KASPERSKY lab

Nowa generacja ochrony punktów końcowych

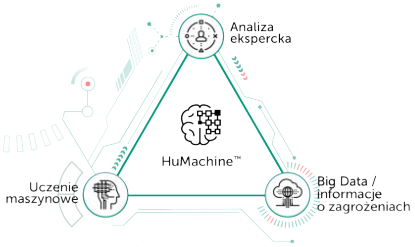
www.kaspersky.pl/biznes
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Ochrona jako element strategii ciągłości działania firmy

Technologia wymusza na firmach transformację – albo za nią nadążasz, albo popadasz w stagnację. Jednak otwiera ona również drzwi cyberprzestępcom, a także jest stanowi główny cel ataków i jest źródłem wielu problemów. Tylko w zeszłym roku ponad 38% firm ucierpiało w wyniku cyberataku, a 39% ataków wymierzonych w zabezpieczone punkty końcowe przebiegło pomyślnie. W środowisku tym firmy muszą być sprytniejsze niż atakujący ich cyberprzestępcy.

Dopóki za cyberatakami będą stali ludzie, do przeciwdziałania im nadal potrzebny jest intelekt człowieka oraz innowacyjne technologie. Ochrona od Kaspersky Lab wykorzystuje globalną analizę zagrożeń oraz algorytmy uczenia maszynowego opierające się na doświadczeniu najlepszych specjalistów w branży. Ta unikatowa kombinacja, zwana HuMachine™, jest kluczowym elementem produktów Kaspersky Lab.



W 2017 roku firma Kaspersky Lab otrzymała nagrodę **Platinum Customer Award** w ramach plebiscytu **Gartner Peer Insights for Endpoint Protection Platforms**. W 90% niezależnych testów i recenzji produkty firmy do ochrony punktów końcowych plasowały się na podium - to więcej niż w przypadku jakiegokolwiek rozwiązania konkurencyjnego.

Inwestuj w przyszłość

Przeciętnie jeden wyciek danych wywołuje u małych i średnich firm straty finansowe rzędu 86,5 tys. dolarów, a w przypadku dużych przedsiębiorstw kwota ta sięga nawet 992 tys. dolarów. Antywirus nowej generacji już nie wystarczy – odpowiedni poziom ochrony może zapewnić tylko wielowymiarowe rozwiązanie zabezpieczające firmową infrastrukturę IT na wielu warstwach technologicznych i funkcjonalnych. Prawdziwa ochrona dla punktów końcowych łączy wiele różnych inteligentnych mechanizmów i technologii, aby chronić firmy przed wszelkiego rodzaju zagrożeniami, a także nadaje się dla każdej platformy. Chroniąc całą sieć IT, dbasz o ciągłość działania swojej firmy.

Chroń to, co najcenniejsze, dzięki rozwiązaniom wykorzystującym technologię HuMachine™

Każda rozwijająca się firma ma ograniczony budżet na ochronę IT. Aby pokonywać wyzwania aktualne nie tylko dziś, ale i jutro, należy optymalizować zasoby. Kaspersky Endpoint Security for Business wykorzystuje analizę HuMachine™ do zapewniania ochrony przed oprogramowaniem ransomware, exploitami i najbardziej zaawansowanymi cyberzagrożeniami. Rozwiązanie optymalnie wykorzystuje zasoby, jest wyposażone w skuteczne narzędzia do ochrony, opcję automatycznego zarządzania lukami i łatami, zintegrowane szyfrowanie, a także może być sterowane z poziomu pojedynczej konsoli obejmującej całą sieć firmową.

Elastyczne zabezpieczenia adaptujące się do środowiska

Rozwiązanie może działać w dowolnym środowisku IT. Wykorzystuje pełen wachlarz technologii nowej generacji o udowodnionej skuteczności. Wbudowane sensory i integracja z rozwiązaniami Endpoint Detection and Response (EDR) umożliwia przechwytywanie i analizę dużych ilości danych, co pozwala wykrywać najbardziej zamaskowane i wyrafinowane cyberataki.

