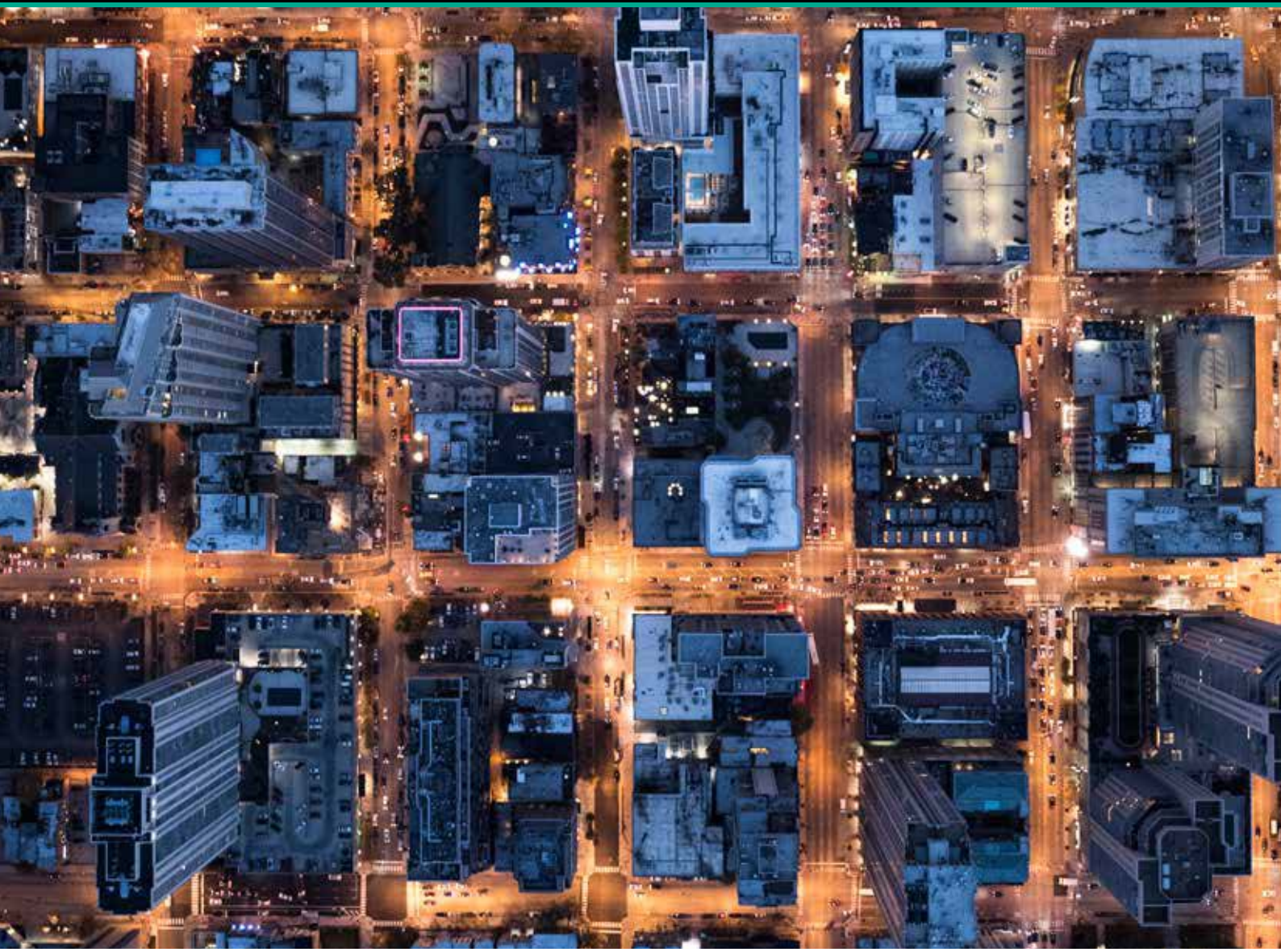

Kaspersky Endpoint Security for Business

Kaspersky Endpoint Security for Business to zaprojektowane przez czołowych ekspertów w branży bezpieczeństwa IT rozwiązanie oferujące wielowarstwową ochronę przed znanymi, nieznanymi i zaawansowanymi cyberzagrożeniami. Nasze unikatowe połączenie rozległej wiedzy o zagrożeniach, uczenia maszynowego i ludzkiej ekspertyzy umożliwia wdrożenie skutecznej i wydajnej ochrony przed wszelkimi zagrożeniami — niezależnie od platform stosowanych w firmowej sieci.

