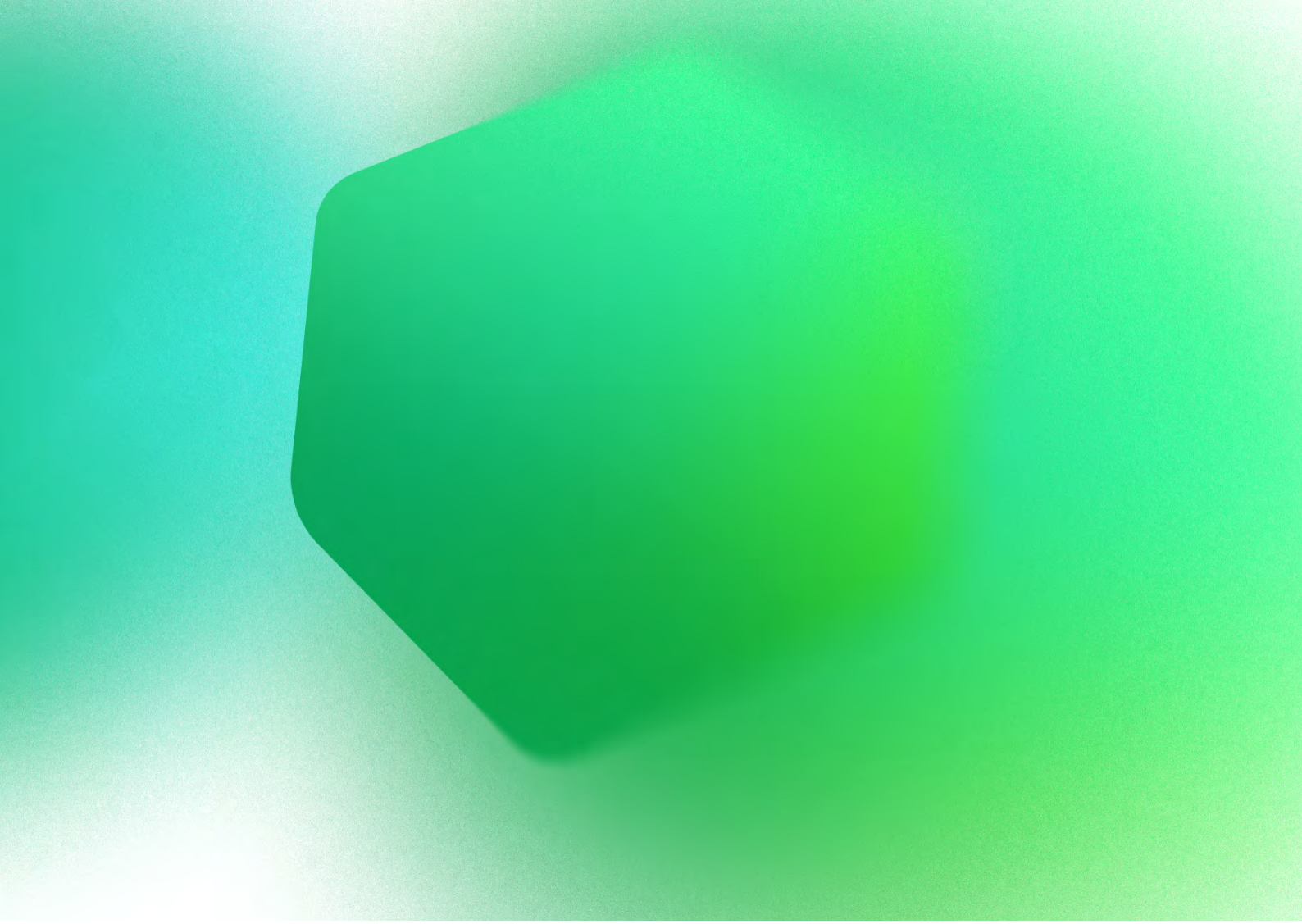


2020

Sprawdzona ochrona i nieograniczona orkiestracja Twojej chmury hybrydowej

kaspersky

Dowiedz się więcej na kaspersky.pl
#truecybersecurity

Kaspersky Hybrid Cloud Security

Wirtualizacja to główny temat w każdej firmie, która chce być elastyczna i wydajna. Kolejnym naturalnym krokiem jest chmura obliczeniowa. Zdejmuje ona ograniczenia związane ze skomplikowaną infrastrukturą i oferuje nieosiągalny wcześniej poziom wydajności. Jednak wykorzystywanie chmury niesie ze sobą również wiele niebezpieczeństw i komplikacji.

