Kaspersky dla korporacji

O ofercie firmy Kaspersky dla korporacji

Stworzenie fundamentu bezpieczeństwa dla własnej organizacji poprzez wybranie odpowiedniego produktu i usługi stanowi pierwszy krok. Jednak kluczem do długotrwałego sukcesu jest opracowanie perspektywicznej strategii cyberbezpieczeństwa korporacyjnego.

Oferta firmy Kaspersky dla korporacji odzwierciedla zapotrzebowanie na bezpieczeństwo wśród dzisiejszych firm, wychodząc naprzeciw potrzebom organizacji na różnym poziomie dojrzałości przy zastosowaniu podejścia krok po kroku. Podejście to łączy różne poziomy ochrony przed wszystkimi rodzajami cyberzagrożeń, zapewniając wykrywanie najbardziej złożonych ataków, szybką i odpowiednią reakcję na każdy incydent oraz zapobieganie przyszłym zagrożeniom.

Rola ochrony punktów końcowych w długoterminowym planowaniu

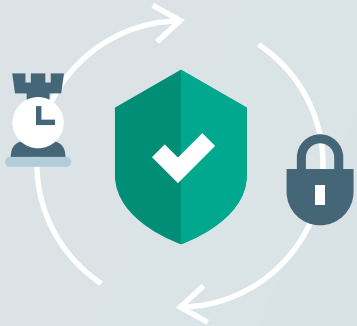
Tradycyjny proces ewolucji bezpieczeństwa

Podejmowanie decyzji:

- Trendy rynkowe
- Odizolowane rozwiązanie bezpieczeństwa
- Podejście oparte na „gaszeniu pożarów"
- Motywowanie zgodnością z przepisami

Stosowanie tradycyjnych produktów:

- Platforma ochrony punktów końcowych (EPP)
- Zapory sieciowe / Zapory sieciowe nowej generacji
- Zapory aplikacji WWW
- Zapobieganie utracie danych
- SIEM (zarządzanie informacjami i zdarzeniami zabezpieczeń)

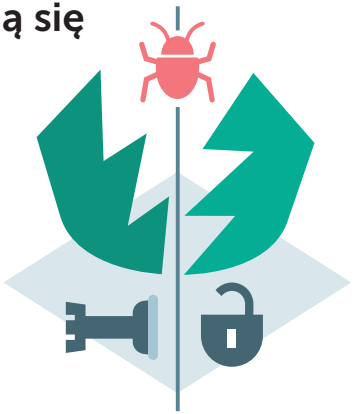


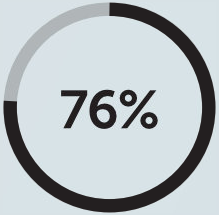
Atrybuty

- Krótkoterminowe planowanie bezpieczeństwa
- Opieranie się na technologiach i funkcjach
- Ochrona sieci oparta na obrzeżach

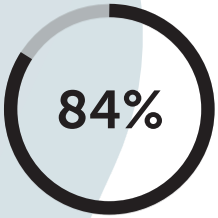
Dlaczego tradycyjne podejścia nie sprawdzają się

- Rosnąca złożoność zagrożeń i krajobrazu cyberprzestępczego
- Złożoność technologii cyberbezpieczeństwa
- Wymagania firm dotyczące długotrwałej strategii cyberbezpieczeństwa





wszystkich alertów jest generowanych przez punkty końcowe



wszystkich incydentów naruszenia bezpieczeństwa punktów końcowych dotyczy więcej niż jednego punktu końcowego

Punkty końcowe stanowią najczęstszą „bramę", przez którą cyberzagrożenia przedostają się do infrastruktury organizacji, główny cel ataków cyberprzestępców oraz kluczowe źródła danych niezbędnych do skutecznego badania złożonych incydentów.

3 kroki w kierunku zapewnienia zaawansowanego planowania w zakresie cyberbezpieczeństwa dla korporacji

2

Zaawansowane zagrożenia i ataki ukierunkowane

Zaawansowana obrona

Koncentruje się na zaawansowanym wykrywaniu i szybkiej reakcji na złożone zagrożenia pominięte przez ochronę prewencyjną.

Punkty końcowe

Kaspersky Endpoint Detection and Response

Usługi

Kaspersky Targeted Attack Discovery Service

1

Szerszy krajobraz zagrożeń

Fundamenty bezpieczeństwa

Wzmocnienie bezpieczeństwa systemów i automatyczne blokowanie możliwie największej liczby zagrożeń.

Punkty końcowe

Kaspersky Endpoint Security for Business

Kaspersky Embedded Systems Security

Sieć

Kaspersky Security for Mail Server

Kaspersky Security for Internet Gateway

3

Kampanie ukierunkowane i cyberbronie

Zintegrowane podejście do cyberbezpieczeństwa

Gotowość na ataki APT. Wysoki poziom wiedzy eksperckiej, zaawansowane możliwości analizy zagrożeń oraz nieustanne wyszukiwanie nowych zagrożeń.

Kaspersky Threat Management & Defense

Sieć

Kaspersky Anti Targeted Attack

Analiza

Kaspersky Threat Intelligence

Ludzie

Kaspersky Cybersecurity Training

Prywatność

Kaspersky Private Security Network

Chmura

Kaspersky Hybrid Cloud Security

Wsparcie

Kaspersky Premium Support and Professional Services

Dane

Kaspersky Security for Storage

Ludzie

Kaspersky Security Awareness

4 korzyści dla firm wynikające z takiego podejścia

Tworzy podstawę rozwoju długotrwałej strategii cyberbezpieczeństwa biorąc pod uwagę specyfikę firmy oraz trendy w krajobrazie zagrożeń.

Zoptymalizowana inwestycja w technologię bezpieczeństwa i zmniejszony całkowity koszt posiadania.

Mniejsze szkody finansowe i operacyjne na skutek cyberprzestępczości.

ROI

Wyższy zwrot z inwestycji dzięki płynnej automatyzacji przepływu pracy oraz braku zakłóceń procesów biznesowych.

1 Fundamenty bezpieczeństwa

Zautomatyzowane technologie prewencyjne oraz świadomość w zakresie bezpieczeństwa

Blokowanie możliwie największej liczby zagrożeń

Podejście idealne dla małych przedsiębiorstw, które nie zatrudniają wyspecjalizowanego zespołu ds. bezpieczeństwa lub posiadają bardzo ograniczoną wiedzę w zakresie cyberbezpieczeństwa

- Wielowektorowe zautomatyzowane zapobieganie dużej liczbie potencjalnych incydentów spowodowanych przez masowe zagrożenia
- Podstawowy krok dla średnich i dużych przedsiębiorstw w zakresie tworzenia zintegrowanej strategii obrony przed złożonymi zagrożeniami

Punkty końcowe

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Chmura

- **Kaspersky Hybrid Cloud Security**

Sieć

- **Kaspersky Secure Mail Gateway**
- **Kaspersky Security for Internet Gateway**

Ludzie

- **Kaspersky Security Awareness**

Dane

- **Kaspersky Security for Storage**

Wsparcie

- **Kaspersky Premium Support**
- **Kaspersky Professional Services**

Kaspersky Endpoint Security for Business

Większość cyberataków na przedsiębiorstwa rozpoczyna się od punktu końcowego. Ograniczone możliwości zapobiegania i automatyzacji prowadzą do przeciążenia specjalistów pracą związaną z incydentami naruszenia bezpieczeństwa. Każdy punkt końcowy może stać się główną przyczyną zakłócenia działalności firmy. Kaspersky Endpoint Security for Business zapobiega zagrożeniom i ogranicza funkcjonalność punktów końcowych poprzez łączenie adaptacyjnej ochrony z rozbudowanymi narzędziami kontroli. Zagrożenia zostają zablokowane, zanim zaszkodzą danym lub spowodują zmniejszenie produktywności użytkownika, nawet jeśli punkt końcowy nie znajduje się w obrębie sieci korporacyjnej.