Więcej informacji na kaspersky.pl.

Kaspersky®
Endpoint Security
for Business

Kaspersky Endpoint Security for Business | Select

Skuteczne cyberbezpieczeństwo dla firm o dowolnym rozmiarze

Kaspersky Endpoint Security for Business Select oferuje efektywną, wielowarstwową ochronę przed wszelkimi rodzajami cyberzagrożeń w ramach jednego, łatwego w zarządzaniu i skalowalnego rozwiązania. Funkcje kontroli aplikacji, urządzeń oraz wykorzystania internetu zwiększają możliwości zarządzania bez konieczności inwestowania w nowe zasoby, a zarządzanie urządzeniami mobilnymi rozszerza bezpieczeństwo na firmowe smartfony i tablety.

OCHRONA PRZED CYBERZAGROŻENIAMI DLA FIRM

Skuteczna i efektywna ochrona	Nasze technologie muszą na co dzień skutecznie walczyć z wszelkimi rodzajami cyberzagrożeń. W tym celu stosujemy unikatowe połączenie rozległej wiedzy o zagrożeniach, uczenia maszynowego i ludzkiej ekspertyzy — HuMachine.
Proaktywne i wyspecjalizowane technologie bezpieczeństwa	Oferujemy najlepsze w swojej klasie zabezpieczenie przed szkodliwym oprogramowaniem wraz z technologią „Automatyczne zapobieganie exploitom" oraz wsparciem chmury Kaspersky Security Network, która gwarantuje dostęp do informacji o najświeższych zagrożeniach w czasie rzeczywistym. Szkodliwe działania i destrukcyjne zachowania wskazujące na obecność cyberzagrożeń są blokowane przez moduł „Kontrola systemu", a system zapobiegania włamaniom (HIPS) wraz z zaporą sieciową pomagają w zabezpieczeniu i kontrolowaniu aktywności aplikacji oraz sieci.

SZEROKI WACHLARZ FUNKCJI KONTROLI I ZARZĄDZANIA

Kontrola aplikacji	Kontrola aplikacji z dynamiczną białą listą pozwala administratorom blokować, kontrolować i zezwalać na działanie aplikacji, łącznie z możliwością zastosowania trybu domyślnej odmowy w środowisku produkcyjnym lub testowym. Kontrola uprawnień aplikacji umożliwia ograniczanie dostępu oprogramowania do określonych plików i zasobów systemu.
Kompletny wgląd w ochronę i wydajne zarządzanie	Zestaw narzędzi kontrolujących użycie łączy internetowych pozwala monitorować oraz definiować zasady korzystania z zasobów online w firmie, z uwzględnieniem zestawu predefiniowanych kategorii stron WWW. Funkcje kontroli mogą zostać skorelowane z usługą Active Directory, co pozwala na ułatwienie procesu zarządzania i definiowania polityk.
Efektywna kontrola wszystkich urządzeń w firmie	Rozwiązanie umożliwia zdefiniowanie zasad kontroli dostępu przenośnych nośników danych i innych urządzeń peryferyjnych do sieci firmowej. Kontrolowany jest także dostęp do urządzeń rejestrujących dźwięk i obraz. Ponadto Kaspersky Endpoint Security for Business rejestruje zdarzenia związane z usuwaniem i kopiowaniem na wymiennych urządzeniach USB, a także zarządza uprawnieniami użytkowników do odczytywania i zapisywania plików na płytach CD/DVD.

OCHRONA SERWERA PLIKÓW

Efektywna i wydajna ochrona przed szkodliwymi programami oraz ransomware	Ochrona serwerów plików (kontrolowana wraz z zabezpieczeniami dla punktów końcowych z poziomu konsoli Kaspersky Security Center) obsługuje wszystkie popularne platformy serwerowe przy minimalnym wpływie na wydajność.