Kaspersky Hybrid Cloud Security oferuje ujednoliconą ochronę dla każdego etapu korzystania z chmury. Zabezpiecza maszyny wirtualne i zwirtualizowane zadania bez względu na to, czy są one realizowane lokalnie, w centrum danych czy chmurze publicznej. Ponieważ aplikacje zostały stworzone z myślą o specyfice zarówno wirtualizacji, jak i funkcjonowania serwerów, zapewnia doskonale wyważoną ochronę przed najbardziej zaawansowanymi istniejącymi i przyszłymi zagrożeniami bez uszczerbku dla wydajności systemu.

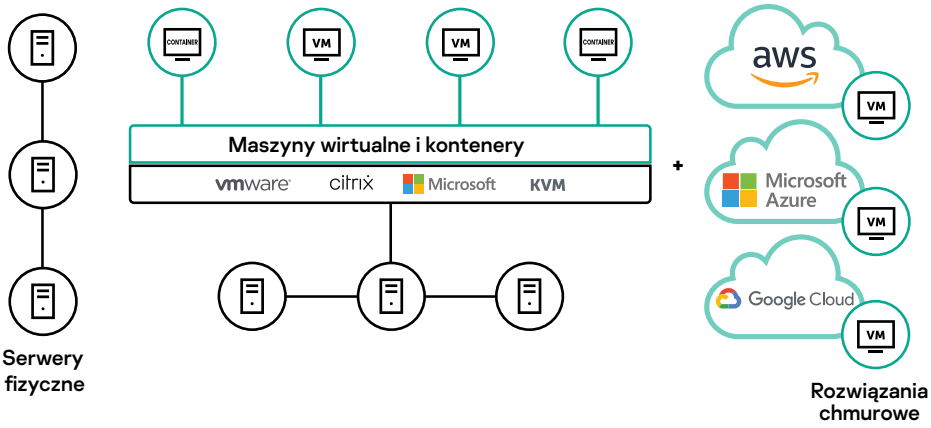
Największe wyzwania dla użytkowników chmury:

- Rosnąca złożoność infrastruktury może skutkować zmniejszoną przejrzystością
- Wielowarstwowe podejście, które jest kluczem do skutecznej ochrony rzadko jest spotykane w jednym produkcie
- Tradycyjne, obciążające zabezpieczenia pochłaniają cenne zasoby systemowe
- Podejście oparte na silosie i różne kontrole niosą ze sobą dodatkowe wyzwania administracyjne i związane z bezpieczeństwem
- Złośliwe oprogramowanie i oprogramowanie ransomware atakują zarówno wirtualne, jak i fizyczne punkty końcowe
- Brak wdrożenia odpowiednich środków cyberbezpieczeństwa w zakresie ochrony danych osobowych może skutkować problemami prawnymi.

Dlaczego Kaspersky Hybrid Cloud Security?

- Zaprojektowany pod kątem środowisk fizycznych, wirtualnych i chmurowych
- Zintegrowane wielowarstwowe zabezpieczenia dla wszystkich typów zasobów
- Spójne, zautomatyzowane i elastyczne zabezpieczenia chmur publicznych AWS Azure i Google
- Pomaga zapewnić kompleksową ochronę dzięki pełnemu zestawowi narzędzi bezpieczeństwa
- Bezproblemowa koordynacja zabezpieczeń w całej chmurze hybrydowej
- Według licznych nagród i niezależnych testów najbardziej przetestowana, najlepsza ochrona

Kluczowe korzyści



Umożliwia bezpieczne korzystanie z chmury – bez kompromisu w zakresie poziomu ochrony

- Opatentowane technologie i nasz wielokrotnie nagradzany silnik cyberbezpieczeństwa chronią wszystkie rozwiązania – fizyczne, wirtualne oraz oparte na chmurze.
- Oparta na uczeniu maszynowym wielowarstwowa ochrona w czasie rzeczywistym, zabezpiecza dane, procesy i aplikacje przed pojawiającymi się zagrożeniami.
- Holistyczne podejście do bezpieczeństwa danych pomaga zmniejszyć ryzyko prawne i reputacyjne związane z przepisami dotyczącymi ochrony danych.