Gotowa na przyszłość ochrona zewnętrznych usług IT

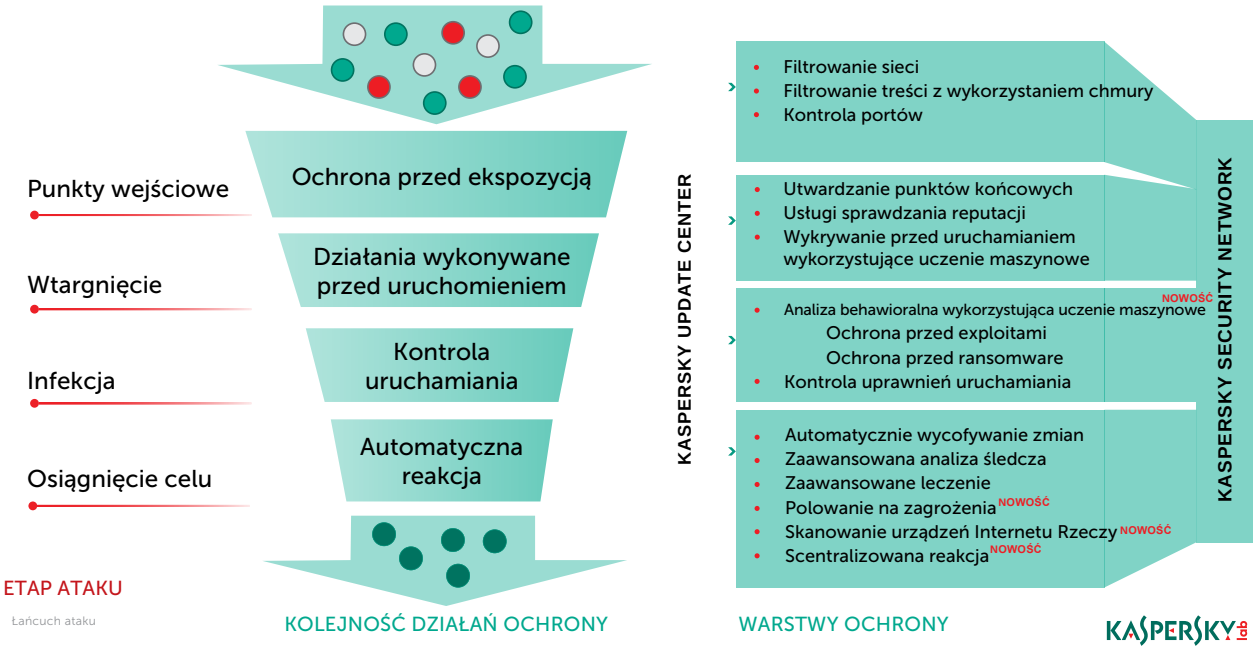
Wbudowana obsługa wielu podmiotów, ochrona przed zagrożeniami, ochrona urządzeń mobilnych, szyfrowanie danych oraz zarządzanie lukami i łatami — wszystko to sprawia, że dostawcy usług zarządzanych (ang. Managed Service Provider, MSP) mogą oferować swoim klientom bogatszą ofertę ochrony IT.

Niskie obciążenie; wysoka wydajność

Najczęściej testowana i najczęściej nagradzana ochrona wykorzystująca HuMachine™ zapewnia optymalną ochronę przy minimalnym wpływie na zasoby komputerów PC. Ponieważ komponenty bezpieczeństwa nie wykorzystują sygnatur, zagrożenia są wykrywane nawet w sytuacji, gdy częstotliwość pobierania aktualizacji jest ograniczona.

Wszechstronna ochrona

Rozwiązanie **Kaspersky Endpoint Security for Business** wykorzystuje różne technologie nowej generacji (np. wzmacnianie punktów końcowych, analiza behawioralna przy użyciu uczenia maszynowego, ochrona przed exploitami) w celu neutralizowania większości zagrożeń, zanim zaatakują one głębsze warstwy zabezpieczające. Podejrzane pliki są wykrywane i blokowane, zanim dotrą do punktu końcowego.



Połączenie zaawansowanych technologii i stosowanie wielu warstw pozwala osiągnąć równowagę między wydajnością a skuteczną ochroną. Ma to kluczowe znaczenie w produktach Kaspersky Lab, które wykazują jeden z najwyższych w branży współczynnik wykrywania, co nieustannie potwierdzają niezależne testy.

