kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Security for Mail Server

Budowanie odporności na najczęstszy typ ataków

Poczta e-mail jest głównym wektorem ataku zagrażającym firmowemu bezpieczeństwu IT. Atakujący mają coraz bardziej wyrafinowane sposoby infiltracji organizacji za pomocą ataków przez pocztę e-mail, co skutkuje stratami finansowymi, operacyjnymi i reputacyjnymi. Aby przeciwdziałać tym zmianom, firmy muszą pomyśleć o odporności i ochronie. Optymalizując swoją odporność i minimalizując powierzchnię ataku, możesz sprawić, że Twoja firma stanie się mniej atrakcyjnym, a nawet nieosiągalnym celem dla napastników. A najlepszym momentem, w którym można wdrożyć środki zaradcze zwiększające odporność jest czas zanim niechciane wiadomości e-mail wejdą w kontakt z użytkownikami i ich punktami końcowymi.

Zbuduj swoją odporność w punkcie wejścia, który jest numerem jeden dla ataków

Aplikacje Kaspersky Security for Mail Server pomagają budować odporność na ataki za pośrednictwem poczty e-mail poprzez:

Identyfikowanie i filtrowanie podejrzanych oraz niechcianych wiadomości e-mail na poziomie bramy

Większość ataków pocztowych zaczyna swoją aktywację dopiero na poziomie punktu końcowego — Kaspersky Security for Mail Server powstrzymuje je zanim zajdą tak daleko. Nasza wielokrotnie nagradzana ochrona wzmacnia odporność wykrywając i przechwytując ataki już na początku, zanim zdołają przekroczyć granicę i skierować się do punktów końcowych oraz użytkowników.

Szybkie i dokładne przetwarzanie

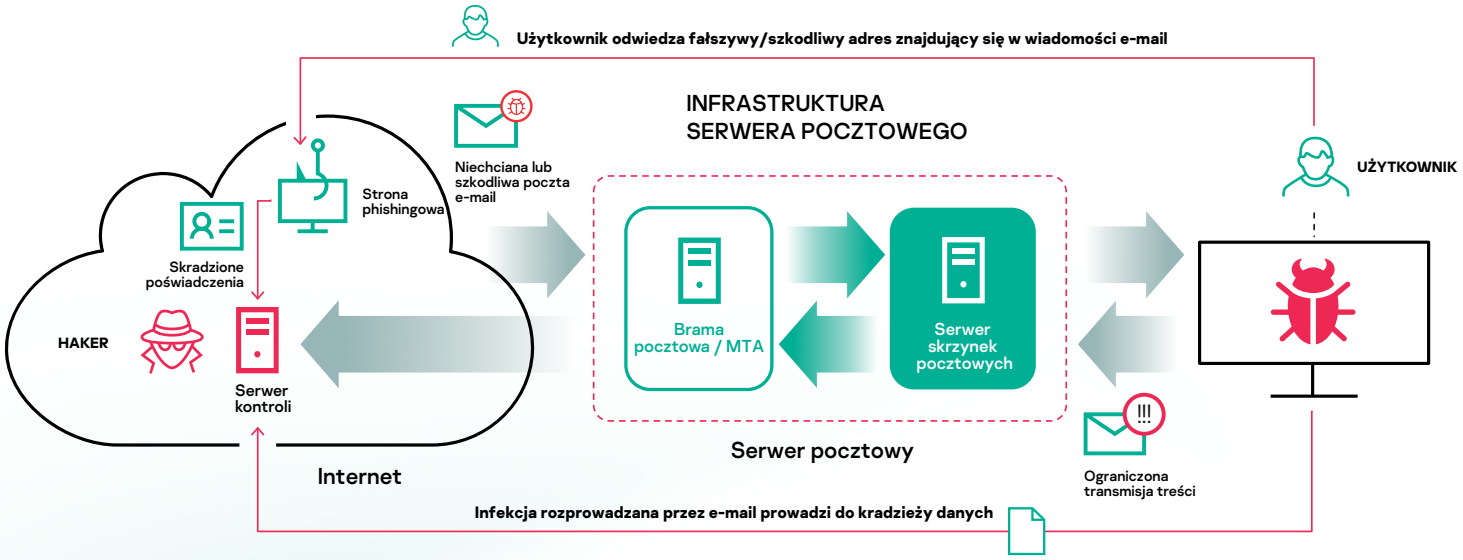
Kluczowa rola poczty e-mail w komunikacji biznesowej oznacza, że przetwarzanie zabezpieczeń musi być szybkie, sprawne i dokładne – bez utrudniania legalnej komunikacji. Kaspersky Security for Mail Server oferuje najskuteczniejsze technologie ochrony w branży przed wszystkimi zagrożeniami: wiadomościami zawierającymi phishing i spam, atakami BEC i oprogramowaniem ransomware. To wszystko przy niemal zerowej liczbie fałszywych alarmów i jednoczesnej możliwości przesyłania legalnych wiadomości e-mail bez zakłóceń.

