

kaspersky

Kaspersky dla małych i średnich firm



Wyzwania w zakresie bezpieczeństwa dla małych i średnich firm



Cyberzagrożenia

Nie ma rozwiązań uniwersalnych. Chociaż małe firmy są narażone na wiele cyberzagrożeń, z którymi borykają się duże przedsiębiorstwa, nie dysponują tymi samymi zasobami.



Przeciążone zasoby

Najlepsza ochrona powinna utatwiać funkcjonowanie nadmiernie obciążonych pracą działów IT. Jeśli prowadzisz małą lub średnią firmę, prawdopodobnie Twoje zasoby są stale przeciążone. Dlatego musisz działać inteligentnie – stawiając na rozwiązanie zabezpieczające, które zapewnia natychmiastową ochronę i stanowi minimalne obciążenie dla Twojego budżetu, czasu oraz uwagi.

Ochrona, która nie wymaga wysiłku i rozwija się wraz z osiągnięciem dojrzałości przez Twoją firmę

Cryptolockery Oszustwa związane z płatnościami Ataki ukierunkowane Błędy użytkowników Zagrożenia WWW
Zagrożenia bezplikowe Nowe nieznane zagrożenia Utrata danych Spam Phishing Ransomware



Kaspersky Small Office Security

NAS, magazyn w chmurze, usługi bezpłatne wyłącznie w podstawowym zakresie (tzw. freemium)



Potrzeby firmy

Zainstaluj i zapomnij

Co wymaga zabezpieczenia

Wrażliwe dane i transakcje online



Kaspersky Endpoint Security Cloud

Bezpieczeństwo jako usługa (SaaS) oraz chmura publiczna



Powierz specjalście

Umowy firmowe oraz informacje finansowe



Kaspersky Endpoint Security for Business

Środowiska mieszane



Kontroluj infrastrukturę oraz koszty

Reputacja i własność intelektualna

Infrastruktura



Ochrona współpracy



Kaspersky Security for Microsoft Office 365



Świadomość w zakresie bezpieczeństwa

Kaspersky Security Awareness

Wybierz swoją strategię



Zalety opartego na chmurze zarządzania ochroną punktów końcowych

Natychmiastowa ochrona punktów końcowych przy pomocy rozwiązania typu „bezpieczeństwo jako usługa”, która stanowi minimalne obciążenie dla Twojego budżetu, czasu oraz energii.

- Brak dodatkowych kosztów związanych z wdrożeniem serwera lub oprogramowania
- Ochrona każdego punktu końcowego – plus bezpieczeństwo urządzenia przenośnego za darmo
- Natychmiastowa ochrona wraz z predefiniowanymi politykami bezpieczeństwa
- Zawsze najnowsze, najbardziej aktualne oprogramowanie



Zalety lokalnego zarządzania ochroną punktów końcowych

Ochrona, która potrafi sprostać przyszłym wymaganiom i umożliwia transformację firmy poprzez wszechstronne zabezpieczenie jej przed zagrożeniami, łącznie z tymi najbardziej zaawansowanymi, oraz rozgraniczenie obowiązków, dzięki czemu masz więcej czasu, aby skupić się na potrzebach biznesowych.

- Łatwe skalowanie, zabezpieczenie różnych środowisk i platform
- Elastyczne zasady ochrony, możliwość wyboru momentu migracji do nowych wersji
- Skuteczna ochrona i kontrola dla każdego urządzenia stacjonarnego oraz przenośnego



Kaspersky Small Office Security

oparty na chmurze

Kaspersky Small Office Security powstał z myślą o bardzo małych firmach, które nie zatrudniają specjalistów IT. Jest łatwy w instalacji, jeszcze łatwiejszy w zarządzaniu, oferując przy tym najczęściej testowaną i najczęściej nagradzaną ochronę dla komputerów, serwerów plików, laptopów oraz urządzeń przenośnych. Produkt zabezpiecza także Twoją działalność przed atakami online, oszustwami finansowymi, oprogramowaniem ransomware oraz utratą danych.