OCHRONA URZĄDZEŃ MOBILNYCH

Wielowarstwowa ochrona urządzeń mobilnych w czasie rzeczywistym	Firmowe urządzenia mobilne są chronione z użyciem zaawansowanych, proaktywnych technologii bezpieczeństwa wspieranych chmurą Kaspersky Security Network. Rozwiązanie zapobiega nieautoryzowanemu dostępowi do danych firmowych, a na wypadek kradzieży lub zgubienia urządzeń dostępne są narzędzia zdalnej administracji.

EFEKTYWNE I SZCZEGÓŁOWE ZARZĄDZANIE OCHRONĄ

Scentralizowane zarządzanie bezpieczeństwem IT	Zarządzanie ochroną rosnącej liczby urządzeń w firmie może być skomplikowane i czasochłonne. Dzięki Kaspersky Security Center — naszej zintegrowanej konsoli — administrator może kontrolować wszystkie technologie bezpieczeństwa Kaspersky Lab z jednego miejsca, co znacznie ułatwia proces zarządzania. Z myślą o mniejszych firmach przygotowaliśmy szereg predefiniowanych zestawów zasad, dzięki czemu możliwe jest błyskawiczne wdrożenie ochrony w sieci i natychmiastowe korzystanie ze skutecznej ochrony bez dodatkowej konfiguracji. Jeżeli jednak administrator potrzebuje większej swobody w ustalaniu reguł ochrony, będzie miał do dyspozycji szeroki wachlarz opcji, które pozwolą dopasować bezpieczeństwo do potrzeb firmy.
Możliwość rozszerzenia funkcjonalności w miarę potrzeb	W celu zwiększenia skuteczności ochrony i usprawnienia zarządzania można rozbudować rozwiązanie Kaspersky Endpoint Security for Business Select o **wyszukiwanie luk w zabezpieczeniach** i **zarządzanie łatami**. Istnieje także możliwość rozbudowania pakietu o **technologię szyfrowania**, która zabezpiecza cenne dane w przypadku awarii sprzętu i oprogramowania, kradzieży urządzeń czy ataku ukierunkowanego.

Kaspersky Endpoint Security for Business | Advanced

Połączenie bezpieczeństwa i wydajności infrastruktury IT

Kaspersky Endpoint Security for Business Advanced łączy bezpieczeństwo i wydajność infrastruktury IT, oferując proaktywną i skuteczną ochronę danych przed cyberzagrożeniami dla firm dowolnych rozmiarów. Rozbudowane możliwości administracji ułatwiają zarządzanie i kontrolowanie wszystkimi zagadnieniami związanymi z ochroną z jednego miejsca, bez potrzeby inwestowania w dodatkowe rozwiązania.

MINIMALIZACJA RYZYKA ATAKU

Rozszerzone bezpieczeństwo	Funkcje oceny luk i zarządzania łatami w systemach operacyjnych oraz aplikacjach automatyzują proces usuwania podatności na ataki. Wykryte luki są klasyfikowane według priorytetu, co umożliwia automatyczne instalowanie poprawek i aktualizacji. Pozwala to na minimalizację prawdopodobieństwa wykorzystania luk przez szkodliwe oprogramowanie.
Błyskawiczne wykrywanie i neutralizowanie luk	Skanowanie w poszukiwaniu luk pozwala na błyskawiczne wykrywanie podatności na ataki. Skanowanie może być realizowane automatycznie lub zgodnie ze zdefiniowanym terminarzem — w zależności od wymagań administratora.

ZWIĘKSZENIE EFEKTYWNOŚCI ZARZĄDZANIA SYSTEMAMI

Oszczędność czasu dzięki dystrybucji i rozwiązywaniu problemów z oprogramowaniem	Zdalne rozsyłanie oprogramowania (łącznie z systemami operacyjnymi) oraz aktualizacji może być realizowane w trybie automatycznym lub zgodnie ze zdefiniowanym terminarzem, z uwzględnieniem metody Wake-on-LAN. Zastosowanie technologii Multicast pozwala na zdalne rozwiązywanie problemów oraz wydajną dystrybucję oprogramowania.
Łatwa instalacja systemów operacyjnych	Łatwe tworzenie, przechowywanie i rozsyłanie obrazów systemów operacyjnych z centralnego magazynu, łącznie z obsługą interfejsu UEFI.
Monitoring w czasie rzeczywistym, łącznie z integracją z systemami SIEM	Dzięki integracji z najpopularniejszymi produktami do zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego (SIEM) — takimi jak HP ArcSight i IBM QRadar — nasz pakiet zabezpieczeń umożliwia firmom monitorowanie przepływu danych w czasie rzeczywistym.