Ochrona poczty e-mail poza bramą

Użytkownicy muszą być chronieni, w tym przed nimi samymi – a firma musi być chroniona przed konsekwencjami niewiedzy lub błędu użytkownika. Kaspersky Security for Mail Server wykrywa zgodnie z zasadami skonfigurowanymi przez administratora obecność szkodliwej lub niepożądanej zawartości na poziomie indywidualnej skrzynki odbiorczej i nadawczej na serwerach Microsoft Exchange — w tym złośliwego oprogramowania, wiadomości phishingowych i potencjalnie niebezpiecznych załączników. Aby powstrzymać przejęcie konta oraz zagrożenia wewnętrzne, wysoce zalecana jest ochrona na poziomie serwera pocztowego.

1 https://www.kaspersky.co.uk/top3

Kluczowe funkcje



Model zagrożeń poczty elektronicznej

Wielowarstwowa ochrona przed złośliwym oprogramowaniem

Wiele warstw zabezpieczeń stosowanych za pośrednictwem sieci głębokiego uczenia powstrzymuje najbardziej złożone złośliwe oprogramowanie przenoszone przez pocztę e-mail — w tym przypadki ukierunkowanego oprogramowania ransomware, programy typu wiper i koparki, które często są wspierane przez ukierunkowany phishing. Analiza zachowań, dane o reputacji z chmury i silniki oparte na sygnaturach, heurystyka i bazy danych sygnatur łączą się z ludzką wiedzą, aby zapewnić wiele warstw nagradzanych poziomów wykrywania i zapobiegania przy minimalnej liczbie fałszywych alarmów.

Piaskownica

Aby chronić przed nawet najbardziej złożonym, mocno ukrytym złośliwym oprogramowaniem, załączniki są wykonywane w bezpiecznym, emulowanym środowisku. Są w nim analizowane, aby zapewnić, że niebezpieczne próbki nie przedostaną się do systemu korporacyjnego. W przypadku użytkowników Kaspersky Anti Targeted Attack pełna integracja obsługuje detonację w zewnętrznym środowisku piaskownicy — zapewniając znacznie głębsze poziomy oceny i analizy dynamicznej. Atak ukierunkowany może wtedy zostać przerwany dzięki zablokowaniu dostarczenia jego komponentów.

Automatyczny anti-spam (z reputacją treści i adresu źródłowego)

System antyspamowy firmy Kaspersky wykorzystuje inteligentne silniki oraz nadzór ekspercki, aby zminimalizować możliwość fałszywych wykryć i dostosować się do zmian w krajobrazie zagrożeń. Zebrane globalnie dane dotyczące reputacji są przetwarzane w chmurze, aby zapewnić solidną podstawę do skutecznego wykrywania spamu.

Przeciwdziałanie naruszeniom firmowej poczty e-mail (BEC)

Dedykowany system wykrywania oparty na uczeniu maszynowym, z modelami algorytmicznymi, które są regularnie aktualizowane o nowe scenariusze przetwarza szereg wskaźników pośrednich, umożliwiając systemowi blokowanie nawet najbardziej wiarygodnych fałszywych wiadomości e-mail. Wsparcie dla mechanizmów uwierzytelniania nadawcy, takich jak SPF / DKIM / DMARC pomaga chronić przed podszywaniem się pod źródła — szczególnie przydatne w sytuacjach zagrożenia dla firmowej poczty e-mail (atakami typu BEC).

Więcej niż brama – odporność na poziomie skrzynki pocztowej

Technologie na poziomie skrzynki e-mail obejmują:
Ponowne skanowanie poczty elektronicznej – przewidywanie scenariuszy, takich jak opóźniona aktywacja phishingowego adresu URL.
Tymczasowa kwarantanna antyspamowa – idealna do środowisk o niskiej tolerancji. Podejrzane wiadomości e-mail z pierwszej linii mogą być przetrzymywane w tymczasowej kwarantannie do czasu zgromadzenia w Kaspersky Security Network wystarczających informacji, które pozwolą ocenić, czy ich dostarczenie jest z całą pewnością bezpieczne.

