskazówki dotyczące reakcji, z opcją automatyzacji działań przez całą dobę
- Pokonaj braki w umiejętnościach lub zasobach, odpowiadając na ataki za pomocą certyfikowanego dostawcy usług wspieranego przez firmę WithSecure

Co wyróżnia WithSecure EDR?

Sensory punktów końcowych

Lekkie, dyskretne narzędzia monitorujące zaprojektowane do pracy z dowolnym rozwiązaniem ochrony punktów końcowych

- Lekkie czujniki są wdrażane na wszystkich istotnych komputerach w organizacji
- Infrastruktura z jednym klientem i zarządzanie z rozwiązaniami firmy WithSecure zabezpieczającymi punkty końcowe
- Czujniki zbierają dane behawioralne z urządzeń punktów końcowych bez naruszania prywatności użytkowników

Ukierunkowana odpowiedź

Przygotowuje do radzenia sobie z nawet najbardziej zaawansowanymi cyberatakami przy użyciu istniejących zasobów

- Wbudowane wskazówki dotyczące reakcji krok po kroku i zdalne działania w celu powstrzymania ataków
- Certyfikowani service providerzy prowadzą i wspierają użytkownika w działaniach związanych z reagowaniem na ataki
- Unikalna analiza zagrożeń Elevate to WithSecure™ i usługa porad ekspertów zapewniają nieustanne wsparcie

Broad Context Detection™

Zastrzeżona technologia wykrywania firmy WithSecure ułatwia zrozumienie zakresu ataku ukierunkowanego

- Analiza behawioralna w czasie rzeczywistym, analiza reputacji i wykorzystanie uczenia maszynowego
- Automatyczne umieszczanie detekcji w kontekście wizualizowane na osi czasu
- Obejmuje poziomy ryzyka, krytyczność hosta oraz dominujący krajobraz zagrożeń

Zautomatyzowane reagowanie

Zmniejsz wpływ ukierunkowanych cyberataków dzięki automatyzacji działań przez całą dobę

- Zautomatyzowane działania w oparciu o krytyczności, poziomy ryzyka i predefiniowany harmonogram
- Poziomy krytyczności i ryzyka zapewniane przez rozwiązanie pozwalają na priorytetyzację działań reagowania
- Szybkie powstrzymywanie ataków, nawet jeśli Twój zespół jest dostępny tylko w określonych godzinach

Widoczność aplikacji

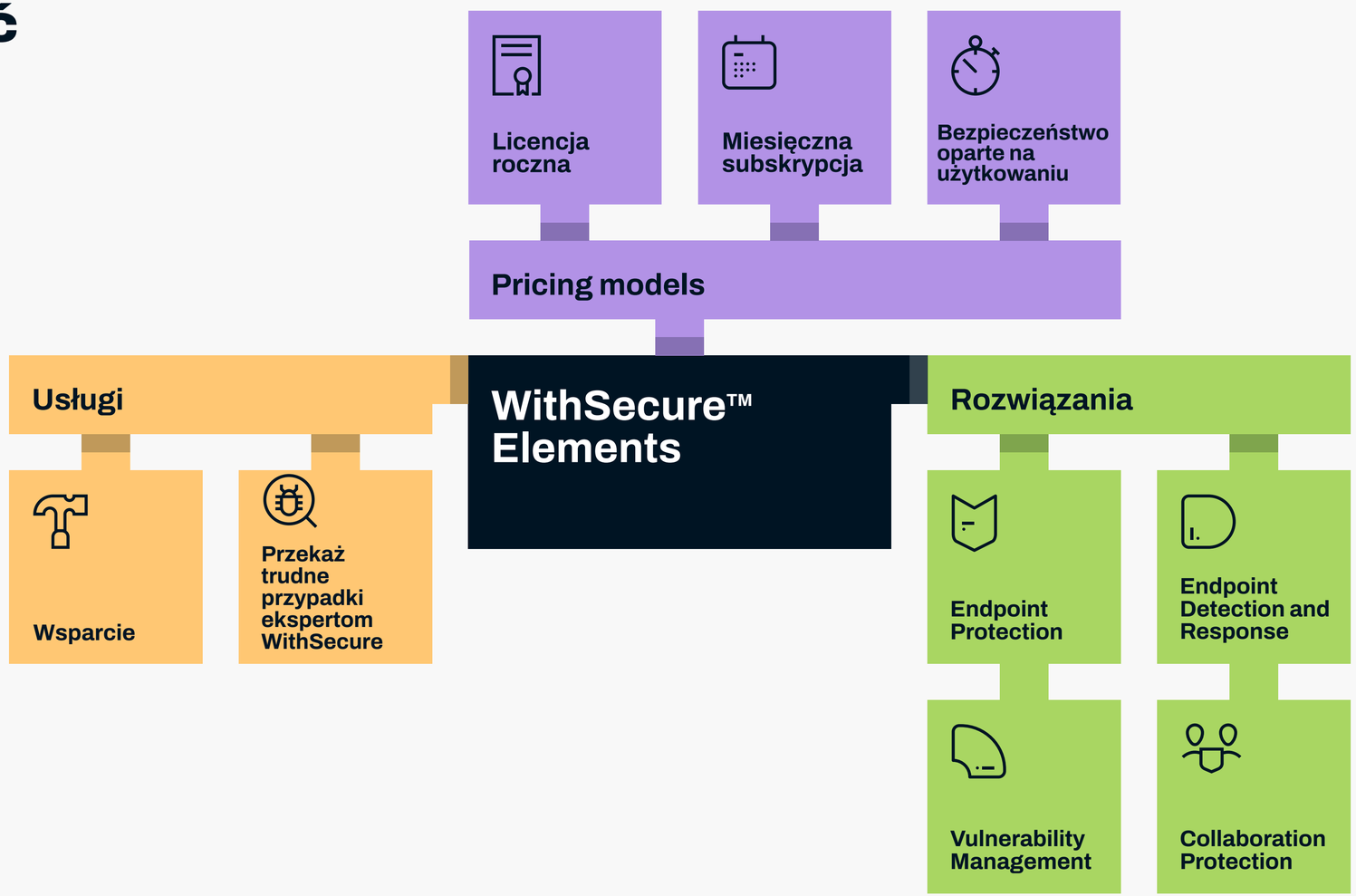
Uzyskanie wglądu w środowisko IT i stan zabezpieczeń nigdy nie było łatwiejsze

- Identyfikuje wszystkie szkodliwe lub niepożądane aplikacje oraz zagraniczne lokalizacje docelowe różnych usług w chmurze
- Wykorzystanie danych firmy WithSecure dotyczących reputacji w celu identyfikacji potencjalnie szkodliwych aplikacji
- Ograniczanie potencjalnie szkodliwych aplikacji i usług w chmurze jeszcze przed wystąpieniem naruszenia danych

WithSecure Elements: zmniejsz ryzyko, złożoność i nieefektywność

Rozwiązanie WithSecure Elements Endpoint Protection jest dostępne jako samodzielne rozwiązanie lub jako integralna funkcja w ramach modułowej platformy cyberbezpieczeństwa WithSecure Elements.

Sprawdź za darmo



Skontaktuj się z nami

Bakotech Sp. z o.o.

www.bakotech.pl
kontakt@bakotech.pl
12 340 90 30
ul. Drukarska 18/5 30-348 Kraków