Ochrona wielowarstwowa dla:
- platformy Windows, Linux oraz Mac,
- urządzeń mobilnych,
- pamięci przenośnych,
- serwerów Windows i Linux,
- serwerów pocztowych,
- bram internetowych,
- Serwerów współpracy.

Niezrównana ochrona przed:
- exploitami,
- oprogramowaniem ransomware,
- mobilnymi szkodliwymi programami,
- nieznanymi zagrożeniami,
- zagrożeniami bezplikowymi,
- atakami wykorzystującymi skrypty typu PowerShell,
- zagrożeniami płynącymi z internetu,
- zagrożeniami dystrybuowanymi przez pocztę e-mail,
- atakami phishingowymi,
- spamem.

Ochrona przed ransomware i exploitami

Dzięki wykorzystywaniu uczenia maszynowego oraz najlepszych źródeł umożliwiających analizę zagrożeń w czasie rzeczywistym technologie Kaspersky Lab nieustannie ewoluują. Chroń swoje punkty końcowe przed najnowszymi exploitami i zabezpiecz swoje dane i foldery współdzielone przed zaawansowanymi zagrożeniami i ransomware.

Ochrona przed przechwytywaniem kont

Moduł Wykrywanie zachowań stosuje mechanizm Ochrona pamięci, który zabezpiecza krytyczne dla systemu procesy i zapobiega wyciekowi danych logowania należących do użytkowników i administratora.

Mniejsza ekspozycja na atak poprzez aplikacje

Moduł Kontrola aplikacji wspierany funkcją Dynamiczne tworzenie białych list znacząco zmniejsza narażenie na ataki dnia zerowego poprzez zapewnienie całkowitej kontroli nad oprogramowaniem uruchamianym na komputerach stacjonarnych i serwerach. Moduł Kontrola aplikacji przechwytuje uruchamianie plików wykonywalnych, bibliotek DLL i skryptów wykonywanych przez inne programy. Moduły Wykrywanie zachowań i Ochrona przed exploitami monitorują zachowanie aplikacji, blokują potencjalnie szkodliwe działania, jak również chronią dostęp do legalnych aplikacji oraz uniemożliwiają użycie ich przez szkodliwe programy. Dzięki temu zaakceptowane i zaufane aplikacje mogą działać płynnie.

Neutralizowanie rootkitów

Atakujący używają rootkitów i bootkitów do ukrywania swoich działań przed rozwiązaniami zabezpieczającymi. Technologia ochrony przed rootkitami, będąca częścią wielowarstwowej ochrony nowej generacji od Kaspersky Lab, pomaga wykrywać i neutralizować nawet najgłębiej ukryte infekcje.

Identyfikowanie większej liczby ataków i intruzów — nawet tych najbardziej zamaskowanych

Wbudowane sensory i integracja z produktem Kaspersky Endpoint Detection and Response umożliwiają przechwytywanie i analizę dużej ilości danych bez obniżania produktywności użytkownika. Dzięki temu możliwe jest polowanie na zaawansowane zagrożenia w oparciu o ślady wtargnięcia – np. wskaźniki włamania (ang. Indicators of Compromise, IoC).

Ochrona ekspozycji ze strony sieci

Szkodliwe programy przeprowadzające ataki polegające na przepełnieniu bufora mogą zmodyfikować działający w pamięci proces i wykonać szkodliwy kod. Moduł Ochrona sieci identyfikuje ataki sieciowe i exploity oraz zatrzymuje je.

Serwis i pomoc techniczna

W 35 biurach zlokalizowanych w ponad 200 krajach na całym świecie pracownicy pomocy technicznej Kaspersky Lab są dostępni 24 godziny na dobę, 7 dni w tygodniu. Jej warunki określa umowa Maintenance Service Agreement (MSA). Eksperci z Kaspersky Lab pomogą Ci podczas wdrożenia wybranego produktu oraz w sytuacji wystąpienia krytycznego incydentu, dzięki czemu w pełni wykorzystasz potencjał ochrony.

