



# Kaspersky® Endpoint Security for Business

Advanced

Kaspersky Endpoint Security for Business Advanced łączy wielowarstwową ochronę z narzędziami rozszerzonej kontroli, dzięki czemu jest elastycznym rozwiązaniem zabezpieczającym, które można szybko dostosować w celu ochrony przed nowymi zagrożeniami. Dodatkowe warstwy ochrony sprawiają, że firmy mogą jeszcze lepiej eliminować luki i strzec swoich wrażliwych danych.

## Poziom ochronę 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:

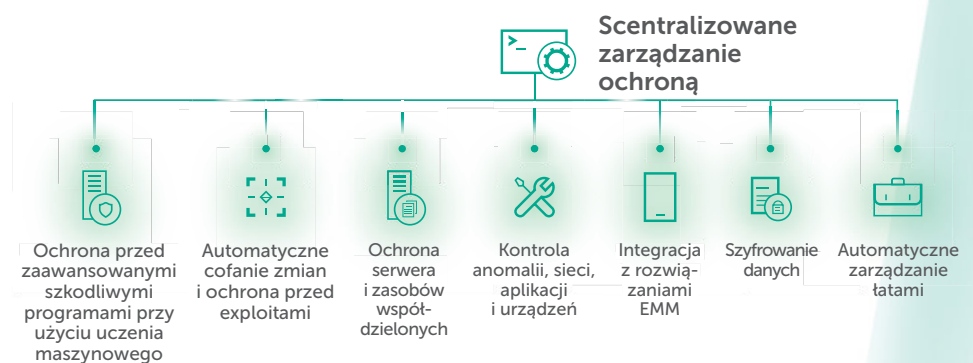
- systemu Windows, Linux oraz macOS,
- serwerów Windows i Linux,
- kontenerów Windows Server,
- urządzeń mobilnych,
- pamięci przenośnych.

### Najlepsza ochrona przed:

- exploitami dla oprogramowania,
- ransomware,
- mobilnymi szkodliwymi programami,
- zaawansowanymi zagrożeniami,
- zagrożeniami bezplikowymi,
- atakami wykorzystującymi skrypty i PowerShell,
- zagrożeniami pochodzącymi z internetu.

### Dostępne funkcje:

- Ochrona przed szkodliwym oprogramowaniem Ulepszono
- Zarządzanie lukami
- Doradca ds. polityki bezpieczeństwa
- Uczenie wykorzystujące sztuczną inteligencję
- Obsługa AMSI Nowość
- Skanowanie ruchu szyfrowanego Nowość
- Izolacja procesów
- Ochrona przed exploitami i cofanie zmian
- Zarządzanie zaporą sieciową i zaporą sieciową systemu operacyjnego
- Ochrona wykorzystująca chmurę
- Zintegrowany agent EDR
- Adaptacyjna kontrola anomalii Nowość
- Kontrola aplikacji, sieci i urządzeń
- Ochrona dla serwerów i kontenerów Ulepszono
- Ochrona dla serwerów terminali
- 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



## Bezpieczeństwo adaptacyjne z rozszerzonym zarządzaniem i ochroną danych

### Jedna konsola zarządzania

Dzięki jednej konsoli zarządzania administratorzy widzą cały krajobraz ochrony i mogą nią zarządzać, a na każdym punkcie końcowym w firmie mogą stosować inną politykę zabezpieczającą. Pomaga to sprawnie dostosowywać ochronę i wymaga jedynie minimalnej przerwy w działaniu, a dodatkowo dostępnych jest wiele wstępnie skonfigurowanych scenariuszy.

### Elastyczna ochrona

Produkt może działać w każdym środowisku IT i stosuje wszystkie 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 i brak ukrytych kosztów

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.

### Satysfakcja klienta gwarantowana

Dzięki dużym nakładom na badania i rozwój nasze produkty zapewniają ochronę, jakiej potrzebujesz. Osoby decyzyjne w firmach konsekwentnie wskazują, że są zadowolone z efektów korzystania z naszych produktów, co regularnie potwierdzają niezależne badania i raporty.

