kaspersky AKTYWUJ PRZYSZŁOŚĆ

Gotowy na RODO

Kaspersky® Total Security for Business

Kaspersky Total Security for Business to nasze najbardziej zaawansowane rozwiązanie bezpieczeństwa. Zawarte w nim technologie nowej generacji w jeszcze większym stopniu chronią infrastrukturę, blokując zagrożenia i filtrując pocztę e-mail oraz ruch sieciowy z jednego miejsca lub na punktach końcowych. Dzięki temu łatwiej można dostosować poziom ochrony oraz zarządzać wydajnością w całej infrastrukturze IT – także w przypadku starszych systemów. Wszechstronne narzędzia kontroli dodają kolejna warstwę ochrony – a wszystkimi funkcjami możesz sterować z poziomu jednej konsoli.

Poziom ochrony i zarządzania, jakiego potrzebujesz

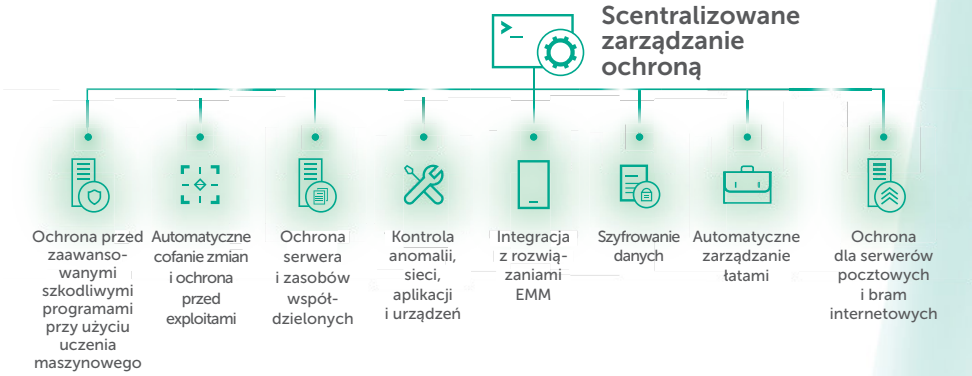
We wszystkich warstwach naszych produktów zastosowaliśmy wszechstronne funkcje klasy korporacyjnej. Zadbaliśmy o to, aby korzystanie z tych technologii było łatwe i elastyczne dla wszystkich firm, bez względu na ich rozmiar.

Który produkt jest najlepszy dla Ciebie?
- SELECT
- ADVANCED
- **TOTAL**

Ochrona wielowarstwowa dla:
- systemu Windows, Linux oraz macOS,
- serwerów Windows i Linux,
- kontenerów Windows Server,
- urządzeń mobilnych,
- pamięci przenośnych,
- serwerów pocztowych,
- bram sieciowych.

Najlepsza ochrona przed:
- exploitami dla oprogramowania,
- ransomware,
- mobilnymi szkodliwymi programami,
- nieznanymi zagrożeniami,
- zagrożeniami bezplikowymi,
- atakami wykorzystującymi skrypty i PowerShell,
- zagrożeniami pochodzącymi z internetu,
- zagrożeniami dystrybuowanymi poprzez pocztę e-mail,
- atakami phishingowymi,
- spamem.

Dostępne funkcje:
- Ochrona przed szkodliwym oprogramowaniem Ulepszono
- Zarządzanie lukami
- Doradca ds. polityki bezpieczeństwa
- Dynamiczne uczenie maszynowe
- Obsługa AMSI Nowość
- Skanowanie ruchu szyfrowanego Nowość
- Izolacja procesów
- Ochrona przed exploitami i cofanie zmian
- Zapora sieciowa i zarządzanie zaporą systemu operacyjnego
- Ochrona wykorzystująca chmurę
- Zintegrowany agent EDR
- Adaptacyjna kontrola anomalii
- Kontrola aplikacji, sieci i urządzeń
- Ochrona dla serwerów i kontenerów Ulepszono
- Ochrona dla serwerów terminalowych
- Obsługa podsystemu Windows w systemie Linux Nowość
- Ochrona przed zagrożeniami mobilnymi Ulepszono
- Zarządzanie szyfrowaniem systemu operacyjnego
- Konfiguracja i instalacja systemu
- Zarządzanie instalacją łat Ulepszono
- Generowanie raportów
- Ochrona przed spamem
- Ochrona ruchu Ulepszono
- Ochrona bram internetowych Ulepszono
- Ochrona serwera poczty Ulepszono



Nasza najlepsza ochrona dla każdego aspektu Twojej firmy

Jedna konsola zarządzania

Dzięki jednej konsoli zarzadzania administratorzy widzą cały krajobraz ochrony i mogą ją kontrolować, a na każdym punkcie końcowym w firmie mogą stosować inna politykę zabezpieczającą. Pomaga to sprawnie dostosowywać ochronę przy jedynie minimalnej przerwie w działaniu, a dodatkowo dostępnych jest wiele wstępnie skonfigurowanych scenariuszy.

Elastyczna ochrona

Produkt może działać w każdym środowisku IT i stosuje technologie nowej generacji o udowodnionej skuteczności. Wbudowane sensory i integracja z produktem Endpoint Detection and Response (EDR) umożliwia przechwytywanie i analizę dużych ilości danych w celu wykrywania nawet najbardziej zamaskowanych, wyrafinowanych cyberataków.