Darmowa wersja próbna

Dowiedz się, dlaczego tylko Prawdziwe bezpieczeństwo łączy łatwość użytkowania i elastyczność z analizą **HuMachine™**, aby chronić Twoją firmę przed wszystkimi rodzajami zagrożeń. Odwiedź tę stronę i zyskaj darmową, 30-dniową wersję próbną pełnej wersji produktu **Kaspersky Endpoint Security for Business**. Ponieważ aplikacja będzie już zainstalowana na punktach końcowych, pod koniec okresu próbnego wystarczy zakupić licencję, aby móc dalej cieszyć się korzyściami, jakie ze sobą niesie.

Coś więcej niż tylko ochrona punktów końcowych – teraz i w przyszłości

Prosty sposób na inwentaryzację i stosowanie łat

Dbanie o aktualność spisu sprzętu i oprogramowania, a także bieżące łatanie luk to żmudne i czasochłonne zajęcie. Z kolei niezałatane luki na punktach końcowych to jedna z najczęstszych dróg wykorzystywanych przez cyberprzestępców do atakowania infrastruktury IT. Oprócz możliwości zdalnego wdrażania nowego oprogramowania należącego do podmiotów zewnętrznych rozwiązania Kaspersky Lab oferują także automatyczne wyszukiwanie luk i zarządzanie łatami, dzięki czemu masz pewność, że zawsze korzystasz z najbezpieczniejszej wersji potencjalnie podatnego oprogramowania. Zaoszczędzony czas administratorzy IT mogą poświęcić na inne zadania.

Bezpieczne udostępnianie danych dzięki szyfrowaniu

Transparentne dla użytkownika szyfrowanie w standardzie FIPS 140-2 w pełni zabezpiecza poufne dane lokalnie i na urządzeniach przenośnych. Technologia integracji umożliwia wymuszanie szyfrowania firmowych danych na poziomie plików, dysku lub urządzenia i włączanie bezpiecznego udostępniania danych w sieci — a zarządzanie odbywa się z jednego miejsca.

Obsługa scenariuszy zdalnych i mobilnych

Dane są dostępne przez cały czas, swobodnie podróżując w obrębie sieci. Ochrona mobilna zapewnia zabezpieczenie przed zagrożeniami ukierunkowanymi na dane będące w ruchu, jak również przed próbami wykorzystywania podatności w urządzeniach, co często poprzedza przedostanie się do infrastruktury. Moduł Kontrola urządzeń chroni przed konsekwencjami utraty danych znajdujących się na nieautoryzowanych lub niezaszyfrowanych urządzeniach przenośnych oraz zapobiega przesyłaniu zainfekowanych danych z urządzenia.

Optymalizacja wydajności i zarządzania dla wszystkich platform

Pojedyncza konsola oferuje pełną widoczność i kontrolę nad każdą stacją roboczą, serwerem i urządzeniem mobilnym, bez względu na lokalizację i zakres działania. Rozwiązanie to zapewnia niemal nieograniczoną skalowalność, umożliwia dostęp do informacji o licencji, narzędzi zdalnego rozwiązywania problemów i kontroli sieci. Scentralizowane zarządzanie uzupełnia integracja z usługą katalogowania Active Directory, możliwość przydzielenia ról do poszczególnych pracowników i zintegrowane panele sterowania.

Regulowanie dostępu do wrażliwych danych i urządzeń nagrywających

Rozwiązanie Kaspersky Lab ogranicza aplikacjom uprawnienia zgodnie z przypisanymi im poziomami zaufania, ograniczając dostęp do takich zasobów jak szyfrowane dane. W oparciu o lokalną i chmurową (KSN) bazę informacji na temat reputacji, system Host Intrusion Prevention System (HIPS) kontroluje aplikacje i ogranicza ich dostęp do krytycznych zasobów systemu, a także urządzeń rejestrujących dźwięk i obraz.

Powstrzymywanie zagrożeń pochodzących z internetu, zanim dotrą do punktów końcowych

Zatrzymując większość przychodzących zagrożeń na poziomie bramy, znacząco zmniejszamy wpływ czynnika ludzkiego i ograniczamy problemy wynikające ze specyfiki stacji roboczych.