Zaawansowany anti-phishing

W celu uzyskania skutecznych modeli wykrywania zaawansowany system antyphishingowy firmy Kaspersky opiera się na analizie sieci neuronowych. Dzięki ponad 1000 zastosowanym kryteriom – w tym sprawdzeniu obrazów, języka i określonych skryptów – to wspomagane chmurą podejście jest wspierane przez globalnie zebrane dane o złośliwych i zawierających phishing adresach URL i adresach IP, aby zapewnić ochronę zarówno przed znanymi, nieznanymi wiadomościami phishingowymi oraz atakom typu zero-day.

Zapobieganie niebezpiecznemu transferowi treści

W celu identyfikacji potencjalnie niebezpiecznych załączników konfigurowalny system filtrowania firmy Kaspersky wykrywa sposoby ukrywania plików powszechnie używane przez cyberprzestępców. Funkcjonalność filtrowania treści pozwala administratorowi skonfigurować wyspecjalizowane reguły zapobiegające wyciekom danych.

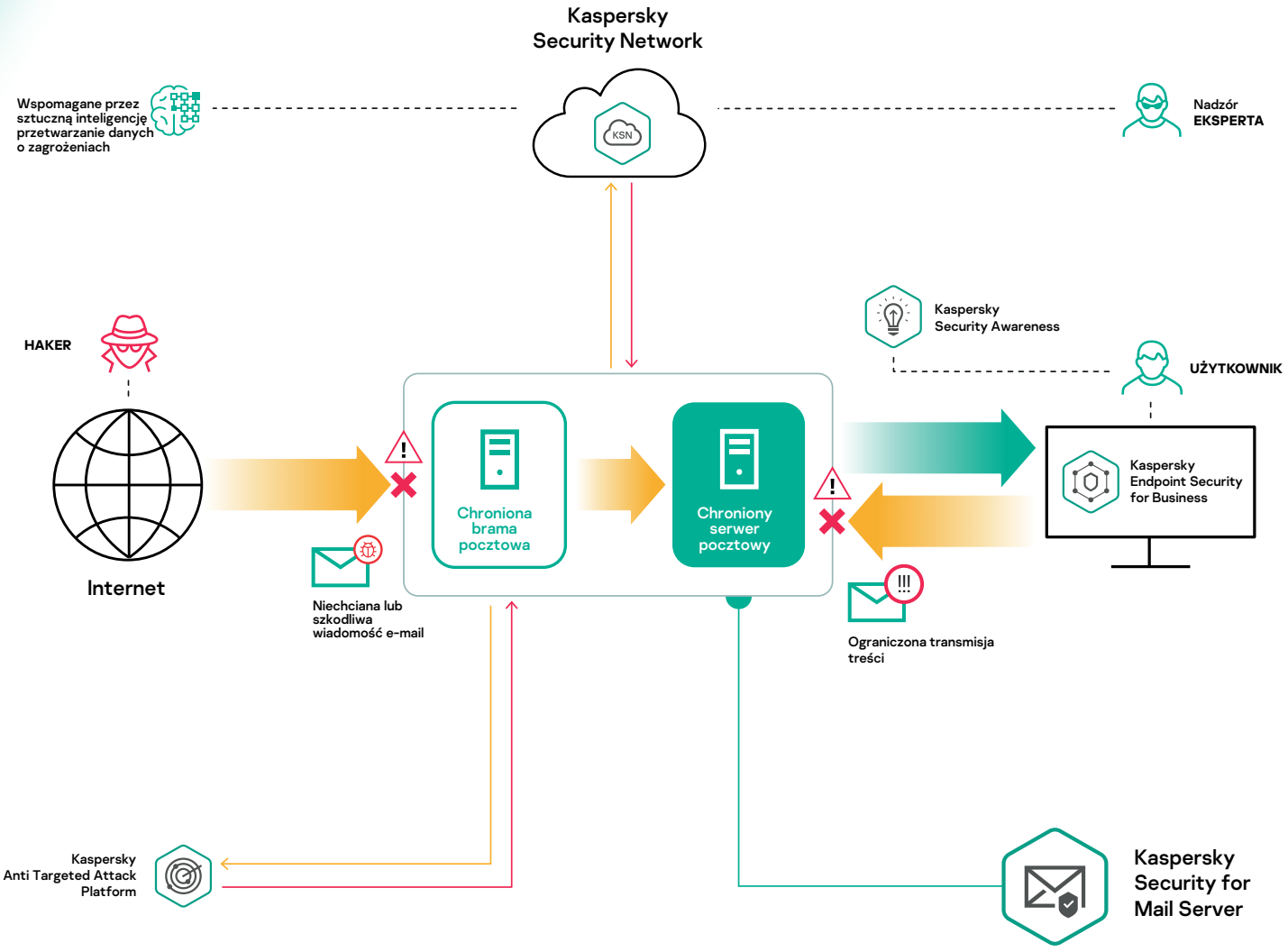
Wbudowana kopia zapasowa

Aby zapewnić, że żadne krytyczne dane nie zostaną utracone w wyniku leczenia lub usunięcia, oryginalne wiadomości mogą być zapisywane w magazynie kopii zapasowych do przetworzenia przez administratora w dogolnej chwili.
Można skonfigurować określone reguły dla warunkowej kopii zapasowej danych.

Zarządzanie i widoczność

Przejrzysty, przyjazny dla użytkownika interfejs sieciowy umożliwia administratorowi monitorowanie poziomu ochrony poczty firmowej za pomocą narzędzi takich jak:

- Elastyczne, ale łatwe w użyciu reguły i konfiguracja zasad.
- Integracja z Active Directory.
- Eksport zdarzeń do systemu SIEM.
- Diagnostyka stanu systemów.



Sposób przeciwdziałania Kaspersky Security for Mail Server cyberzagrożeniom przenoszonym przez pocztę e-mail

Silna ochrona z Kaspersky Security for Mail Server

Kaspersky Security for Mail Server to tylko jeden z wielu produktów i rozwiązań firmy Kaspersky Lab, które zostały stworzone wewnętrznie, przy wsparciu ponad 20 lat doświadczenia, zbudowanych na podstawie jednej bazy kodu i zaprojektowanych tak, aby płynnie się ze sobą łączyć w celu zapewnienia kompleksowej i niepodważalnej platformy ochrony.

