kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Optimum Security

Osiągnij optymalny poziom cyberbezpieczeństwa dzięki ochronie zarządzanej, opartej na chmurze ochronie punktów końcowych i możliwościom reagowania

Wyzwanie

Musisz być w stanie skutecznie ochronić swoją firmę przed nowymi, nieznanymi i unikającymi wykrycia zagrożeniami, bez nadmiernego poświęcania swojego czasu i zasobów.

W 30% skutecznych cyberataków wykorzystane zostały legalne narzędzia systemowe[1]

Liczba zaawansowanych ataków rośnie

Obecnie zagrożenia starają się unikać wykrycia poprzez omijanie tradycyjnej ochrony punktów końcowych, przez co stwarzają znacznie większe zagrożenie dla firm niż wcześniej. Trudniej jest więc wykryć atak, przeprowadzić analizę i podjąć działania w ramach reakcji. Jeśli niewykryte zagrożenie zdoła przedostać się do infrastruktury, może:

- zakłócić najważniejsze procesy biznesowe,
- doprowadzić do uszczerbku na reputacji i utraty klientów,
- skutkować otrzymaniem kar, grzywien i utratą zysków.

Ochrona punktów końcowych musi zostać wzmocniona

Unikające wykrycia ataki są bardzo skuteczne, ponieważ przestępcy wykorzystują w nich legalne narzędzia systemowe oraz inne gotowe metody i technologie, dzięki którym szybciej mogą zdobyć dostęp do infrastruktury, uniknąć rozpoznania i wykonywać szkodliwe działania.

Sytuację tę dodatkowo pogarsza rozmycie obwodu IT w firmie i coraz większa skala pracy zdalnej — punkty końcowe są tradycyjnie najatrakcyjniejszym punktem wejścia do infrastruktury.

Zasoby są na granicy wyczerpania

Aby zapewnić dodatkowe korzyści ochronie punktów końcowych, organizacja musi we własnym zakresie rozwijać swoje możliwości reagowania na incydenty.

Jednak koszty takich projektów mogą szybko wymknąć się spod kontroli:

- koszty związane z oprogramowaniem i sprzętem rosną,
- autonomiczne i pofragmentowane narzędzia zabezpieczające oraz procesy zmniejszają skuteczność ochrony,
- rutynowe zadania pochłaniają zbyt dużo czasu.

Rozwiązanie

Kaspersky Optimum Security to: skuteczne wykrywanie zagrożeń oraz reagowanie na nie, rozwiązanie wspierane całodobowym monitorowaniem stanu bezpieczeństwa, zautomatyzowana reakcja i polowanie na zagrożenia, jak również pomoc techniczna i porady ekspertów z firmy Kaspersky.

45% ataków zostało wykrytych na podstawie obecności podejrzanych plików lub podejrzanej aktywności na punktach końcowych[1]

Zaawansowana ochrona przed zagrożeniami

Osiągnij optymalną równowagę między prostotą i skutecznością, inteligencją człowieka i automatyzacją, wydajnością i funkcjonalnością — nie ryzykując obniżeniem poziomu ochrony.

Kaspersky Optimum Security pomaga zmniejszyć ryzyko utraty pieniędzy, klientów i reputacji, a także wzmacnia ochronę przed nowymi, nieznanymi i unikającymi wykrycia zagrożeniami. Dzięki niemu możesz stawić czoła szybko ewoluującemu krajobrazowi zagrożeń.

Szybkie i skalowalne gotowe rozwiązanie

Automatyczna ochrona to podstawa bezpieczeństwa każdego punktu końcowego, ale muszą ją uzupełniać zaawansowane narzędzia odpierające nawet najniebezpieczniejsze zagrożenia, które starają się unikać wykrycia.

Kaspersky Optimum Security zapewnia zaawansowane wykrywanie i możliwości szybkiego reagowania — a wszystko z poziomu chmury. Osoby odpowiedzialne za cyberbezpieczeństwo będą teraz w stanie poradzić sobie z takimi zagrożeniami, które zwykle działają w ukryciu, szybko i precyzyjnie.