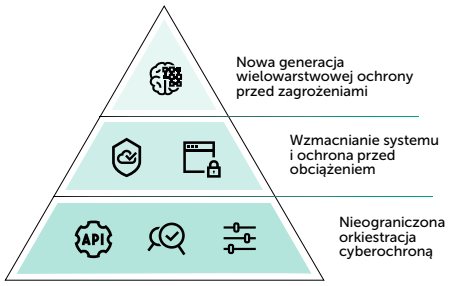
Zapewnia maksymalne wykorzystanie zasobów i inwestycji

- Ochrona oparta na lekkich agentach oraz bezagentowa zabezpiecza zwirtualizowane zasoby w sieciach zwykłych i zdefiniowanych programowo bez wpływu na wydajność.
- Integracja z natywną publiczną i zarządzaną ochroną w chmurze pomaga zabezpieczyć aplikacje, systemy operacyjne, przepływ danych i obszary robocze użytkowników przy bardzo niskim zużyciu zasobów.
- Zarządzanie zasobami fizycznymi i wirtualnymi z jednego miejsca oszczędza czas przeznaczany na wdrażanie i konserwację.

1 Testy, o których mowa obejmowały szereg produktów firmy Kaspersky opartych na tych samych technologiach ochrony przed zagrożeniami, które są wykorzystywane w Kaspersky Hybrid Cloud Security. Dowiedz się więcej na www.kaspersky.com.pl/top3

Funkcje

Funkcje	Opis
Wielowarstwowa ochrona przed zagrożeniami Nowa generacja ochrony przed złośliwym oprogramowaniem firmy Kaspersky obejmuje wiele proaktywnych warstw zabezpieczeń, które są w stanie blokować najszerszy zakres cyberataków zagrażających zasobom o znaczeniu krytycznym dla Twojej firmy.	
Globalne informacje o zagrożeniach	Dostarcza w czasie rzeczywistym dane o stanie krajobrazu zagrożeń. Nawet gdy się on zmienia, zapewnia ochronę przez cały czas.
Uczenie maszynowe	Duże zbiory danych z globalnej analizy zagrożeń są przetwarzane przy użyciu połączonej mocy algorytmów uczenia maszynowego i ludzkiej wiedzy, aby zapewnić wysoki poziom wykrywania przy minimalnej liczbie fałszywych alarmów.
Ochrona przed zagrożeniami z poczty e-mail i sieci	Umożliwia bezpieczne działanie wirtualnych i zdalnych komputerów, chroniąc je przed zagrożeniami z poczty e-mail i sieci.
Inspekcja dzienników zdarzeń	Skanuje wewnętrzne pliki dziennika w celu zapewnienia optymalnej higieny pracy.
Analiza zachowań	Monitoruje aplikacje i procesy chroniąc przed zaawansowanymi zagrożeniami, w tym złośliwym oprogramowaniem bezcielesnym oraz opartym na skryptach.
Silnik naprawczy	W razie potrzeby cofa wszelkie złośliwe zmiany wprowadzone w zasobach chmurowych.
Ochrona przed exploitami	Zapewnia skuteczną ochronę przed atakami, zapewniając jednocześnie doskonałą kompatybilność z chronionymi aplikacjami, a wszystko to przy minimalnym wpływie na wydajność.
Funkcjonalność anty-ransomware	Chroni zwirtualizowane zasoby przed wszelkimi próbami zablokowania danych o znaczeniu krytycznym w celu zapłacenia okupu. Przywraca pliki, których dotyczy problem do ich stanu przed zaszyfrowaniem i blokuje szyfrowanie inicjowane zdalnie.
Ochrona przed zagrożeniami sieciowymi	Wykrywa i zapobiega włamaniom sieciowym do zasobów w chmurze.
Ochrona kontenerów	Zapewnia, że infekcje nie mogą zostać przeniesione do Twojej hybrydowej infrastruktury IT za pośrednictwem kontenerów Docker lub Windows, których zabezpieczenia zostały naruszone.
Wzmocnienie systemu	
Kontrola aplikacji	Umożliwia zablokowanie wszystkich zasobów chmury hybrydowej w trybie domyślnej odmowy w celu optymalnego wzmocnienia systemu. Pozwala to ograniczyć zakres uruchomionych aplikacji tylko do legalnych i zaufanych.
Kontrola urządzeń	Określa, które zwirtualizowane urządzenia mogą uzyskiwać dostęp do poszczególnych zasobów w chmurze.
Kontrola sieci	Reguluje wykorzystanie zasobów sieciowych przez komputery wirtualne i zdalne, aby zmniejszyć ryzyko oraz zwiększyć produktywność.
Ochrona przed włamaniami (HIPS)	Przypisuje kategorie zaufania uruchamianym aplikacjom, ograniczając ich dostęp do krytycznych zasobów i ograniczając ich możliwości.
Monitorowanie integralności plików	Pomaga zapewnić integralność krytycznych komponentów systemu i innych ważnych plików.
Zarządzanie lukami i poprawkami	Centralizuje i automatyzuje podstawowe zadania związane z bezpieczeństwem, konfiguracją systemu i zarządzaniem, takie jak ocena luk, dystrybucja poprawek i aktualizacji, zarządzanie zasobami oraz wdrażanie aplikacji.
Nieograniczona przejrzystość	
Zunifikowane zarządzanie ochroną	Kaspersky Security Center ułatwia administrowanie bezpieczeństwem całej infrastruktury punktów końcowych i serwerów z jednego miejsca - w biurze, w Twoim centrum danych oraz w chmurze.
Cloud API	Bezproblemowa integracja z publicznymi środowiskami AWS i Azure umożliwia wykrywanie infrastruktury, zautomatyzowane wdrażanie agentów bezpieczeństwa i zarządzanie oparte na zasadach, a także łatwiejsze zarządzanie zasobami i zabezpieczeniami.
Elastyczne opcje zarządzania	Funkcje wielu dzierżawców, zarządzanie kontami oparte na uprawnieniach i kontrola dostępu oparta na rolach zapewniają elastyczność przy jednoczesnym zachowaniu korzyści płynących z ujednoliconej orkiestracji z jednego serwera.
Integracja z systemami SIEM	W infrastrukturach z bardziej dojrzałymi systemami informatycznymi informacje o bezpieczeństwie i systemy zarządzania mogą być używane jako ujednolicone okno dla różnych aspektów cyberbezpieczeństwa firmy – w całej hybrydowej sieci IT.