Idealny dla organizacji poszukujących nieskomplikowanej ochrony typu „zainstaluj i zapomnij”

0

Wymagane
umiejętności

1

Dostosowanie do
indywidualnych
potrzeb
i skalowalność

1

Koszt

Korzyści dla firm



Instalacja trwa do **10 minut**



Natychmiastowa, łatwa w użyciu ochrona –
**wystarczy skonfigurować i zapomnieć
o obsłudze ochrony**



Zabezpiecza wrażliwe dane i **chroni Twoją
działalność** zapobiegając incydom naruszenia
bezpieczeństwa danych, karom oraz utraconym
szansom biznesowymi

Zalety

- Wiele poziomów ochrony w jednym, łatwym w użyciu pakiecie
- Maksymalne bezpieczeństwo w całej firmie przy minimalnym wysiłku bez konieczności posiadania doświadczenia








Kaspersky Endpoint Security Cloud

oparty na chmurze

Kaspersky Endpoint Security Cloud oferuje małym i średnim firmom niewymagającą wysiłku a jednocześnie pełną, opartą na chmurze ochronę przed znanymi i nieznanymi zagrożeniami – łącznie ze szkodliwymi programami szyfrującymi, oprogramowaniem ransomware oraz innymi atakami. A wszystko to bez obciążania Twojego czasu oraz budżetu, ponieważ wiemy, jak ograniczone mogą być zasoby firm.

Idealny dla firm poszukujących natychmiastowej i łatwej w użyciu ochrony opartej na chmurze

Korzyści dla firm

-  Krótszy czas uzyskania ochrony
-  **Brak konieczności inwestycji kapitałowych**
-  Uwolnienie Twoich zasobów IT
-  **Płacisz w miarę rozwoju firmy**
-  Umożliwia outsourcing

Zalety

- Ochrona działalności bez przeznaczania na to ogromnych zasobów IT, czasu czy budżetu
- Zautomatyzowane rozwiązanie umożliwiające zmniejszenie kosztów IT oraz uwolnienie zasobów

1 Wymagane umiejętności

2 Dostosowanie do indywidualnych potrzeb i skalowalność

1.5 Koszt



Kaspersky Endpoint Security for Business

w chmurze lub lokalnie

Kaspersky Endpoint Security for Business jest przeznaczony dla mieszanych środowisk IT i zawiera elastyczną konsolę WWW wraz z pełnym wachlarzem sprawdzonych technologii. Oprócz zabezpieczenia wszystkich Twoich punktów końcowych oraz serwerów zapewnia adaptacyjne warstwy ochrony dla danych wrażliwych.

Idealny dla organizacji posiadających bardziej rozbudowane potrzeby w zakresie bezpieczeństwa IT



Wymagane
umiejętności



Dostosowanie do
indywidualnych
potrzeb
i skalowalność



Koszt

Korzyści dla firm



Łatwe skalowanie **bez ograniczeń**



Szczegółowe profile ochrony
uwzględniające firmy dowolnego rozmiaru



Działa natywnie z Twoimi systemami



Masz kontrolę nad wszystkimi ustawieniami



Konsola w chmurze bez dodatkowych kosztów

Zalety

- Pełna ochrona przed nawet najbardziej zaawansowanymi zagrożeniami
- Dostosowuje się do Twoich unikatowych potrzeb biznesowych
- Zabezpiecza przed narażeniem organizacji na atak przez pracowników
- Dzięki uproszczeniu automatyzacji rutynowych zadań pozwala skoncentrować się na innych rzeczach



Ochrona dla punktów końcowych wspierana przez EDR rozwiązanie

Niedobór specjalistów raczej nie ulegnie szybko zmniejszeniu, tymczasem ryzyko prawdziwego ataku ukierunkowanego rośnie. Na szczęście nasz ściśle zintegrowany proaktywny system cyberochrony zapewnia szybką i bezproblemową analizę. Widoczność punktów końcowych i zautomatyzowana ocena umożliwiają skupienie się tylko na tych atakach, które stanowią największe zagrożenie — czyli na atakach ukierunkowanych. Wielokrotnie nagradzana ochrona punktów końcowych, zautomatyzowana piaskownica i ujednoczona ochrona w chmurze wraz z technologią EDR zapewniają skuteczną ochronę Twojej firmy.