Jeden produkt – przejrzyste koszty

Dzięki umieszczeniu wielu technologii zabezpieczających w jednym rozwiązaniu nie musisz martwić się o ukryte koszty. Jeden produkt to jedna licencja – czyli wszystko, czego potrzebujesz do ochrony swojej infrastruktury IT.

Cyberbezpieczeństwo, któremu możesz ufać

Firmy wymagają neutralności i suwerenności danych – nasz produkt skanuje, ale nie gromadzi informacji. Dane statystyczne są przetwarzane w Szwajcarii, co zapewnia neutralność geopolityczną.

Szczegółowe informacje znajdują się na naszych stronach.

Kluczowe funkcje

Wykorzystujące chmurę narzędzia do kontroli punktów końcowych

Unikatowe narzędzia do kontroli anomalii i aplikacji
Adaptacyjna kontrola anomalii automatycznie zwiększa bezpieczeństwo do najwyższego poziomu, dostosowanego do poszczególnych ról w organizacji, a uzupełnia ją Kontrola aplikacji klasy korporacyjnej oraz nieustannie aktualizowana biała lista.
Kontrola urządzeń, system zapobiegania włamaniom i więcej...

Funkcje ochrony mobilnej

Innowacyjne technologie chroniące przed szkodliwymi programami
Połączenie opartego na uczeniu maszynowym, proaktywnego i wykorzystującego chmurę wykrywania zapewnia ochronę w czasie rzeczywistym, którą zwiększa bezpieczna przeglądarka, a także skanowanie na żądanie lub zgodnie z harmonogramem.
Integracja z systemami EMM i więcej...

Funkcje ochrony punktów końcowych i serwerów

Ochrona przed exploitami
Zapobiega uruchamianiu szkodliwego oprogramowania, a także wykorzystaniu luk w istniejących programach i systemie operacyjnym, zapewniając dodatkową warstwę zabezpieczającą przed nieznanymi zagrożeniami dnia zerowego.
Wykrywanie niebezpiecznego zachowania i automatyczne wycofywanie zmian
Identyfikuje i chroni przed zaawansowanymi zagrożeniami, w tym ransomware, atakami bezplikowymi i przechwytywaniem kont administratorów. Moduł Wykrywanie zachowań blokuje ataki, a Automatyczne wycofywanie zmian unieważnia wszelkie dokonane zmiany.
Ochrona przed szyfrowaniem dla folderów współdzielonych
Unikatowy mechanizm potrafi blokować próby szyfrowania plików znajdujących się w zasobach współdzielonych przez szkodliwy proces działający na innym sprzęcie w tej samej sieci.
Ochrona dla kontenerów, serwerów terminalowych i więcej...

Ochrona poczty i sieci

Ochrona ruchu
Nasze technologie zabezpieczające nowej generacji filtrują ruch przechodzący przez bramy i systemy zewnętrzne obsługujące protokół ICAP, automatycznie blokując nadchodzące zagrożenia, zanim dotrą one do punktów końcowych i serwerów.
Ochrona przed spamem
Wykorzystujący chmurę Moduł antyspamowy nowej generacji firmy Kaspersky potrafi wykrywać nawet najbardziej wyrafinowane, nieznane wiadomości spamowe przy minimalnym ryzyku utraty korespondencji ze względu na fałszywe trafienia.
Większa elastyczność
Umożliwia podjęcie decyzji, czy filtrowanie poczty i sieci ma się odbywać na serwerze, czy na komputerach PC. W ten sposób możesz dostosować ochronę do różnych systemów i zadbać o wydajność zarówno nowszych, jak i starszych systemów.

Szyfrowanie i ochrona danych

Kompleksowe szyfrowanie
Pracownicy działów bezpieczeństwa mogą wymusić szyfrowanie z użyciem certyfikatu FIPS 140-2 – na poziomie pliku, dysku lub urządzenia – oraz zarządzać wbudowanymi narzędziami szyfrującymi typu BitLocker w systemie Microsoft czy FileVault w systemie macOS.

Zarządzanie systemami, lukami i łatami

Zarządzanie łatami
Zaawansowane, głębokie skanowanie w poszukiwaniu luk uzupełnia automatyczna dystrybucja łat.
Instalacja systemu operacyjnego i oprogramowania, zarządzanie licencjami i więcej...

Serwis i pomoc techniczna

W 34 biurach zlokalizowanych w ponad 200 krajach na całym świecie pracownicy pomocy technicznej Kaspersky pomagają klientom w pełni wykorzystać możliwości ochrony. W Polsce pomoc jest dostępna, działa 24 godziny na dobę i 7 dni w tygodniu.

Przekonaj się

Sprawdź, na czym polega prawdziwe cyberbezpieczeństwo! Aby skorzystać z 30-dniowej wersji testowej produktu Kaspersky Endpoint Security for Business, wejdź na tę stronę.

Informacje o cyberzagrożeniach: securelist.pl
Informacje ze świata bezpieczeństwa IT: kaspersky.pl/blog
Ochrona IT dla MŚP: kaspersky.pl/biznes
Ochrona IT dla korporacji: kaspersky.pl/korporacje

www.kaspersky.pl

Jesteśmy skuteczni. Jesteśmy niezależni. Jesteśmy transparentni. Zobowiązaliśmy się do budowania bezpieczniejszego świata, w którym technologia czyni nasze życie lepszym. Dlatego go chronimy, aby każda osoba wszędzie mogła korzystać z jego nieskończonych możliwości. Aktywuj cyberbezpieczeństwo dla lepszego jutra.

Dowiedz się więcej na stronie kaspersky.pl/future.

Sprawdzony.
Transparentny.
Niezależny.