OCHRONA POUFNYCH DANYCH BIZNESOWYCH

Skuteczna ochrona danych	Metoda szyfrowania na poziomie całych dysków (FDE) operuje na sektorach dysku twardego, aby zapewnić szyfrowanie na poziomie zbliżonym do sprzętowego i ułatwić prowadzenie strategii szyfrowania wszystkiego jednocześnie. Metoda szyfrowania na poziomie plików (FLE) umożliwia bezpieczne udostępnianie danych w sieci. Po zaszyfrowaniu pliku jego pierwotna, niezaszyfrowana wersja może zostać usunięta z dysku. W celu zabezpieczenia danych przechowywanych na nośnikach zewnętrznych mogą one zostać zaszyfrowane metodą FDE lub FLE.

Łatwiejsze logowanie się użytkowników	Po uruchomieniu komputera przez użytkownika i zalogowaniu się za pomocą nazwy i hasła funkcja pojedynczego logowania zapewnia mu natychmiastowy dostęp do zaszyfrowanych plików znajdujących się na dysku twardym komputera. Dzięki temu procesy szyfrowania i deszyfrowania są dla użytkownika niemal transparentne, co zwiększa efektywność i wydajność pracy. Obsługiwane jest także uwierzytelnianie dwupoziomowe przy użyciu kart inteligentnych i tokenów.
Unikatowe, zintegrowane narzędzia do definiowania zasad	Unikatowa integracja szyfrowania z kontrolą aplikacji oraz urządzeń stanowi dodatkową warstwę ochrony i znacznie ułatwia zarządzanie.
Zwiększona kompatybilność z urządzeniami i minimalny wpływ na komfort pracy	Szyfrowanie dysków twardych na urządzeniach z systemem Microsoft Windows może być realizowane z użyciem rozwiązania Microsoft BitLocker. Obsługa tego rozwiązania z poziomu konsoli administracyjnej Kaspersky Lab pozwala na łatwe wykorzystanie tej technologii wbudowanej w system operacyjny.

Kaspersky Endpoint Security for Business Advanced obejmuje wszystkie komponenty warstwy Select.

Kaspersky Total Security for Business

Najskuteczniejsze rozwiązanie oferujące bezpieczeństwo każdego aspektu firmy

To najbardziej kompleksowe rozwiązanie zabezpieczające firmy Kaspersky Lab dla biznesu, które zapewnia skuteczną ochronę sieci informatycznej firmy. Pakiet ten nie tylko zabezpiecza komputery stacjonarne, laptopy i serwery plików, zapewniając algorytmy szyfrowania danych, mechanizmy kontroli punktów końcowych i funkcje ochrony urządzeń mobilnych, ale także zawiera specjalne technologie ochrony serwerów poczty elektronicznej i środowisk współpracy oraz sterowania przepływem danych przez bramy internetowe. W jego skład wchodzą także rozbudowane narzędzia do zarządzania systemami, które automatyzują szeroką gamę zadań administracyjnych, oszczędzając w ten sposób czas i zasoby.

KOMPLETNA OCHRONA SERWERA POCZTOWEGO

Dzięki zastosowaniu aktualizacji dostarczanych w czasie rzeczywistym z użyciem chmury nasze rozwiązanie skutecznie chroni ruch e-mail przed szkodliwym oprogramowaniem i spamem, przy minimalnej liczbie fałszywych alarmów. Rozwiązanie obsługuje szeroki zakres serwerów pocztowych. Kaspersky Total Security for Business pozwala także na skonfigurowanie wyspecjalizowanej bramy pocztowej. Dodatkowo istnieje możliwość rozbudowania funkcjonalności o ochronę przed wyciekiem danych (DLP) dla serwera Microsoft Exchange.