Idealny dla

Organizacji o rosnących i coraz bardziej zróżnicowanych oczekiwaniach w zakresie IT

Organizacji chcących ograniczyć możliwość i częstotliwość błędów użytkowników prowadzących do incydentów naruszenia bezpieczeństwa

Korzyści dla firm

Zapobiega zakłóceniom działalności firmy oraz błędom ludzkim

Wspiera transformację cyfrową i chroni pracowników mobilnych

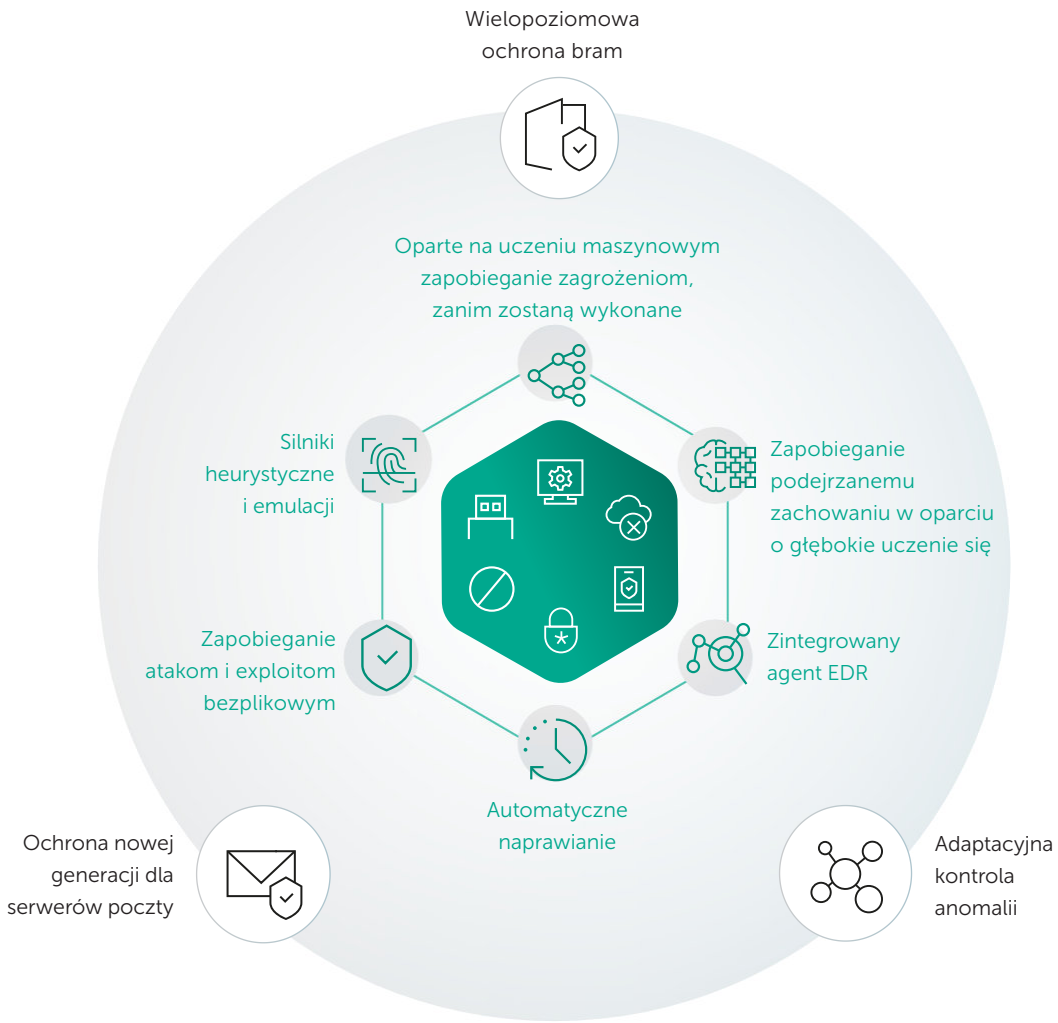
Zwiększa gotowość na audyt – identyfikuje i eliminuje luki w zabezpieczeniach, zmiany konfiguracji w czasie oraz niezaszyfrowane urządzenia

Maksymalizuje zwrot z inwestycji poprzez zmniejszenie powierzchni ataków oraz liczby incydentów do zarządzania

Umożliwia kontrolę każdego punktu końcowego dzięki zintegrowanej konsoli oraz ujednoliconemu agentowi

Przypadki zastosowania

- Zmniejsza podatność na atak poprzez stosowanie adaptacyjnego ograniczenia funkcjonalności, ochronę punktów końcowych, serwerów poczty i plików oraz bram internetowych
- Zapewnia zgodność punktu końcowego z wymaganiami regulacyjnymi
- Automatyzuje zadania wykrywania, reagowania i wdrażania oprogramowania, uwalniając czas specjalistów ds. bezpieczeństwa
- Usprawnia integrację i stosowanie innych technologii bezpieczeństwa


Wielopoziomowa ochrona bram
Oparte na uczeniu maszynowym zapobieganie zagrożeniom, zanim zostaną wykonane
Silniki heurystyczne i emulacji
Zapobieganie podejrzanemu zachowaniu w oparciu o głębokie uczenie się
Zapobieganie atakom i exploitom bezplikowym
Zintegrowany agent EDR
Automatyczne naprawianie
Ochrona nowej generacji dla serwerów poczty
Adaptacyjna kontrola anomalii

Kaspersky Hybrid Cloud Security

Hybrid Cloud Security to rozwiązanie, które upraszcza i zabezpiecza transformację cyfrową, gdy organizacje wirtualizują zadania lub przenoszą je do chmury. Opatentowana technologia Light Agent umożliwia centralizację oraz inteligentną optymalizację funkcji bezpieczeństwa, znacząco zmniejszając wykorzystanie zasobów hipernadzorcy. Natywna integracja z szerokim wachlarzem platform wirtualizacji, kontenerów oraz chmur publicznych zapewnia stałą widoczność oraz kontrolę w całej infrastrukturze. Pełny zakres technologii bezpieczeństwa zarządzanych z tej samej konsoli umożliwia sprawniejszą kontrolę ryzyka w różnorodnych środowiskach.