# Kluczowe funkcje



## Wykorzystujące chmurę narzędzia do kontroli punktów końcowych

### Unikatowa kontrola anomalii i aplikacji

Adaptacyjna kontrola anomalii automatycznie podnosi bezpieczeństwo do najwyższego poziomu dostosowanego do poszczególnych ról w organizacji, a uzupełnia ją Kontrola aplikacji klasy korporacyjnej oraz nieustannie aktualizowana biała lista.

### System zapobiegania włamaniom (HIPS)

Reguluje dostęp do wrażliwych danych i urządzeń nagrywających obraz oraz dźwięk na podstawie lokalnej i chmurowej (Kaspersky Security Network) bazy zawierającej informacje związane z reputacją, nie zmniejszając szybkości działania autoryzowanych aplikacji.

Kontrola urządzeń, sieci i wiele więcej...



## Najważniejsze funkcje zapewniające ochronę przed zagrożeniami

### 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 i serwerów terminalowych

Zabezpiecza kontenery Windows Server i wiele środowisk dostępu zdalnego, w tym Microsoft Terminal Services i Citrix XenApp/Xen Desktop. Moduł Ochrona ruchu dba o bezpieczeństwo ruchu sieciowego i pocztowego przechodzącego przez serwer terminalowy.

Ochrona przed exploitami, technologia zabezpieczająca przed rootkitami i więcej...



## Szyfrowanie i ochrona danych

### Kompleksowe szyfrowanie

Pracownicy działów bezpieczeństwa mogą wymusić szyfrowanie z użyciem certyfikatu FIPS 140.2 i normy Common Criteria – na poziomie plików, dysków lub urządzeń – oraz zarządzać wbudowanymi narzędziami szyfrującymi typu BitLocker w systemie Microsoft czy FileVault w systemie macOS.

### Ujednolicona i zintegrowana polityka

Niepowtarzalna integracja między szyfrowaniem a narzędziami kontroli aplikacji i urządzeń zapewnia dodatkową warstwę ochrony oraz łatwość zarządzania.



## Zarządzanie systemami, lukami i łatami

### Zarządzanie łatami

Zaawansowane, głębokie skanowanie w poszukiwaniu luk wraz z automatyczną dystrybucją łat.

### Oszczędzająca czas instalacja systemu operacyjnego i oprogramowania

Twórz obrazy systemu, przechowuj je i instaluj z jednego miejsca. To idealne rozwiązanie np. do migracji do systemu Microsoft Windows 10 czy wdrożenia 150 popularnych aplikacji rozpoznawanych przez Kaspersky Security Network.

### Zarządzanie sprzętem, oprogramowaniem i licencjami

Raporty dotyczące posiadanego sprzętu i oprogramowania pomagają kontrolować zobowiązania licencyjne w odniesieniu do oprogramowania. Oszczędzaj pieniądze poprzez przydzielanie praw do oprogramowania.



## 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, skanowanie na żądanie lub zgodnie z harmonogramem.

Instalacja bez połączenia przewodowego (Over the Air, OTA) 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](https://securelist.pl)  
Informacje ze świata bezpieczeństwa IT: [kaspersky.pl/blog](https://kaspersky.pl/blog)  
Ochrona IT dla MŚP: [kaspersky.pl/biznes](https://kaspersky.pl/biznes)  
Ochrona IT dla korporacji: [kaspersky.pl/korporacje](https://kaspersky.pl/korporacje)

[www.kaspersky.pl](https://www.kaspersky.pl)

© 2019 AO Kaspersky Lab. Wszelkie prawa zastrzeżone. Zarejestrowane znaki handlowe i nazwy usług należą do ich właścicieli.



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](https://kaspersky.pl/future).



Sprawdzony. Transparentny. Niezależny.