**Idealny dla organizacji,
które chcą być chronione
przed zaawansowanymi
ukierunkowanymi atakami,
przy ograniczonych zasobach
bezpieczeństwa IT**

Korzyści dla firm



Stosuje **wiele warstw ochrony**, aby zapobiegać zakłóceniom w działaniu i szkodom w firmie



Najwyższe współczynniki ochrony przy minimalnym udziale ze strony człowieka



Umożliwia szybkie i łatwe **zmniejszenie możliwości wykonania przez personel** działań narażających firmę na atak



Maksymalizuje współczynnik zwrotu z inwestycji bez zwiększania kosztów w postaci nakładu pracy człowieka

Przykłady użycia

- Automatycznie wykrywa i reaguje na ataki ukierunkowane oraz unikające wykrycia zagrożenia na wszystkich chronionych punktach końcowych
- Rozpoznaje i blokuje nietypowe zachowanie użytkownika
- Umożliwia przeprowadzanie analizy podstawowych przyczyn incydentów i polowanie na podstawowe zagrożenia
- Zapewnia całkowity wgląd w aktualny stan ochrony



Kaspersky EDR Optimum

Rozwiązanie Kaspersky EDR Optimum uzupełnia nasz flagowy produkt Kaspersky Endpoint Security for Business o możliwości EDR. Zapewnia najskuteczniejszą ochronę przed zagrożeniami złożonymi i analizuje podstawowe przyczyny wystąpienia incydentów. Specjaliści ds. bezpieczeństwa IT otrzymują informacje oraz szczegóły potrzebne do przeprowadzenia skutecznej analizy, polowania na zagrożenia w podstawowym zakresie, jak również szybkiej i dokładnej reakcji na incydenty (np. umieszczanie plików w kwarantannie, izolacja hostów, zatrzymywanie procesów, usuwanie obiektów itd.).

Idealny dla

Firm, w których za funkcje bezpieczeństwa IT odpowiada dział IT

Małych organizacji, które nie planują angażowania dodatkowych zasobów w bezpieczeństwo IT, ale chcą wiedzieć, co dzieje się w ich sieciach



Wymagane umiejętności



Dostosowanie do indywidualnych potrzeb i skalowalność



Koszt

Korzyści dla firm



Zmniejszanie ryzyka ze strony cyberzagrożeń



Poprawa ogólnego **poziomu bezpieczeństwa IT** przy jednoczesnym utrzymaniu wartości z poprzednich inwestycji



Skrócony czas analizy i reagowania na incydenty



Zaawansowana i pełna ochrona infrastruktury **punktów końcowych**

Przykłady użycia

- Automatyczne wykrywanie i eliminowanie zaawansowanych zagrożeń
- Analiza podstawowych przyczyn wystąpienia incydentów
- Udostępnianie analitykom pełnego obrazu ataku poprzez dostarczanie wszystkich informacji potrzebnych do szybkiego działania
- Pobieranie zewnętrznych wskaźników włamania na potrzeby skanowania infrastruktury w czasie rzeczywistym
- Scentralizowana reakcja na wszystkich zagrożonych punktach końcowych



Kaspersky Sandbox

Dzisiejsze przedsiębiorstwa muszą chronić się przed coraz większą liczbą zagrożeń, które są coraz bardziej skomplikowane i potrafią omijać istniejące rozwiązania klasy EPP. Jednocześnie na świecie brakuje wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa, więc zatrudnienie takich osób może być trudne i kosztowne. Wobec tego firmy szukają sposobów na to, aby w jak największym stopniu zautomatyzować wykrywanie i reagowanie na zaawansowane zagrożenia. Uzupełniając funkcjonalność Kaspersky Endpoint Security for Business, Kaspersky Sandbox zapewnia automatyczną reakcję na nieznane zagrożenia, omijające zastosowane bariery bezpieczeństwa.

Idealny dla

Firm, w których funkcje bezpieczeństwa IT są przypisane do działu IT

Małych organizacji, które nie planują angażowania dodatkowych zasobów bezpieczeństwa IT