Idealny dla

Przedsiębiorstw, które wirtualizują serwery oraz stacje robocze

Organizacji, które utrzymują infrastrukturę w chmurach publicznych lub przenoszą ją do chmur

Przedsiębiorstw wykorzystujących chmury publiczne oraz kontenery do operacji programistycznych

Korzyści dla firm

Zapewnia stałą widoczność i kontrolę w centrum danych oraz we wdrożeniach w chmurze

Ogranicza powierzchnię ataków oraz czas przebywania zagrożenia w systemie, utrudniając dalsze rozprzestrzenianie się infekcji w sieci

Uwalnia do 30% zasobów hipernadzorcy i skraca czas logowania się z minut do sekund

Ułatwia zachowanie zgodności z przepisami

Zapewnia sprawną współpracę między zespołami ds. IT, bezpieczeństwa informacji oraz wdrożeń, zmniejszając ryzyko oraz luki w zabezpieczeniach

Przypadki zastosowania

- Nieobciążająca zasobów ochrona zwirtualizowanych infrastruktur serwerów
- Bezpieczeństwo dla infrastruktury wirtualnych stacji roboczych VMWare oraz Citrix
- Umożliwia zachowanie zgodności z przepisami poprzez spełnienie podstawowych wymogów bezpieczeństwa
- Ochrona obciążeń w chmurze dla instancji AWS oraz Azure z automatycznym wdrożeniem i ciągłą widocznością dzięki natywnej integracji API
- Bezpieczeństwo dla operacji programistycznych z ochroną kontenera oraz interfejsem API zarządzania

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server chroni przed zagrożeniami rozprzestrzenianymi za pośrednictwem poczty e-mail, powstrzymując je przed dotarciem do punktu końcowego, który w większości przypadków stanowi domenę socjotechniki oraz szkodliwego oprogramowania. Blokowane są wszelkiego rodzaju szkodliwe programy, w tym oprogramowanie ransomware oraz szkodliwe kryptokoparki, jak również próby ataków phishingowych. W szczególności rozwiązanie zapobiega naruszaniu bezpieczeństwa przy użyciu biznesowych wiadomości e-mail (BEC). Ponadto blokuje niechciane masowe wysyłki i zapobiega niepożądanym transmisjom danych.

Idealny dla

Każdej firmy posiadającej dobrze rozwiniętą technologię informacyjną oraz dbającej o prywatność i bezpieczeństwo danych

Każdej firmy polegającej w dużym stopniu na komunikacji za pośrednictwem poczty e-mail oraz wymagającej szczegółowego zarządzania

Przedsiębiorstw chcących wzbogacić swoje dane umożliwiające wykrywanie ataków APT o kontekst e-mail oraz blokować komponenty ataków APT wykorzystujące pocztę e-mail

Korzyści dla firm

Zwiększa produktywność poprzez blokowanie niechcianych masowych wiadomości e-mail – w tym spamu – oraz oferowanie kategorii poczty dla wygodniejszego zarządzania komunikacją

Pomaga zapobiegać zakłóceniu działalności poprzez blokowanie zagrożeń wykorzystujących pocztę e-mail

Zwiększa bezpieczeństwo danych poprzez uniemożliwianie transferów określonych rodzajów danych

Pomaga obniżyć koszty ogólne poprzez ograniczenie incydentów na poziomie użytkownika

Zwiększa skuteczność dotychczasowej ochrony bram pocztowych poprzez zapewnienie lepszych możliwości wykrywania – bez dodatkowych fałszywych trafień

Przypadki zastosowania

- Działa z szerokim zakresem serwerów poczty elektronicznej lub jako uniwersalne urządzenie wirtualne
- Zapewnia ochronę poczty zintegrowaną z interfejsem API dla serwerów Microsoft Exchange, zarówno na poziomie bramy jak i skrzynki pocztowej
- Blokuje transfery określonych typów plików
- Integruje się z Kaspersky Anti Targeted Attack w celu blokowania komponentów ataków APT wykorzystujących pocztę e-mail

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway zapewnia ochronę przed zagrożeniami WWW na poziomie obrzeży systemu obrony firmy, uniemożliwiając im dotarcie do ostatecznego, głównego celu wszystkich rodzajów ataków, jakim jest punkt końcowy. Rozwiązanie pomaga zapobiegać atakom wykorzystującym socjotechnikę i blokuje wszelkie rodzaje szkodliwego oprogramowania – w tym oprogramowanie ransomware i szkodliwe kryptokoparki – jak również ataki phishingowe. Produkt może zostać połączony z obecnie wykorzystywanym firmowym serwerem proxy w celu uzyskania lepszych wyników lub wdrożony jako gotowe do użycia, uniwersalne urządzenie wirtualne.

Idealny dla

Każdej firmy posiadającej dobrze rozwiniętą technologię informacyjną oraz dbającej o prywatność i bezpieczeństwo danych

Dostawców usług zarządzanych oraz dostawców dowolnych usług (w tym usług telekomunikacyjnych)

Korzyści dla firm

Zapobiega zakłóceniu działalności firmy poprzez blokowanie zagrożeń WWW, zanim ktoś coś kliknie i „wpuści" je do sieci

Zwiększa skuteczność dotychczasowej ochrony bram pocztowych poprzez zapewnienie lepszych możliwości wykrywania bez dodatkowych fałszywych trafień

Pomaga obniżyć koszty ogólne poprzez ograniczenie incydentów na poziomie użytkownika

Zwiększa produktywność i ogranicza ryzyko poprzez zarządzanie korzystaniem z internetu oraz przesyłaniem określonych rodzajów plików

Przypadki zastosowania

- Blokuje szkodliwe i phishingowe zasoby WWW jak również pobrane szkodliwe oprogramowanie
- Zapobiega wykorzystywaniu niepożądanych zasobów WWW
- Umożliwia zarządzanie osobnymi obszarami roboczymi przy pomocy ich własnych zestawów reguł
- Odfiltrowuje niepożądane typy plików przemieszczających się w obie strony w oparciu o liczne kryteria
- Integruje się z rozwiązaniem Kaspersky Anti Targeted Attack jako sensor WWW i blokuje komponenty ataków ukierunkowanych na podstawie zaawansowanych wyników wykrywania

Kaspersky Security for Storage

Łatwo dostępna pamięć połączona może łatwo stać się źródłem infekcji w całej infrastrukturze – oraz celem zagrożeń takich jak ransomware. Kaspersky Security for Storage zabezpiecza dane korporacyjne i zapobiega infekcji sieci przy pomocy sprawdzonego zestawu technologii bezpieczeństwa wspomaganych globalną analizą zagrożeń. Rozwiązanie obejmuje unikatowe funkcje takie jak Remote Anti-Cryptor (zdalna ochrona przed programami kryptograficznymi) wspierane integracją z interfejsami API systemu przechowywania.