Jeśli korzystasz już z Kaspersky Endpoint Security for Business, zainstalowanie Kaspersky Security for Mail Server możesz mieć pewność, że ochrona Twojej bramy pocztowej działa zgodnie z tymi samymi niezrównanymi standardami wydajności, co reszta zabezpieczeń.

Jeśli nie, teraz może być dobry moment, aby wzmocnić swoje granice i zbudować odporność instalując Kaspersky Security for Mail Server obok lub zamiast obecnej ochrony poczty e-mail.

Jak kupić

Kaspersky Security for Mail Server jest sprzedawany jako samodzielne rozwiązanie ukierunkowane lub jako dodatek dostępny tylko dla klientów korzystających z Kaspersky Endpoint Security for Business.

Aplikacje w pakiecie

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server

Licencja

Kaspersky Security for Mail Server jest dostępny jako:

- Licencja roczna
- Subskrypcja miesięczna

Może Cię również zainteresować…

Kaspersky Security for Microsoft Office365 — specjalnie zaprojektowany, aby wypełnić luki w zabezpieczeniach w ofercie Microsoft opartej na chmurze, w tym Outlook 365 i OneDrive.

Kaspersky Security for Internet Gateway — uzupełnij ochronę granic swojej poczty e-mail równie potężnymi zabezpieczeniami bramy internetowej — dostępny również w Kaspersky Total Security for Business
.

Kaspersky Endpoint Security for Business — nasze flagowe rozwiązanie zabezpieczające punkty końcowe, zapewniające najlepiej przetestowaną i najczęściej nagradzaną ochronę punktów końcowych na rynku.

Wypróbuj przed zakupem
Sprawdź Kaspersky Security for Mail Server bezpłatnie przez 30 dni.

Zapytaj o ofertę
Potrzebujesz uzyskać więcej informacji? Zostaw swoje dane, a skontaktujemy się z Tobą.

Kup przez naszego zaufanego Partnera
Chcesz dokonać zakupu? Wyszukaj Partnera w swojej okolicy.

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 www.kaspersky.pl/transparentnosc

Sprawdzony. Transparentny. Niezależny.