Optymalny poziom inwestycji

Nie musisz zatrudniać więcej osób, przeprowadzać szkoleń ani zajmować się skomplikowanym wdrożeniem — Kaspersky Optimum Security upraszcza i pomaga zautomatyzować najważniejsze procesy reagowania na incydenty, zgodnie z Twoimi konkretnymi wymogami.

Rozwiązanie dostosowuje się do potrzeb dzięki opcji lokalnej i chmurowej, a także dzięki skalowalnemu, gotowemu do użycia zestawowi narzędzi bezpieczeństwa. W ten sposób pomaga ograniczyć złożoność systemu IT, utrzymać produktywność użytkowników oraz zapewnia transparentne koszty wdrożenia.

Kluczowe korzyści

- Przygotuj się na destrukcyjne i unikające wykrycia ataki i już dziś zabezpiecz swoją firmę przed poważnymi zagrożeniami w postaci szkód i przestojów w działaniu organizacji
- Opracuj własną drogę reagowania w przypadku wystąpienia incydentu z prostym w użytkowaniu zestawem narzędzi Endpoint Detection and Response (EDR)
- Znacząco obniż ryzyko infekcji poprzez edukację pracowników oraz zwiększ ich świadomość w kwestii zagrożeń
- Ochroń cenne zasoby poprzez automatyzację działań i funkcje zarządzane
- Oszczędź czas i nakład pracy dzięki rozwiązaniu, którym możesz zarządzać w chmurze lub poprzez konsolę lokalną

Najważniejsze możliwości

55% ataków trwało co najmniej kilka tygodni, zanim zostały wykryte[1]

Kaspersky Optimum Security oferuje szeroki wachlarz najważniejszych funkcji służących do ochrony przed unikającymi wykrycia zagrożeniami, a do jego najważniejszych możliwości należy wykrywanie, analizowanie i reagowanie.

Zaawansowane wykrywanie

- Oparte na uczeniu maszynowym algorytmy analizujące zachowanie pozwalają szybko i dokładnie ujawnić podejrzane działania
- Zautomatyzowane polowanie na zagrożenia, oparte na naszych autorskich wskaźnikach ataków, pozwala ujawnić złożone i działające w ukryciu zagrożenia, przy wsparciu ze strony ekspertów z firmy Kaspersky
- Adaptacyjna kontrola anomalii automatycznie dostosowuje konfigurację narzędzi, co zmniejsza powierzchnię ataku na profilach użytkowników

Uproszczone analizowanie

- Wszystkie informacje związane z incydentem są gromadzone automatycznie w jednym miejscu
- Zwizualizowany i uproszczony proces analizy umożliwia szybki i skuteczny wgląd w incydent w pojedynczym środowisku oraz podjęcie decyzji odnośnie dalszych działań
- Wszystkie zdarzenia związane z aktywnością wskaźników ataku otrzymują odpowiedni priorytet i są analizowane przez firmę Kaspersky, która udziela stosownych zaleceń

Automatyczne reagowanie

- Reakcja za pomocą jednego kliknięcia umożliwia szybkie powstrzymanie konkretnego incydentu
- Oparte na doświadczeniu ekspertów z firmy Kaspersky wskazówki dotyczące podjęcia reakcji pozwalają radzić sobie z nawet najbardziej złożonymi i niebezpiecznymi zagrożeniami
- Zautomatyzowana reakcja na wielu punktach końcowych pomaga w zidentyfikowaniu zagrożeń w sieci i zareagowaniu na nie

Jak przebiega wdrożenie

Rozwiązanie Kaspersky Optimum Security zawiera liczne narzędzia i kluczowe możliwości, które skutecznie zapobiegają zagrożeniom, wykrywają je i stosują odpowiednie działania w ramach reakcji na różnych etapach ataku:

Przeniknięcie

Użytkownik otrzymuje phishingową wiadomość e-mail lub uzyskuje dostęp do szkodliwego zasobu sieciowego, infekując swoje urządzenie

Instalacja

Infekcja wstępna umieszcza niezbędne komponenty, komunikuje się z serwerem kontroli[1] i bada otoczenie

Uzyskiwanie dostępu na poziomie administratora

Wiele narzędzi, także tych legalnych i wbudowanych w system, jest wykorzystywanych do przetrwania zagrożenia i umożliwienia mu poruszania się w sieci