Brama ochronna jest pierwszą linią obrony w większości scenariuszy bezpieczeństwa w firmach, a mobilność nie stanowi już żadnej przeszkody. Technologie zabezpieczające Kaspersky Lab filtrują ruch przechodzący przez bramy, automatycznie blokując zagrożenia z zewnątrz, zanim dotrą do punktów końcowych i serwerów. Znacząco zmniejsza to ryzyko wykorzystania luk i zauważalnie zmniejsza nakład pracy personelu odpowiedzialnego za bezpieczeństwo IT.

Większa produktywność i mniejsze ryzyko zagrożeń

Wykorzystująca chmurę ochrona przed spamem nowej generacji od Kaspersky Lab wykrywa nawet najbardziej wyrafinowany, nieznany spam przy minimalnym ryzyku utraty cennej komunikacji wynikającym z fałszywych alarmów. Skrócenie czasu, zasobów i zagrożeń związanych z otrzymywaniem spamu oszczędza zasoby systemowe i ludzkie. Ochrona obejmuje wiele proaktywnych warstw, w tym uczenie maszynowe i mechanizmy wykorzystujące analizę zagrożeń w chmurze, co pozwala na odfiltrowywanie szkodliwych załączników, a także znanych i nowych szkodliwych programów docierających do firmy w poczcie e-mail.

Bezpieczna współpraca

Rozwiązanie Kaspersky Lab przeznaczone dla programu Microsoft SharePoint® obejmuje ochronę przed szkodliwym oprogramowaniem oraz filtrowanie treści i plików, dzięki czemu pomaga firmom wymuszać zasady współpracy i uniemożliwia przechowywanie nieodpowiedniej zawartości w sieci firmowej.

Dzięki rozwiązaniu **Kaspersky Endpoint Security for Business** administratorzy mają pełny obraz środowiska IT: mogą je monitorować, kontrolować i odpowiednio zabezpieczać. Działanie narzędzi i technologii nowej generacji jest zoptymalizowane na wszystkich poziomach, dzięki czemu produkt umożliwia modyfikację ochrony oraz spełnia potrzeby związane z IT na każdym etapie rozwoju firmy.

Kaspersky® Endpoint Security for Business Select

Ponieważ Twoja firma w coraz większym stopniu działa w świecie cyfrowym, nie możesz zapominać o ochronie każdego serwera, laptopa i urządzenia mobilnego. Ochrona nowej generacji od Kaspersky Lab pomaga chronić każdy punkt końcowy w Twojej firmie — to samodzielne rozwiązanie z pojedynczą, elastyczną w konfiguracji konsolą zarządzania.

Kaspersky® Endpoint Security for Business Advanced

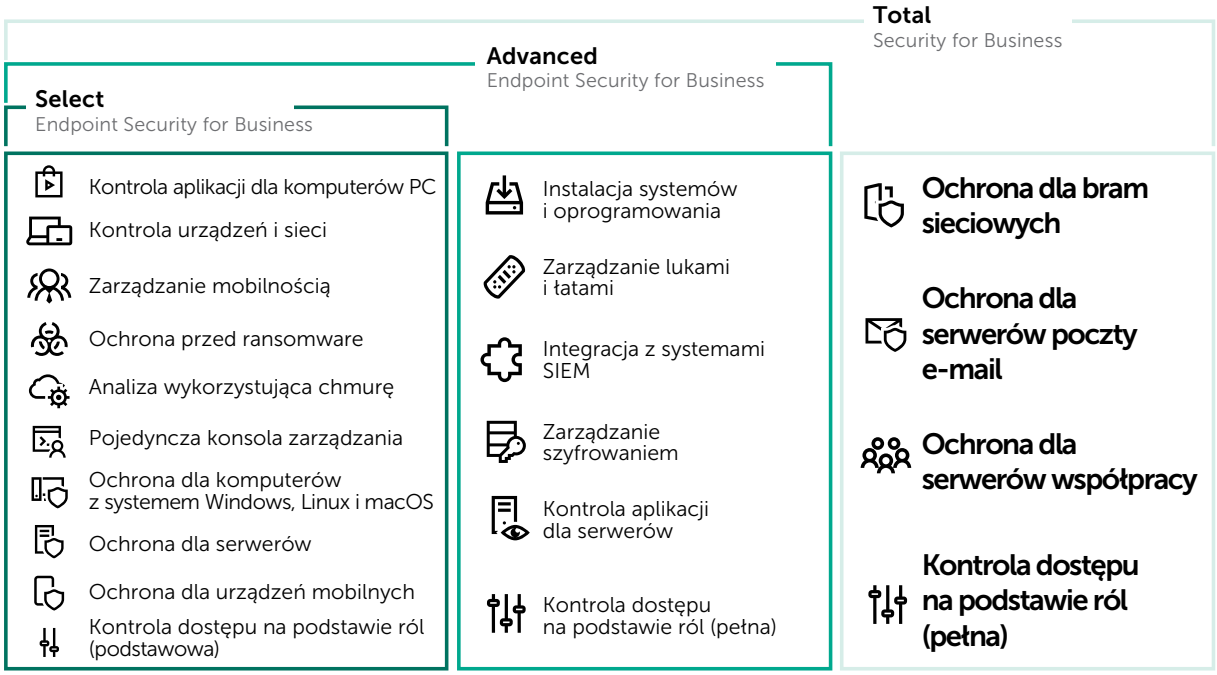
Bardziej rozbudowaną ochronę zapewnia rozwiązanie **Kaspersky Endpoint Security for Business Advanced**. Oprócz ochrony wszystkich punktów końcowych i serwerów zapewnia ono dodatkowe warstwy zabezpieczające, dzięki czemu chroni wrażliwe dane i eliminuje luki, a ponadto upraszcza zadania związane z zarządzaniem systemami.