Idealny dla

Każdej firmy posiadającej dobrze rozwiniętą technologię informacyjną oraz dbającej o prywatność i bezpieczeństwo danych

Firm działających w takich branżach jak bankowość, handel elektroniczny czy ubezpieczenia, które obsługują ogromne ilości wrażliwych/prywatnych danych

Korzyści dla firm

Chroni dane w pamięciach połączonych bez zakłócania oprogramowania pamięci

Zmniejsza uciążliwości administracyjne i zwiększa bezpieczeństwo dzięki konsoli zarządzania umożliwiającej podgląd z jednego miejsca

Pozwala zachować ciągłość działalności poprzez ochronę przechowywanych danych przed zdalnie działającym oprogramowaniem ransomware oraz programami kryptograficznymi usuwającymi dane (crypto-wiper)

Wspomaga zachowanie zgodności z przepisami poprzez oferowanie ochrony dla szerokiego wachlarza modeli

Przypadki zastosowania

- Zabezpiecza zarówno pamięci połączone z siecią, jak i serwer, na którym działa
- Za każdym razem, gdy w zabezpieczonej pamięci pojawia się nowy plik lub zmianie ulega istniejący plik, zostaje on sprawdzony pod kątem szkodliwości. Możliwe jest również skanowanie na żądanie
- Gdy pliki zaczynają być zdalnie szyfrowane, rozwiązanie wykrywa i blokuje źródło problemu w sieci, zapobiegając dalszym szkodom*

* Integracja z API jest dostępna tylko dla wybranych magazynów pamięci

Kaspersky Embedded Systems Security

Dzięki zaawansowanej analizie zagrożeń, wykrywaniu szkodliwego oprogramowania w czasie rzeczywistym, wszechstronnym funkcjom kontroli aplikacji i urządzeń oraz elastycznemu zarządzaniu, Kaspersky Embedded Systems Security zapewnia pełną ochronę stworzoną przede wszystkim z myślą o systemach wbudowanych.

Idealny dla

Usług finansowych

Branży sprzedaży detalicznej i transportowej

Dostawców usług bankomatowych i punktów sprzedaży

Korzyści dla firm

Ogranicza ryzyko związane z zagrożeniami atakującymi określone infrastruktury finansowe

Spełnia wymogi zgodności z przepisami takich regulacji jak PCI/DSS, SWIFT itd.

Optymalizuje koszty administracyjne dzięki pojedynczej konsoli zarządzania

Przypadki zastosowania

- Zabezpiecza geograficznie rozproszone i rzadko aktualizowane systemy wbudowane, które stanowią specyficzny i unikatowy problem dla bezpieczeństwa
- Ochrona niewspieranego już systemu Windows XP, który nadal jest powszechnie wykorzystywany na sprzęcie niższej klasy
- Zaprojektowany w sposób zapewniający skuteczną ochronę bez ryzyka przeciążenia systemów

Kaspersky Premium Support (MSA) usługa

W przypadku incydentu naruszenia bezpieczeństwa, istotne jest to, jak szybko uda się zidentyfikować i wyeliminować jego przyczynę. Natychmiastowe wykrycie i rozwiązanie problemu może uchronić firmę przed znacznymi kosztami. Właśnie dlatego stworzyliśmy plany w ramach umowy o obsługę serwisową (MSA). Całodobowy dostęp do naszych ekspertów, odpowiednia priorytetyzacja problemów z gwarantowanymi czasami reakcji i prywatnymi łatami – wszystko czego potrzebujesz, aby mieć pewność, że Twój problem zostanie rozwiązany możliwie najszybciej.

Idealny dla

każdej organizacji wykorzystującej produkty firmy Kaspersky

1 Wymagane umiejętności

5 Dostosowanie do indywidualnych potrzeb i skalowalność

3 Koszt

Korzyści dla firm

Zapewnia ciągłość działalności dzięki przydzielonym, dyżurującym ekspertom, którzy mają za zadanie zająć się Twoją sprawą i rozwiązać ją w jak najkrótszym czasie

Zmniejszony koszt incydentu naruszenia bezpieczeństwa dzięki dostępowi do priorytetowej linii pomocy technicznej, gwarantowanym czasom reakcji oraz prywatnym łatom

Wydzielony menedżer ds. technicznych pełni funkcję Twojego przedstawiciela w firmie Kaspersky i może uzyskać wszelką specjalistyczną wiedzę niezbędną do szybkiego rozwiązania danej kwestii

Przypadki zastosowania

- Przyspieszenie rozwiązania krytycznych kwestii poprzez skierowanie ich do specjalistów pracujących w Kaspersky „za kulisami", do sztabu, który posiada największe kompetencje, aby dostarczyć Ci odpowiednie rozwiązanie w krótkim czasie
- Proaktywne środki dostosowane do Twojego systemu, w tym poprawki priorytetowe oraz zindywidualizowane łaty, zapewniają Ci pełną ochronę
- Skrócenie czasu poświęcanego przez Twoje cenne zasoby wewnętrzne na konserwację oraz rozwiązywanie problemów

Kaspersky Professional Services usługa

Cyberbezpieczeństwo to spora inwestycja. Zyskaj maksymalne korzyści, współpracując z ekspertami, którzy wiedzą, jak zoptymalizować Twoje bezpieczeństwo z uwzględnieniem unikatowych potrzeb Twojej organizacji. Działając zgodnie z Twoimi najlepszymi praktykami oraz metodami, nasi eksperci ds. bezpieczeństwa pomogą Ci w każdym aspekcie dotyczącym wdrażania, konfigurowania oraz aktualizowania produktów firmy Kaspersky w całej infrastrukturze IT Twojego przedsiębiorstwa.

Usługi Kaspersky Professional Services obejmują:

- Implementację i aktualizację do nowszej wersji
- Konfigurację
- Szkolenie w zakresie produktu

Idealne dla każdej organizacji wykorzystującej produkty firmy Kaspersky

Korzyści dla firm

Maksymalizacja Twojego zwrotu z inwestycji w rozwiązania bezpieczeństwa dzięki wykorzystaniu 100% ich możliwości

Obniżenie kosztów związanych z wewnętrznym personelem IT

Minimalizacja ryzyka związanego z przestojem w pracy poprzez okresowe audyty konfiguracji produktów i zapewnienie stosowania najbardziej aktualnych mechanizmów ochrony

Skrócenie okresu adaptacji produktu, co umożliwia szybsze czerpanie korzyści z zaimplementowanego produktu

Przypadki zastosowania

- Ograniczenie ryzyka związanego z implementacją, które może osłabić ochronę, niekorzystnie wpłynąć na produktywność, a nawet prowadzić do przestoju w pracy
- Minimalizacja wpływu implementacji nowego rozwiązania zabezpieczającego na bieżące operacje biznesowe i obniżenie ogólnych kosztów implementacji
- Przygotowanie personelu na bieżącą obsługę produktu dzięki naszym programom szkoleniowym, które pomagają zapobiegać błędom, przedstawiają możliwości produktów i wyjaśniają zasady ich działania

Kaspersky Security Awareness

Nasze komputerowe programy szkoleń pozwalają zmienić nawyki i kształtować nowe wzorce zachowań, które stanowią prawdziwy cel szkolenia w zakresie podnoszenia świadomości. Oferta szkoleń Kaspersky Security Awareness obejmuje: Automated Security Awareness Platform (ASAP) – szkolenie dla wszystkich pracowników, które pozwala stopniowo rozwijać umiejętności w zakresie higieny cyfrowej; Cybersecurity for IT Online (CITO) – szkolenie przeznaczone dla ogólnych specjalistów IT, umożliwiające rozwój praktycznych umiejętności dotyczących rozpoznawania potencjalnego scenariusza ataków oraz gromadzenia danych o incydencie; Kaspersky Interactive Protection Simulation (KIPS) – gra o tematyce cyberbezpieczeństwa dla osób podejmujących decyzje.