OCHRONA BRAM INTERNETOWYCH

Bezpieczny ruch	Nasze technologie bezpieczeństwa chronią ruch przepływający przez najpopularniejsze bramy (oparte na systemach Windows lub Linux), automatycznie usuwając szkodliwe i potencjalnie niebezpieczne programy pojawiające się w strumieniu danych HTTP(S), FTP, SMTP oraz POP3.
Ochrona poczty	Pakiet Kaspersky Total Security for Business oferuje ochronę firmowej poczty przesyłanej przez bramy Microsoft Forefront TMG i serwery Microsoft ISA Server.
Wysoka skuteczność wykrywania bez negatywnego wpływu na wydajność	Dzięki zoptymalizowanym funkcjom inteligentnego skanowania oraz mechanizmom równoważenia obciążenia rozwiązanie zapewnia wysoką skuteczność wykrywania zagrożeń bez znaczącego obciążania systemów.

BEZPIECZNA WSPÓŁPRACA

Serwery współpracy oferują wysoką produktywność, jednak podobnie jak inne zasoby IT — wymagają ochrony. Nasze funkcje ochrony platformy SharePoint przed szkodliwymi programami oraz mechanizmy filtrowania treści i plików umożliwiają skuteczne egzekwowanie firmowych zasad współpracy i zapobiegają przechowywaniu nieodpowiednich materiałów w sieci korporacyjnej. Funkcje ochrony przed utratą danych uwzględniające zawartość są dostępne jako opcja.

Kaspersky Total Security for Business obejmuje wszystkie komponenty warstw Advanced oraz Select.

Prawdziwe cyberbezpieczeństwo to część naszego DNA

Kaspersky Lab oferuje najefektywniejsze rozwiązania do ochrony przed szkodliwym oprogramowaniem. Jest to możliwe dzięki eksperckiej wiedzy o cyberzagrożeniach, która stanowi część naszego DNA, wpływa na wszystko, co robimy, i na sposób, w jaki to robimy. Dzięki temu, że jesteśmy niezależną firmą, możemy działać szybciej, sprawniej i myśleć nieszablonowo.

- **Ekspercka wiedza przejawia się w Kaspersky Lab na wszystkich szczeblach**, począwszy od dyrektora generalnego — Jewgienija Kasperskiego.
- **Wszystkie nasze technologie rozwijamy i udoskonalamy wewnętrznie**, dzięki czemu nasze produkty są maksymalnie stabilne i wydajne. Dział badawczo-rozwojowy stanowi trzon firmy.
- **Nasz Globalny Zespół ds. Badań i Analiz (GReAT)** składa się z czołowych badaczy ds. cyberbezpieczeństwa na świecie, którzy ujawnili i zbadali wiele najniebezpieczniejszych cyberataków. Zespół GReAT poświęca się także rozwojowi i innowacjom w zakresie technologii walki ze szkodliwym oprogramowaniem.
- Jesteśmy **partnerem globalnych** organizacji walczących z cyberprzestępczością, łącznie z Interpolem i Europolem.
- Nasi klienci otrzymują najwyższą jakość ochrony potwierdzoną w niezależnych testach. **Produkty Kaspersky Lab to najczęściej testowane i najczęściej wyróżniane rozwiązania bezpieczeństwa na rynku.**
- Chronimy ponad 400 milionów użytkowników w 140 krajach na całym świecie.
- **Profesjonalne organizacje zajmujące się analizą rynku** — Gartner, Inc., Forrester Research oraz International Data Corporation (IDC) — uznały nas za lidera w wielu kluczowych kategoriach związanych z bezpieczeństwem IT. W 2017 r. Kaspersky Lab został po raz szósty z rzędu uznany za lidera w raporcie Magic Quadrant Gartnera.
- Naszym technologiom zaufało wiele czołowych firm technologicznych, m.in. Microsoft, Cisco, Juniper oraz TrustWave.

www.kaspersky.pl

© 2017 AO Kaspersky Lab. Wszelkie prawa zastrzeżone. Zarejestrowane znaki towarowe i nazwy usług należą do ich właścicieli.