Kaspersky® Total Security for Business

Firmy posiadające dojrzałe środowiska IT, w których znajduje się wiele nowszych i starszych systemów, muszą dostosować do nich swoją ochronę. Zadanie to ułatwia najbardziej wszechstronne rozwiązanie zabezpieczające Kaspersky Lab dla punktów końcowych, infrastruktury i serwerów współpracy – dzięki niemu możesz skonfigurować niezawodną ochronę, dopasowaną do stanu swojej infrastruktury IT.

Które rozwiązanie jest odpowiednie dla Ciebie?

Bez względu na to, jakie są potrzeby Twojej unikatowej, ewoluującej infrastruktury IT, z pewnością znajdziesz odpowiednie dla siebie rozwiązanie wśród produktów z linii **Kaspersky Endpoint Security for Business**.



Zwiększanie ochrony w razie potrzeby

Funkcja automatycznego i scentralizowanego wykrywania luk w oprogramowaniu oraz zarządzania łatami chroni przed najbardziej niebezpiecznymi zagrożeniami, w tym ransomware. Dla klientów rozwiązania **Kaspersky Endpoint Security for Business Select** automatyzacja ta odbywa się w ramach rozszerzenia **Kaspersky Vulnerability and Patch Management**.

Ponadto dzięki rozszerzeniu **Kaspersky Encryption** klienci korzystający z rozwiązania Select mogą rozbudować ochronę o szyfrowanie całych dysków lub poszczególnych plików/folderów. Pojedyncze logowanie ułatwia natychmiastowy dostęp do szyfrowanych plików oraz kart elektronicznych/tokenów służących do autoryzacji dwuskładnikowej. Ponadto możliwe jest szyfrowanie plików i folderów, które są przechowywane na dyskach lokalnych i przenośnych.

Aby w łatwy sposób zwiększyć poziom ochrony, możesz aktywować wymagany zestaw funkcji bezpośrednio z poziomu Kaspersky Security Center.

Dlaczego warto korzystać z najnowszej wersji ochrony dla punktów końcowych?

Zawiera najnowsze technologie – szybko dostępne i łatwe w obsłudze: jeden serwer, jedna konsola, jeden agent

Obsługuje wszystkie procesy biznesowe dzięki głębszej integracji – wspólna, autorska baza kodu zaprojektowana wewnątrz Kaspersky Lab

Eliminuje dodatkowe koszty i oddzielne licencje – jeden zakup zawiera wszystko, czego potrzebujesz

Zwiększone możliwości audytu i kontroli; ujednolicone zarządzanie z dostępem opartym o role