Idealny dla

Organizacji o rosnących i coraz bardziej zróżnicowanych oczekiwaniach w zakresie IT

Organizacji chcących ograniczyć możliwość i częstotliwość błędów użytkowników prowadzących do incydentów naruszenia bezpieczeństwa

Korzyści dla firm

Ochrona firm od środka

Utrzymanie podejścia nastawionego na cyberbezpieczeństwo w całej kulturze organizacyjnej

Ograniczenie liczby błędów człowieka nawet o 80%

Przypadki zastosowania

- Kształtuje zachowanie sprzyjające cyberbezpieczeństwu poprzez przedstawianie typowych scenariuszy i sytuacji, symulacje cyberataków, rozmaite zadania oraz wyjaśnienia
- Umożliwia zrozumienie potencjalnych zagrożeń i kształtuje umiejętności niezbędne do zabezpieczenia się przed nimi
- Rozwija praktyczne umiejętności umożliwiające rozpoznanie potencjalnego ataku w pozornie nieszkodliwym incydencie komputerowym oraz gromadzenie danych dotyczących incydentu w celu przekazania ich do działu bezpieczeństwa IT
- Pomaga menedżerom wyższego szczebla oraz osobom podejmującym decyzje lepiej zrozumieć kwestie dotyczące bezpieczeństwa

2 Zaawansowana obrona

Zaawansowana technologia wykrywania i scentralizowane reagowanie

Maksymalna automatyzacja na etapie wykrywania i reagowania na złożone zagrożenia pominięte przez technologie prewencyjne

- Coraz większe i coraz bardziej złożone środowiska IT o zwiększonej powierzchni ataków
- Niewielki zespół ds. bezpieczeństwa o ograniczonej wiedzy eksperckiej
- Podstawowe możliwości w zakresie reagowania na incydenty

Idealny dla średnich przedsiębiorstw:

Punkt końcowy

Kaspersky Endpoint Detection and Response

Ludzie

Kaspersky Cybersecurity Training

Usługi

Kaspersky Targeted Attack Discovery

Sieć

Kaspersky Anti Targeted Attack

Prywatność

Kaspersky Private Security Network

Analiza

Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

Skuteczna ochrona przed zaawansowanymi atakami na możliwie najwcześniejszym etapie wymaga dopełnienia technologii prewencyjnych zaawansowanymi możliwościami w zakresie wykrywania i reagowania na zagrożenia atakujące punkty końcowe. Kaspersky EDR to wyspecjalizowane rozwiązanie, które chroni przed zaawansowanymi zagrożeniami dla punktów końcowych i posiada tego samego agenta co nasze wielokrotnie nagradzane rozwiązanie zabezpieczające Kaspersky Endpoint Security. Kaspersky EDR zapewnia pełną widoczność na wszystkich punktach końcowych w sieci korporacyjnej, umożliwiając automatyzację rutynowych zadań w celu szybkiego wykrywania, priorytetyzowania, badania oraz neutralizowania złożonych zagrożeń.

Idealny dla

Korporacji

Organizacji, które wykorzystują już rozwiązanie Kaspersky Endpoint Security

Centrów operacji bezpieczeństwa oraz zespołów ds. reagowania na incydenty

Korzyści dla firm

Ogranicza ryzyko związane z zaawansowanymi zagrożeniami oraz atakami ukierunkowanymi

Optymalizuje koszty administracyjne poprzez automatyzację zadań oraz pojedynczy, uproszczony interfejs

Zwiększa prędkość i skuteczność przetwarzania incydentów bez dodatkowych kosztów

Zwiększa produktywność, dzięki czemu Twój zespół ds. IT oraz bezpieczeństwa może przeznaczyć więcej czasu na inne zadania

Ułatwia zapewnienie zgodności z wewnętrznymi politykami bezpieczeństwa oraz wymaganiami regulacyjnymi

Przypadki zastosowania

- Obsługuje pełny cykl ochrony punktu końcowego, od automatycznego blokowania zagrożeń po reagowanie na zaawansowane ataki w ramach złożonych incydentów, przy użyciu jednego agenta
- Zapewnia szybki dostęp do danych dot. punktu końcowego, nawet gdy nie jest możliwy dostęp do zainfekowanych stacji roboczych lub dane zostały zaszyfrowane
- Uzupełnia prace dochodzeniowe w sprawie incydentów o wyszukiwanie zagrożeń, analizę IoA oraz mapowanie MITRE ATT&CK
- Umożliwia sprawną reakcję w infrastrukturach rozproszonych poprzez zautomatyzowane działania o szerokim zasięgu

Kaspersky Anti Targeted Attack

Liczba i jakość ataków ukierunkowanych nieustannie rośnie. W celu zwalczania tych nowych zagrożeń konieczne jest ciągłe dostosowywanie systemów bezpieczeństwa. Kaspersky Anti Targeted Attack koncentruje się na wykrywaniu zaawansowanych zagrożeń na poziomie sieci przy pomocy w pełni automatycznego gromadzenia, analizowania i korelowania danych, umożliwiając dogłębne zrozumienie zakresu zagrożenia. Rezultatem jest skuteczna ochrona infrastruktury firmowej przed złożonymi zagrożeniami oraz atakami ukierunkowanymi bez konieczności wykorzystywania dodatkowych zasobów.

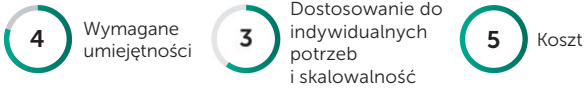
Idealny dla

Korporacji

Zespołów pracujących w centrach operacji bezpieczeństwa (SOC)

Dostawców zarządzanych usług bezpieczeństwa

Organizacji zobligowanych do przestrzegania określonych przepisów



Korzyści dla firm

Ogranicza ryzyko związane z zaawansowanymi zagrożeniami oraz atakami ukierunkowanymi

Zmniejsza szkody finansowe i operacyjne poprzez wprowadzenie jednego, niezawodnego systemu ochrony przed złożonymi atakami

Optymalizuje koszty administracyjne poprzez automatyzację zadań oraz pojedynczy, uproszczony interfejs

Usprawnia zadania dzięki płynnej automatyzacji przepływu pracy bez zakłócania procesów biznesowych

Przypadki zastosowania

- Szybkie wykrywanie działań cyberprzestępców, którzy zdołali obejść technologie prewencyjne, poprzez scentralizowane monitorowanie i kontrolę potencjalnych punktów wniknięcia do infrastruktury
- Wykrywanie oznak wskazujących na zagrożenie oraz zestawianie wielowektorowych zdarzeń w ramach jednego ataku w spójny „obraz" w celu umożliwienia skuteczniejszego prowadzenia prac dochodzeniowych
- Niezwłoczne dostarczanie zespołowi ds. reagowania na incydenty wszelkich niezbędnych informacji dotyczących wykrytych zagrożeń

Kaspersky Private Security Network

Kaspersky Private Security Network pozwala organizacjom czerpać większość korzyści, jakie oferuje globalna, oparta na chmurze analiza zagrożeń, bez przekazywania jakichkolwiek danych poza sieć korporacyjną. To rodzaj osobistej, lokalnej i całkowicie prywatnej wersji rozwiązania Kaspersky Security Network.