Świadomość kwestii bezpieczeństwa u pracowników

Zmniejszenie powierzchni ataku

Automatyczne polowanie na zagrożenia

Zaawansowane mechanizmy wykrywania, w tym oparta na uczeniu maszynowym analiza zachowania i piaskownica

Automatyczne polowanie na zagrożenia wykorzystujące wskaźniki ataku[2]

Analiza podstawowych przyczyn ataku i skanowanie w poszukiwaniu oznak włamania[3]

Zautomatyzowane, wspierane wskazówkami, zdalne scenariusze reakcji

[1] Serwer kontroli
[2] Wskaźniki ataku
[3] Oznaki włamania

Ochrona, która sięga dalej

Możesz zwiększyć swoją ochronę, stosując liczne narzędzia dostosowane do różnych aspektów Twojego bezpieczeństwa — wykrywania, analizy i świadomości.

Szkodliwe e-maile stanowiły element 31% skutecznych cyberataków, co oznacza, że wielu z nich mogli zapobiec sami pracownicy[1]

Dodatkowa warstwa wykrywania

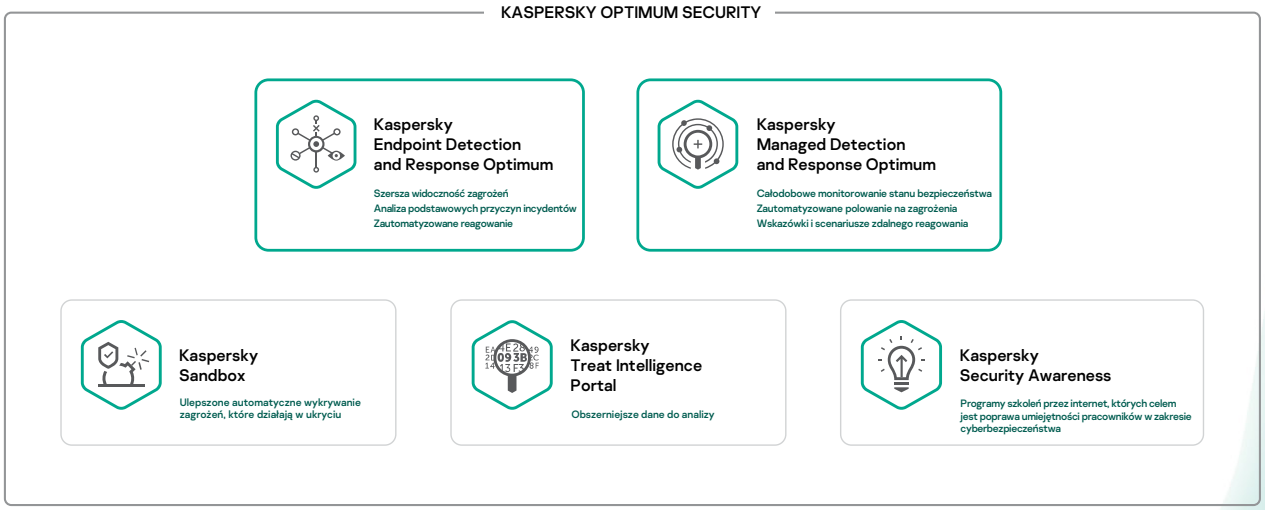
Ujawniaj nowe i nieznane zagrożenia jeszcze szybciej i wiarygodniej dzięki rozwiązaniu **Kaspersky Sandbox**, które pozwala analizować zagrożenia automatycznie w środowisku izolowanym, za pomocą opatentowanych algorytmów wykrywania i technik zapobiegających zdemaskowaniu. Ustalona reakcja jest stosowana automatycznie wobec wykrytego zagrożenia, co znacząco zwiększa możliwości ochrony, a przy tym wymaga zaledwie początkowego wdrożenia.

Więcej informacji do analizy

Pomóż swoim specjalistom ds. cyberbezpieczeństwa przeanalizować i zrozumieć zagrożenia szybciej i dokładniej dzięki najnowszym informacjom na temat plików, skrótów (hash), a także adresów IP i URL powiązanych z zagrożeniami. Zapewnij sobie szerszy obraz sytuacji bez dodatkowych kosztów dzięki łatwemu w użytkowaniu rozwiązaniu **Kaspersky Threat Intelligence Portal**.