Geograficznie rozproszonych sieci bez specjalistów w dziedzinie bezpieczeństwa

1 Wymagane umiejętności

4 Dostosowanie do indywidualnych potrzeb i skalowalność

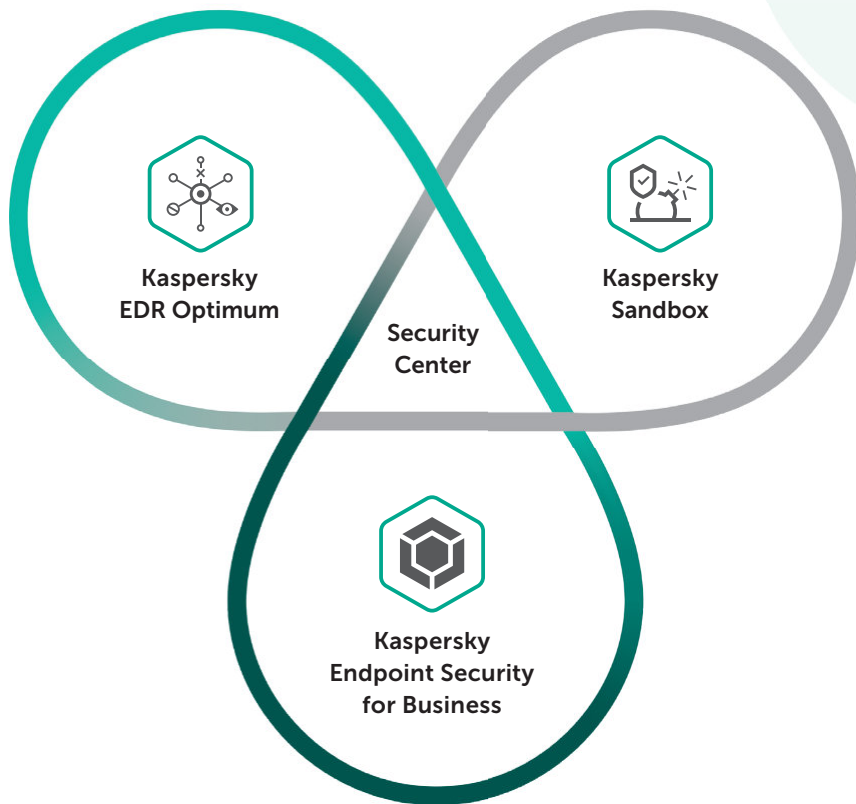
2 Koszt

Korzyści dla firm

-  Zmniejsza zagrożenia dla bezpieczeństwa IT i **zapewnia ciągłość działania firmy**
-  Chroni przed zaawansowanymi zagrożeniami **bez wpływu** na wydajność punktu końcowego i produktywność użytkowników
-  Minimalizuje koszty pracy dzięki **zmniejszeniu liczby operacji wykonywanych ręcznie**
-  Optymalizuje koszty zaawansowanej ochrony przed zagrożeniami **w biurach zdalnych**

Przykłady użycia

- Umożliwia dogłębną analizę dynamiczną i wykrywanie nieznanych i unikających wykrycia zagrożeń
- Zapewnia automatyczną reakcję na wszystkich chronionych punktach końcowych
- Skutecznie chroni serwery terminali o dużym obciążeniu
- Integruje się z rozwiązaniami innych firm za pośrednictwem interfejsu API



- ✓ **Pojedynczy agent**
- ✓ **Jedna konsola**
- ✓ **Scentralizowane zarządzanie**
(lokalne i w chmurze)
- ✓ **Maksymalna automatyzacja**
- ✓ **Najlepsze podejście do ochrony**



Kaspersky Security for Microsoft Office 365

oparty na chmurze

Kaspersky Security for Microsoft Office 365 to najpopularniejszy wybór jeśli chodzi o ochronę działalności zorientowanej na chmurę przed znanymi i nieznanymi zagrożeniami rozprzestrzeganymi za pośrednictwem wiadomości e-mail. Natychmiast powstrzymuje rozprzestrzenianie phishingu, oprogramowania ransomware, szkodliwych załączników, spamu oraz ataków wykorzystujących zainfekowane wiadomości biznesowe (BEC), a jego instalacja i obsługa nie wymaga specjalistycznych umiejętności IT.

Idealny dla użytkowników Microsoft Office 365 poszukujących dodatkowej warstwy ochrony

2 Wymagane umiejętności

2 Dostosowanie do indywidualnych potrzeb i skalowalność

1 Koszt

Korzyści dla firm



Zaawansowana ochrona firmowych skrzynek pocztowych, na której możesz polegać



Nie wpływa na produktywność użytkownika – brak opóźnień w dostarczeniu oraz czasu oczekiwania na przestanie wiadomości e-mail



Brak zgubionych wiadomości e-mail



Zgodność z **RODO**

Zalety

Zaawansowana ochrona rozwiązania Microsoft Office 365 nawet dla użytkowników nieposiadających wiedzy w zakresie bezpieczeństwa.



Kaspersky Automated Security Awareness Platform

oparty na chmurze

Kaspersky ASAP umożliwił zmianę zachowania pracowników poprzez wyposażenie ich w umiejętności ochrony firmy i pomaga stworzyć środowisko cybernetyczne, w którym każdy jest bezpieczny. ASAP opiera się na zasadach nauki interwałowej z ciągłym wzmacnianiem w celu rozwinięcia „percepcji schematów”: pracownicy potrafią rozpoznać nowe zagrożenia i zachowywać się w sposób bezpieczny nawet po zetknięciu się z nieznanymi zagrożeniami.