Idealny dla

Przedsiębiorstw podlegających rygorystycznym wymogom dot. kontroli dostępu do danych

Infrastruktur krytycznych z fizycznie odizolowanymi sieciami

Dostawców usług telekomunikacyjnych, zarządzanych usług bezpieczeństwa oraz innych

4 Wymagane umiejętności

4 Dostosowanie do indywidualnych potrzeb i skalowalność

5 Koszt

Korzyści dla firm

Wspomaga lepsze wykrywanie zagrożeń atakujących Twoją firmę

Zapewnia szybszy czas reakcji dzięki dostępowi w czasie rzeczywistym do statystyk dotyczących zagrożeń oraz reputacji

Zwiększa efektywność działania ochrony poprzez minimalizację fałszywych trafień

Wspomaga pełną zgodność z wymogami regulacyjnymi w celu zapewnienia bezpieczeństwa odizolowanych systemów oraz środowisk

Przypadki zastosowania

- Wszystkie korzyści oferowane przez ochronę wspomaganą chmurą bez konieczności przekazywania informacji poza kontrolowaną infrastrukturę
- Umożliwia stworzenie zindywidualizowanej ochrony poprzez dodawanie własnych „werdyktów”
- Dostosowany do odizolowanych sieci krytycznych

Kaspersky Targeted Attack Discovery

usługa

Kaspersky Targeted Attack Discovery to wszechstronna usługa oceny pod kątem naruszenia bezpieczeństwa, która pozwala określić, czy stanowisz obecnie cel ataku, co się dzieje i kto przeprowadza atak. Nasi eksperci wykrywają, identyfikują oraz analizują zarówno bieżące jak i przeszłe incydenty, tworząc listę systemów, które zostały zaatakowane. Pomagamy Ci wykrywać szkodliwe działania, identyfikować potencjalne źródła incydentu oraz planować najskuteczniejsze działania naprawcze.

Idealny dla

Przedsiębiorstw, które nie zatrudniają zespołu ds. bezpieczeństwa lub w których taki zespół nie osiągnął jeszcze dojrzałości

Instytucji rządowych

Infrastruktur krytycznych

Korzyści dla firm

Zapobiega i minimalizuje szkody wynikające z naruszenia bezpieczeństwa systemów, powodując znaczące obniżenie kosztów

Pomaga utrzymywać relacje oparte na zaufaniu z klientami, partnerami oraz inwestorami w celu dalszego wykorzystywania możliwości biznesowych

Pozwala uniknąć kar i mandatów za nieprzestrzeganie przepisów

Wzmacnia Twoją ochronę na wypadek przyszłych incydentów poprzez zalecenia działań zaradczych

Przypadki zastosowania

- Pozwala poznać „ślad cyfrowy" Twojej organizacji oraz związane z nim zagrożenia
- Pomaga w ocenie ryzyka za pomocą szczegółowych inspekcji Twojej infrastruktury oraz danych IT (takich jak pliki dzienników) jak również analizy Twoich wychodzących połączeń sieciowych
- Identyfikuj sygnały bieżących lub przeszłych włamań w obrębie Twoich sieci
- Dowiedz się, w jaki sposób atak wpływa na Twoje systemy i co możesz zrobić w takim przypadku

Kaspersky Threat Intelligence

Zwalczanie dzisiejszych cyberzagrożeń wymaga pełnego obrazu taktyk i narzędzi wykorzystywanych przez cyberprzestępców. Uzyskanie takich informacji oraz zidentyfikowanie najskuteczniejszych środków zaradczych wymaga nieustannej czujności i wysokiego poziomu wiedzy eksperckiej. Mając do dyspozycji petabajty danych dotyczących zagrożeń, zaawansowane technologie uczenia maszynowego oraz unikatowy zespół ekspertów na całym świecie, firma Kaspersky dostarczy Ci najnowsze dane analityczne dotyczące zagrożeń z całego globu, dzięki czemu będziesz odporny nawet na całkowicie nowe cyberataki.

Idealny dla

Korporacji

Instytucji rządowych

Centrów operacji bezpieczeństwa oraz zespołów ds. reagowania na incydenty

Dostawców zarządzanych usług bezpieczeństwa

Korzyści dla firm

Natychmiastowe wykrywanie zagrożeń w celu zapobiegania zakłóceniu operacji biznesowych

Minimalizacja potencjalnych strat finansowych na skutek incydentów

Gwarantuje opłacalność inwestycji w określone technologie oraz personel w oparciu o uzyskiwane w odpowiednim czasie informacje dotyczące zagrożeń atakujących Twoje przedsiębiorstwo

Uniemożliwia innym firmom zdobycie **nieuczciwej przewagi konkurencyjnej** poprzez kradzież własności intelektualnej

Pomaga stworzyć **proaktywną i adaptacyjną ochronę**

Przypadki zastosowania

- Wzmocnij rozwiązania bezpieczeństwa sieciowego przy pomocy nieustannie aktualizowanych źródeł danych o zagrożeniach
- Skutecznie priorytetyzuj ogromne ilości alertów zabezpieczeń i błyskawicznie identyfikuj te, które powinny zostać przekazane do zespołów ds. reagowania na incydenty
- Zyskaj „świadomość sytuacji" w czasie rzeczywistym i skuteczniej wykorzystuj źródła analizy zagrożeń
- Zidentyfikuj „ślad cyfrowy" Twojej organizacji i zredukuj związane z nim ryzyko

Kaspersky Cybersecurity Training: Incident Response

usługa

Edukacja w zakresie cyberbezpieczeństwa ma krytyczne znaczenie w przypadku przedsiębiorstw stykających się z coraz większą liczbą nieustannie ewoluujących zagrożeń. Personel ds. bezpieczeństwa IT musi opanować zaawansowane techniki leżące u podstaw skutecznych strategii kontroli i łagodzenia zagrożeń korproacyjnych. Szkolenie Kaspersky Cybersecurity Training zapewnia Twojemu wewnętrznemu zespołowi ds. bezpieczeństwa niezbędną wiedzę pomagająca radzić sobie z nieustannie ewoluującym środowiskiem zagrożeń.