Zunifikowana ochrona dla chmur:

Chmury publiczne
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Prywatne centra danych
- VMware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox

Środowiska virtualne
- VMware Horizon
- Citrix Virtual Apps and Desktops

Serwery fizyczne
- Windows
- Linux

Komputery fizyczne
- Windows
- Linux

aws

Microsoft Azure

vmware

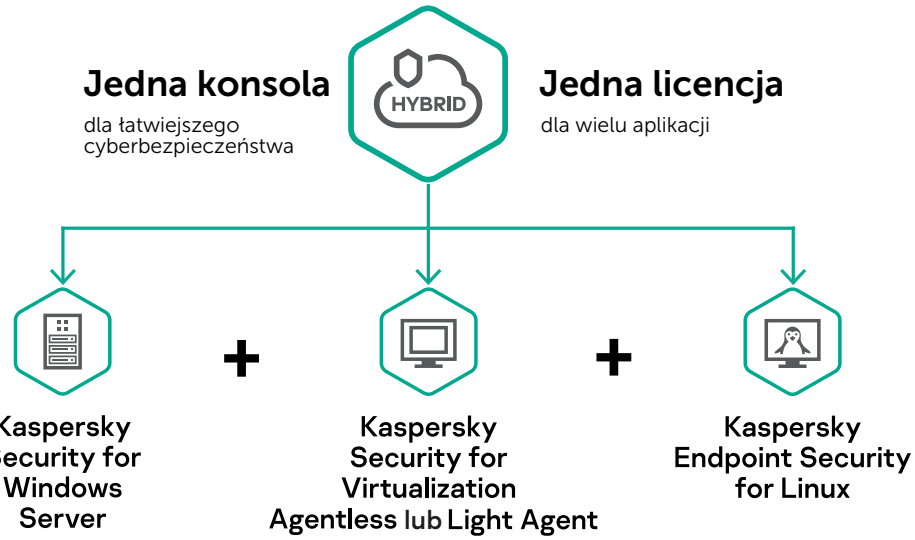
citrix

Google Cloud

KVM

Zapewnia spójną widoczność i kontrolę niezależnie od konfiguracji infrastruktury hybrydowej

- Łatwiejsze udostępnianie usług bezpieczeństwa i operacje oparte na zasadach są dostępne dla całej Twojej chmury hybrydowej.
- Zarządzanie i orkiestracja zabezpieczeń działają bezproblemowo w wielu chmurach.
- Pełna widoczność, kontrola i całościowa ochrona przed najbardziej zaawansowanymi zagrożeniami dla każdego rozwiązania, w każdej lokalizacji.



Kaspersky Hybrid Cloud Security zapewnia wiele wielokrotnie nagradzanych, uznanych w branży technologii bezpieczeństwa, które wspierają i upraszczają transformację środowiska IT. Zabezpiecza migrację z środowisk fizycznych do wirtualnych oraz chmurowych, a widoczność i przejrzystość gwarantują bezbłędną orkiestrację bezpieczeństwa.

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

www.kaspersky.com.pl

2020 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 www.kaspersky.com.pl/transparentnosc

Sprawdzony. Transparentny. Niezależny.