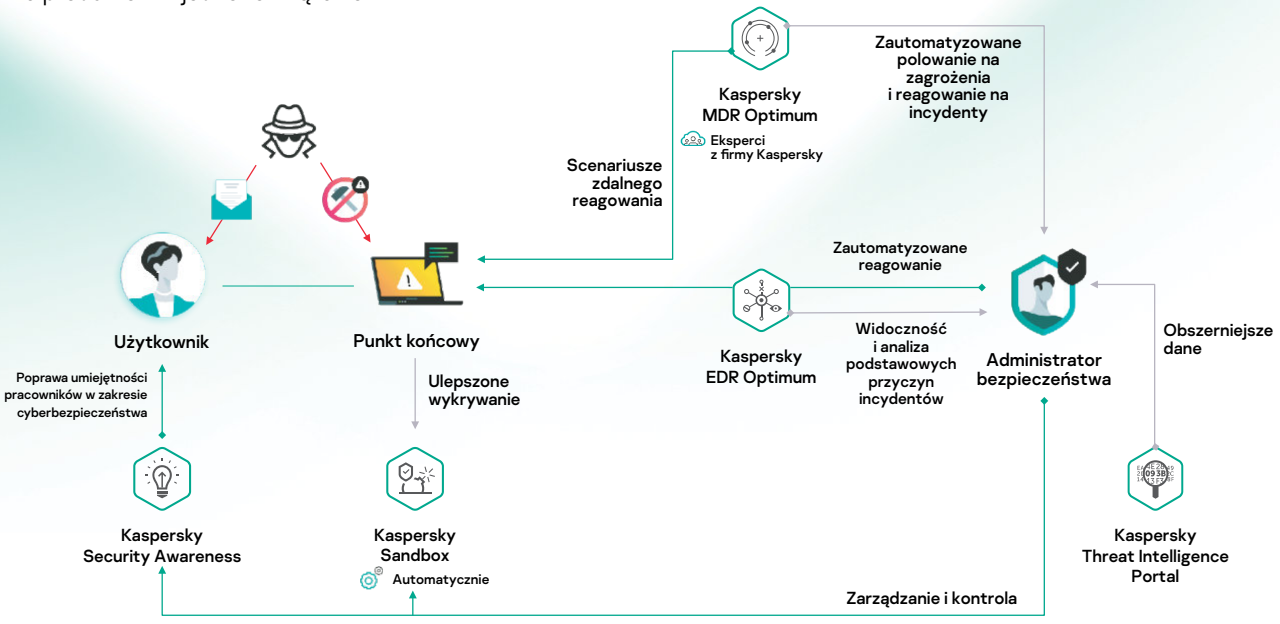
Ludzie są kluczowym elementem ochrony

W zmniejszaniu powierzchni ataku oraz liczby incydentów najważniejsze znaczenie ma edukacja pracowników w kwestii cyberzagrożeń, które mogą wpuścić do infrastruktury firmy poprzez zaniedbanie lub brak wiedzy. **Kaspersky Security Awareness** uczy i pozwala nabyć umiejętności, jakich potrzebują wszyscy pracownicy, aby uczestniczyć w ochronie infrastruktury.



Jak to działa

Możesz wybrać, w jaki sposób chcesz używać Kaspersky Optimum Security — jako rozwiązanie zarządzane zapewniające całodobową ochronę, jako łatwy w użytkowaniu zestaw narzędzi EDR czy jako połączenie obu możliwości, które zapewnia doświadczenie i wiedzę ekspertów z firmy Kaspersky, a także umożliwia rozwijanie własnych możliwości wykrywania i reagowania. Kaspersky Optimum Security łączy kilka produktów w jedno rozwiązanie:



W działaniu

Kaspersky Optimum Security jest łatwy w zarządzaniu poprzez pojedynczą konsolę, dzięki czemu pozwala zaoszczędzić sporo czasu i zasobów.