Kaspersky Lab tworzy i dopracowuje własne technologie, dzięki czemu wszystkie aplikacje firmy działają stabilnie i wydajnie. Firma posiada własny rozbudowany dział badań i rozwoju i stosuje w swoich produktach wiele technologicznych innowacji, takich jak:

- Wielowarstwowe uczenie maszynowe — metody uczenia maszynowego są wykorzystywane na punktach końcowych i w chmurze, na różnych etapach zwalczania zagrożeń.
- Aktywne polowanie na zagrożenia dzięki integracji produktu do ochrony punktów końcowych i rozwiązania Endpoint Detection & Response lub Anti Targeted Attack.
- Unikatowy tryb chmury do ochrony komponentów zapewnia optymalne zabezpieczenie przy minimalnym wpływie na zasoby komputera PC oraz nieznacznym zużyciu łącza internetowego.
- Obsługa kontenerów Microsoft Windows Server, ochrona ruchu z zewnątrz i zarządzanie zaporą sieciową.
- Rozszerzona funkcjonalność kontroli aplikacji i Anti-Bridging.
- Kontrola aplikacji rozszerzona o kategorię „zaufane certyfikaty" i tryb testowy dla profili.
- Nowy, przejrzysty interfejs przedstawia wiele warstw zabezpieczeń, stan ochrony i działanie najnowszych technologii Kaspersky Lab w czasie rzeczywistym.

Prawdziwe cyberbezpieczeństwo: nieodłączny element DNA Kaspersky Lab

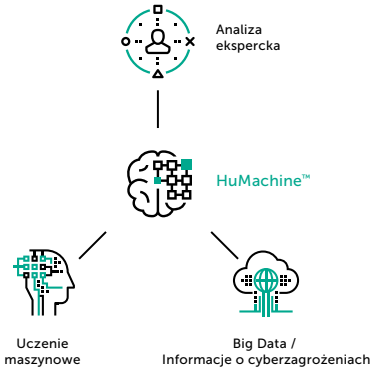
Kaspersky Lab oferuje kompleksowe rozwiązania cyberbezpieczeństwa wykorzystujące najlepszą na świecie analizę zagrożeń, która ma wpływ na wszystkie działania firmy. Jako firma niezależna Kaspersky Lab może działać nieszablonowo i często znacznie szybciej niż konkurencja, dzięki czemu jesteśmy skuteczniejsi.

- **Doświadczenie i wiedza** - Kaspersky Lab to ekspercka wiedza i gromadzone od ponad 20 lat doświadczenie w dziedzinie zwalczania cyberzagrożeń.
- **Globalny Zespół ds. Badań i Analiz (GReAT)** - elitarna grupa ekspertów ds. cyberbezpieczeństwa, która wykryła jedne z najniebezpieczniejszych zagrożeń i ataków ukierunkowanych na świecie.
- Przełomowa inicjatywa transparentności - **Global Transparency Initiative** - kolejny dowód na to, że Kaspersky Lab chroni swoich klientów przed wszystkimi cyberzagrożeniami bez względu na to, skąd pochodzą i jaki jest ich cel.

Prawdziwe cyberbezpieczeństwo to zgodność z nowymi przepisami RODO
Kaspersky Lab zwiększa świadomość w zakresie aspektów RODO związanych z cyberbezpieczeństwem. Rozwiązania firmy pomagają klientom zmniejszać ryzyko wystąpienia wycieku danych i zapobiegają incydentom bezpieczeństwa.

Szerszy obraz – rozwiązania do ochrony firmowej infrastruktury IT od Kaspersky Lab

Ochrona punktów końcowych ma znaczenie krytyczne, jednak jest zaledwie jednym z wielu etapów w całym procesie. Kaspersky Lab oferuje szeroki wachlarz produktów, które mogą współpracować lub działać niezależnie, dzięki czemu nie musisz się martwić o wydajność czy wolność wyboru. Więcej informacji znajduje się na oficjalnej stronie Kaspersky Lab.



Kaspersky Lab
Ochrona dla firm: **kaspersky.pl/biznes**
Unikatowa technologia: **kaspersky.pl/true-cybersecurity**
Wszystko o cyberzagrożeniach: **securelist.pl**
Oficjalny blog: **kaspersky.pl/blog**

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

www.kaspersky.pl