Idealny dla

Korporacji

Instytucji rządowych

Centrów operacji bezpieczeństwa oraz zespołów ds. reagowania na incydenty

Dostawców zarządzanych usług bezpieczeństwa

3 Wymagane umiejętności

3 Dostosowanie do indywidualnych potrzeb i skalowalność

2 Koszt

Korzyści dla firm

Szybko i skutecznie łagodzi potencjalne szkody wynikające z incydentu naruszenia bezpieczeństwa w celu znacznego zmniejszenia kosztu incydentu

Pozwala uniknąć kar i mandatów związanych z nieprzestrzeganiem przepisów

Pomaga utrzymywać **oparte na zaufaniu relacje z klientami, partnerami oraz inwestorami** w celu dalszego wykorzystywania możliwości biznesowych

Wzmacnia Twoją ochronę na wypadek przyszłych incydentów dzięki zdobytym doświadczeniom

Przypadki zastosowania

- Rozróżniaj wyrafinowane ataki APT od innych zagrożeń
- Poznaj techniki stosowane przez różne cyberugrupowania oraz anatomię ataków ukierunkowanych
- Stosuj określone metody monitorowania i wykrywania
- Twórz skuteczne reguły wykrywania
- Odtwarzaj chronologię oraz logikę incydentów i monitoruj przepływ pracy dotyczący reagowania na incydenty

3 Zintegrowane podejście do cyberbezpieczeństwa

Zarządzanie zagrożeniami i ochrona przed nimi

Przygotuj się na ataki na poziomie APT

Idealny dla przedsiębiorstw posiadających zespoły dysponujące wysokim poziomem wiedzy eksperckiej, przyzwyczajone do aktywnego wyszukiwania nowych zagrożeń oraz pracy z analizą zagrożeń

- Złożone i rozproszone środowiska
- Wewnętrzny zespół ds. bezpieczeństwa lub centrum operacji bezpieczeństwa
- Wyższe koszty incydentów oraz naruszenia bezpieczeństwa danych
- Zobligowane do przestrzegania regulacji

Usługi

- **Kaspersky Managed Protection**
- **Kaspersky Incident Response**

Ludzie

- **Kaspersky Cybersecurity Training**

Analiza

- **Kaspersky Threat Intelligence**

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense to wyspecjalizowane rozwiązanie umożliwiające szybkie wykrywanie zagrożeń, badanie incydentów, reagowanie na nie oraz ich eliminowanie. Obejmuje globalną analizę zagrożeń, zaawansowane technologie wykrywania zagrożeń i reagowania, wybór szkoleń w zakresie cyberbezpieczeństwa, nieustanne wyszukiwanie zagrożeń oraz reagowanie na zagrożenia, które zdołały obejść istniejące bariery zabezpieczające. Rozwiązanie może zostać zintegrowane z aktualną strategią organizacji w celu zwalczania złożonych zagrożeń, uzupełniając dotychczasowe technologie ochrony oraz wspierając Cię czołową w branży wiedzą ekspercką.

Idealny dla

Korporacji

Instytucji rządowych

Centrów operacji bezpieczeństwa i zespołów ds. reagowania na incydenty

Dostawców zarządzanych usług bezpieczeństwa

5 Wymagane umiejętności

5 Dostosowanie do indywidualnych potrzeb i skalowalność

5 Koszt

Korzyści dla firm

Minimalizuje szkody finansowe i operacyjne na skutek cyberprzestępczości i pomaga zachować stabilność działalności

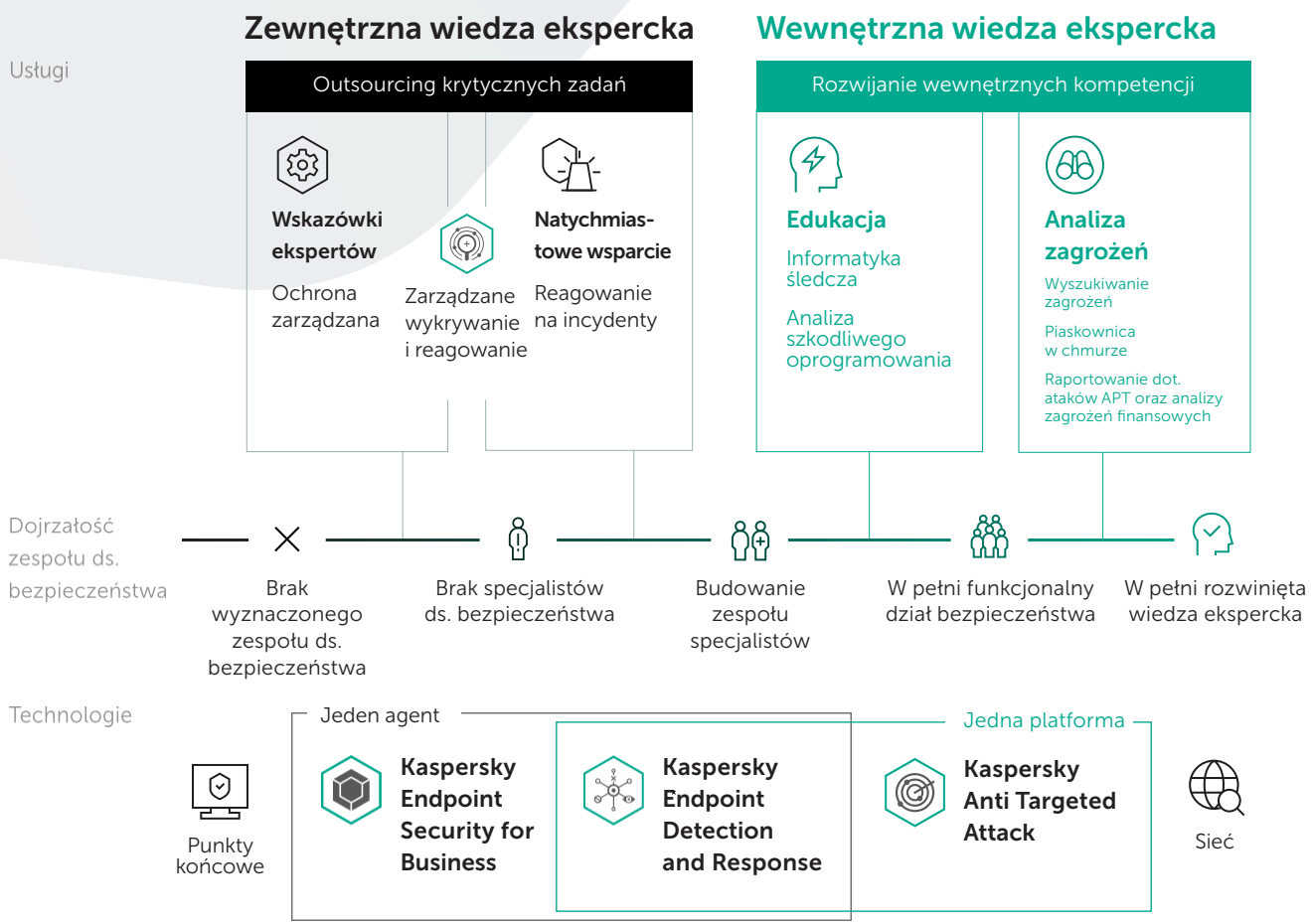
Zwiększa zwrot z inwestycji poprzez automatyzację i zapobieganie zakłóceniom procesów biznesowych