56% ankietowanych twierdzi, że ich organizacja jest narażona na zagrożenia ze względu na niewystarczającą liczbę personelu ds. cyberbezpieczeństwa[2]

Pełny pakiet

- Część ekosystemu ochrony firmy Kaspersky, który buduje bezpieczeństwo — od funkcji podstawowych po te zoptymalizowane i zaawansowane
- Do zarządzania funkcjami Kaspersky Optimum Security służy pojedyncza konsola w chmurze
- Rozwiązanie zapewnia wiele warstw ochrony, które chronią przed zagrożeniami unikającymi wykrycia, jak również przed możliwościami popełnienia błędu przez człowieka

Łatwość zarządzania

- Chmurowa konsola do zarządzania zapewnia szybką i skuteczną kontrolę z dowolnego miejsca na świecie
- Zarówno lokalna, jak i chmurowa wersja konsoli zapewnia administratorowi takie same możliwości i łatwość obsługi
- Wdrożenie przebiega szybko i bezproblemowo, przy czym nie ma znaczenia, czy użytkownik zna już produkty marki Kaspersky
- Wszystkie narzędzia są kontrolowane i zarządzane w sposób łatwy i intuicyjny, a także nie wymagają długiego zaznajamiania się ani przekwalifikowania

Oszczędzaj czas i zasoby

- Ochrona zarządzana pomaga organizacjom, które nie mają wystarczającej liczby personelu ds. bezpieczeństwa IT lub doświadczenia, w zbudowaniu ochrony i reagowania na zagrożenia bez konieczności inwestowania w ochronę
- Najważniejsze procesy cyberbezpieczeństwa są zautomatyzowane, dzięki czemu reagowanie na incydent przebiega szybciej, dokładniej i skuteczniej
- Lepsza świadomość kwestii bezpieczeństwa u pracowników oznacza, że organizacja będzie w mniejszym stopniu narażona na zagrożenia — a więc będzie mniej incydentów, którymi trzeba się zająć.

Podejście etapowe firmy Kaspersky

Razem możemy zbudować bezpieczeństwo Twojej firmy w oparciu o niezawodną ochronę, jaką zapewnia Kaspersky Security Foundations. Dzięki Kaspersky Optimum Security reakcje na incydenty są płynnie dostosowywane, a zaawansowane narzędzia i doświadczenie ekspertów z firmy Kaspersky zapewnią ochronę przed nawet najbardziej zaawansowanymi zagrożeniami.

Wybierz najbardziej odpowiedni etap Twojej organizacji:

Kaspersky Security Foundations

Automatyczne blokowanie zdecydowanej większości zagrożeń

- Wielowektorowe i zautomatyzowane zapobieganie incydentom wywołanym przez zdecydowaną większość wszystkich cyberataków
- Etap podstawowy dla organizacji dowolnej wielkości i z dowolnym stopniem złożoności w budowaniu zintegrowanej strategii ochronnej
- Niezawodna ochrona punktów końcowych dla firm dysponujących niewielkimi zespołami ds. IT oraz wiedzą w zakresie bezpieczeństwa

Kaspersky Optimum Security

Budowanie ochrony przed unikającymi wykrycia zagrożeniami dla firm, które:

- Dysponują niewielkimi zespołami ds. IT oraz podstawową wiedzą w zakresie bezpieczeństwa
- Mają środowisko IT, które rośnie i staje się coraz bardziej złożone, co zwiększa powierzchnię ataku
- Doświadczają braku zasobów w obszarze cyberbezpieczeństwa przy dużych potrzebach związanych z ochroną
- Coraz bardziej potrzebują rozwijać możliwości reagowania na incydent

Kaspersky Expert Security

Przygotowanie na ataki złożone i długotrwałe, w których:

- Środowiska IT są złożone i rozproszone
- Zespół ds. bezpieczeństwa IT ma doświadczenie lub istnieje centrum operacji bezpieczeństwa (SOC)
- Koszty incydentów bezpieczeństwa i wycieku danych mogą być wysokie
- Zgodność z wymogami prawnymi jest wyzwaniem

Aby dowiedzieć się więcej na temat tego, w jaki sposób rozwiązanie Kaspersky Optimum Security chroni przed zagrożeniami, odwiedź stronę: http://go.kaspersky.com/optimum.

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Informacje o cyberzagrożeniach: securelist.pl
Informacje ze świata bezpieczeństwa IT: kaspersky.pl/blog

www.kaspersky.pl