Idealny dla wszystkich rodzajów organizacji, zwłaszcza tych zainteresowanych szybką konfiguracją programu oraz nieskomplikowanym zarządzaniem



1 Wymagane umiejętności



4 Dostosowanie do indywidualnych potrzeb i skalowalność



4 Koszt

Korzyści dla firm



Nauka przyrostowa poprzez **lekcje oparte na rozwijaniu umiejętności**: pracownicy każdego dnia nabywają nową umiejętność



Automatyczne zarządzanie nauką **pozwała zaoszczędzić setki godzin** zarządzania platformą **każdego roku**



Wszystkie lekcje mają związek z **codziennym życiem zawodowym pracowników**



Zgodność z **RODO**

Zalety

Tworzy „ludzką zaporę sieciową” w celu zabezpieczenia firmy od środka.



Kaspersky Managed Service Providers Program

Nasza oferta ochrony dla dostawców usług zarządzanych (MSP) obejmuje elastyczne, rozbudowane narzędzia służące do zabezpieczenia, monitorowania oraz zarządzania infrastrukturą klienta – wszystko z poziomu jednej, łatwej do zarządzania konsoli. Dostarczaj rozwiązania cyberbezpieczeństwa nowej generacji do infrastruktury fizycznej i wirtualnej swoich klientów, lokalnie bądź z chmury.

Idealny dla dostawców usług zarządzanych zorientowanych na oferowanie wysokiej jakości usług bezpieczeństwa IT

Korzyści dla firm

Dzięki możliwościom wielodostępności nasze lekkie a zarazem skuteczne narzędzia umożliwiają wdrożenie oraz zarządzanie rozwiązaniami bezpieczeństwa dla **wszystkich Twoich klientów** z jednej konsoli, bez konieczności posiadania dodatkowego sprzętu.

Integracja

Nasze rozwiązania bezpieczeństwa są zintegrowane z najpopularniejszymi platformami RMM oraz PSA:

- ConnectWise® Automate™
- ConnectWise® Manage™
- Autotask®
- Tigerpaw® One
- SolarWinds® N-central®

Obsługiwane produkty

Kaspersky Endpoint Security for Business Advanced

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security Cloud

Kaspersky Security for Microsoft Office 365

Kaspersky Hybrid Cloud Security

Kaspersky Automated Security Awareness Platform (ASAP)

Dlaczego warto wybrać rozwiązania marki Kaspersky



Najczęściej testowane. Najczęściej nagradzane

Nasze produkty więcej razy zajęły pierwsze miejsce w niezależnych testach niż rozwiązania jakiegokolwiek innego dostawcy bezpieczeństwa. I jesteśmy w tym konsekwentni. Każdego roku. www.kaspersky.pl/top3



Jedne z najbardziej polecanych

Firma Kaspersky po raz kolejny zdobyła tytuł „Wybór Klientów w zakresie platform ochrony punktów końcowych” w raporcie Gartner Peer Insights, uzyskawszy wysoki współczynnik zadowolenia klientów na poziomie 4,6 przy maksymalnym wyniku 5 (27 listopada 2019 r.)*



Firma Kaspersky została uznana liderem w zestawieniu Forrester

Firma Kaspersky otrzymała tytuł lidera w zestawieniu The Forrester Wave™: Endpoint Security Suites, Q3 2019.



Najbardziej transparentny

Nasze Centra Transparentności już działają, a przetwarzanie danych statystycznych odbywa się w Szwajcarii. Dzięki temu gwarantujemy suwerenność Twoich danych w większym stopniu niż inni dostawcy rozwiązań.

*Gartner Peer Insights Customers' Choice obejmuje obiektywne opinie zawarte w recenzjach indywidualnych użytkowników końcowych, oceny oraz dane wykorzystane zgodnie z udokumentowaną metodologią; nie stanowią one opinii ani poparcia firmy Gartner lub jej podmiotów zależnych.

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.

Skontaktuj się z nami

Kaspersky dla biznesu: www.kaspersky.pl/biznes

Ochrona dla korporacji: www.kaspersky.pl/korporacje

Oficjalny blog: www.kaspersky.pl/blog

#aktywujprzyszlosc

www.kaspersky.pl

© 2020 AO Kaspersky Lab. Wszelkie prawa zastrzeżone.

Zarejestrowane znaki handlowe i usługowe stanowią własność ich stosownych właścicieli.

kaspersky

**Aktywuj
przyszłość**

www.kaspersky.pl