Zmniejsza rotację personelu i zwiększa skuteczność działania poprzez budowanie wewnętrznej wiedzy eksperckiej

Wdraża oparte na wiedzy oraz racjonalne pod względem kosztów strategie bezpieczeństwa informacyjnego w oparciu o zindywidualizowane modele zagrożeń

Przypadki zastosowania

- Uniwersalna platforma technologiczna automatyzuje czasochłonne gromadzenie dowodów oraz rutynowe zadania ręczne
- Proaktywna analiza zagrożeń dostarcza kontekst niezbędny do szybkiego wykrywania, priorytetyzowania oraz badania zagrożeń, jak również reagowania na nie
- Strategia kontroli zagrożeń dla przedsiębiorstwa poprzez zapewnianie zaawansowanych umiejętności
- Wyszukiwanie zagrożeń umożliwia wykrywanie nieznanych i zaawansowanych zagrożeń mających na celu obejście technologii prewencyjnych
- Dostęp do zewnętrznej wiedzy eksperckiej wspiera skuteczne badanie i reagowanie na złożone incydenty


Zewnętrzna wiedza ekspercka
Wewnętrzna wiedza ekspercka
Usługi
Outsourcing krytycznych zadań
Rozwijanie wewnętrznych kompetencji
Wskazówki ekspertów
Ochrona zarządzana
Zarządzane wykrywanie i reagowanie
Natychmiastowe wsparcie
Reagowanie na incydenty
Edukacja
Informatyka śledcza
Analiza szkodliwego oprogramowania
Analiza zagrożeń
Wyszukiwanie zagrożeń
Piaskownica w chmurze
Raportowanie dot. ataków APT oraz analizy zagrożeń finansowych
Dojrzałość zespołu ds. bezpieczeństwa
Brak wyznaczonego zespołu ds. bezpieczeństwa
Brak specjalistów ds. bezpieczeństwa
Budowanie zespołu specjalistów
W pełni funkcjonalny dział bezpieczeństwa
W pełni rozwinięta wiedza ekspercka
Technologie
Jeden agent
Jedna platforma
Punkty końcowe
Kaspersky Endpoint Security for Business
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Sieć

O czym należy pamiętać, opracowując długoterminową strategię cyberbezpieczeństwa

Odizolowane podejście do bezpieczeństwa naraża firmy na ryzyko

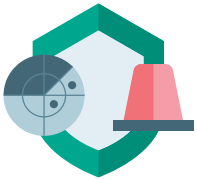
Coraz wyższe koszty incydentów naruszenia bezpieczeństwa sieci i danych stanowią poważne obciążenie finansowe dla firm dążących do transformacji, dlatego cyberbezpieczeństwo staje się tak istotną kwestią. Aby odnieść sukces w tym środowisku firmy muszą traktować cyberbezpieczeństwo jako integralny element swojej ogólnej strategii biznesowej, odgrywający kluczową rolę w zarządzaniu ryzykiem oraz długoterminowym planowaniu.

Cyberbezpieczeństwo nie jest celem – to ciągła podróż

Plan bezpieczeństwa firmy wymaga nieustanej rewizji i modyfikacji wraz z pojawianiem się nowej wiedzy i narzędzi. Każdy incydent naruszenia bezpieczeństwa powinien podlegać szczegółowej analizie i prowadzić do opracowania nowych procedur postępowania w przypadku ataku jak również środków pozwalających zapobiec podobnym incydentom w przyszłości. Należy nieustannie doskonalić aktualne mechanizmy bezpieczeństwa.

Świadomość, komunikacja oraz współpraca stanowią klucz do sukcesu w świecie nieustannie zmieniających się cyberzagrożeń

Ponad 80% wszystkich cyberincydentów wynika z błędu ludzkiego. Niezbędne jest szkolenie personelu na każdym szczeblu w celu zwiększenia świadomości dotyczącej bezpieczeństwa w całej organizacji oraz zmotywowania pracowników do zwracania uwagi na cyberzagrożenia oraz środki zaradcze – nawet jeśli uważają, że nie wchodzi to w zakres ich obowiązków związanych z pracą.



Proaktywne podejście do wykrywania i reagowania na cyberzagrożenia jest najlepszym sposobem na przeciwdziałanie obecnym, nieustannie ewoluującym zagrożeniom

Tradycyjne systemy prewencyjne powinny działać w harmonii z zaawansowanymi technologiami wykrywania, analizą zagrożeń, możliwościami reagowania oraz technikami ochrony predykcyjnej. W ten sposób można stworzyć system cyberbezpieczeństwa, który nieustannie dostosowuje się i reaguje na wyzwania, wobec których stają przedsiębiorstwa.

Powody, dla których powinieneś postawić na rozwiązania firmy Kaspersky

Najczęściej testowane. Najczęściej nagradzane

Firma Kaspersky uzyskała więcej pierwszych miejsc w niezależnych testach niż jakikolwiek inny dostawca rozwiązań bezpieczeństwa. I jesteśmy w tym konsekwentni. Każdego roku. www.kaspersky.pl/top3

Jedne z najbardziej zalecanych

Firma Kaspersky po raz kolejny zdobyła tytuł „Customers' Choice for Endpoint Protection Platforms" w raporcie Gartner Peer Insights, uzyskawszy wysoki współczynnik zadowolenia klientów na poziomie 4.6 przy maksymalnym wyniku 5 (28 maja 2019 r.)*

Najbardziej transparentny

Uruchomiliśmy Centra Transparentności w Szwajcarii, Hiszpanii oraz Malezji, a przetwarzanie danych odbywa się w Zurychu. To oznacza, że gwarantujemy suwerenność Twoich danych w większym stopniu niż inni dostawcy rozwiązań.

*Gartner Peer Insights Customers' Choice odzwierciedla subiektywne opinie przedstawione w recenzjach indywidualnych użytkowników końcowych, rankingi oraz dane, wobec których zastosowano udokumentowaną metodologię; nie odzwierciedla poglądów ani nie stanowi poparcia firmy Gartner lub jej podmioty zależne.

400M+

użytkowników chronionych

przez technologie firmy Kaspersky

Nasi klienci wiedzą, że mogą nam zaufać w kwestii zabezpieczania tego, co najważniejsze - prywatności, plików, zdjęć, rodziny i innych aspektów życia cyfrowego.

270K+

chronionych firm

Korporacje, organizacje sektora publicznego i mniejsze firmy wybierają rozwiązania Kaspersky do zabezpieczania swoich systemów IT, danych i procesów.

Ochrona dla firm: kaspersky.pl/biznes
Ochrona dla korporacji: kaspersky.pl/korporacje
Oficjalny blog: kaspersky.pl/blog

Kaspersky Lab Polska sp. z o.o.
ul. Trawiasta 35, 04-607 Warszawa

#aktywujprzyszlosc

www.kaspersky.pl

kaspersky

Aktywuj przyszłość

www.kaspersky.pl