PRZEGLĄD

# CLOUD OFFICE SECURITY

Zaawansowana ochrona poczty e-mail, współpracy i pamięci masowej w chmurze z proaktywną ochroną przed zagrożeniami.

Progress. Protected.

# Czym jest **ESET Cloud Office Security?**

## ESET Cloud Office Security zapewnia zaawansowaną ochronę dla aplikacji Microsoft 365 i Google Workspace z najlepszymi możliwościami ochrony przed zagrożeniami typu zero-day.

ESET Cloud Office Security to nasze rozwiązanie z zakresu Zintegrowanego Bezpieczeństwa Poczty w Chmurze (Integrated Cloud Email Security, ICES) lub chmurowego, wykorzystującego interfejsy API, rozwiązania Email Security (Cloud-native, API-enabled Email Security, CAPES). Połączenie filtracji spamu, skanowania antywirusowego, ochrony przed phishingiem oraz zaawansowanej obrony z wykorzystaniem chmurowej piaskownicy pomaga chronić komunikację, współpracę i przestrzeń dyskową Twojej firmy. Nasza łatwa w obsłudze konsola w chmurze umożliwia przegląd wykrytych zagrożeń i natychmiast informuje Cię o każdym wykryciu.


Rozwiązanie posiada dedykowaną konsolę zarządzania, do której dostęp można uzyskać z dowolnego miejsca.

# Dlaczego warto wzmocnić ochronę narzędzi do współpracy?

Wraz z rosnącą popularnością chmurowej poczty e-mail i nasileniem ataków na skrzynki firmowe, wzmocnienie środków obrony staje się kluczowe. Zwiększ swoją odporność na cyberzagrożenia, wdrażając rozwiązanie chroniące Twoje narzędzia do współpracy. ESET Cloud Office Security zapewnia dodatkową, zaawansowaną warstwę ochrony, uzupełniając wbudowane zabezpieczenia Microsoftu i Google. Chroni firmę przed infekcjami, minimalizuje zakłócenia w pracy spowodowane niechcianymi wiadomościami oraz pomaga przeciwdziałać atakom ukierunkowanym i nieznanym wcześniej zagrożeniom – zwłaszcza ransomware.

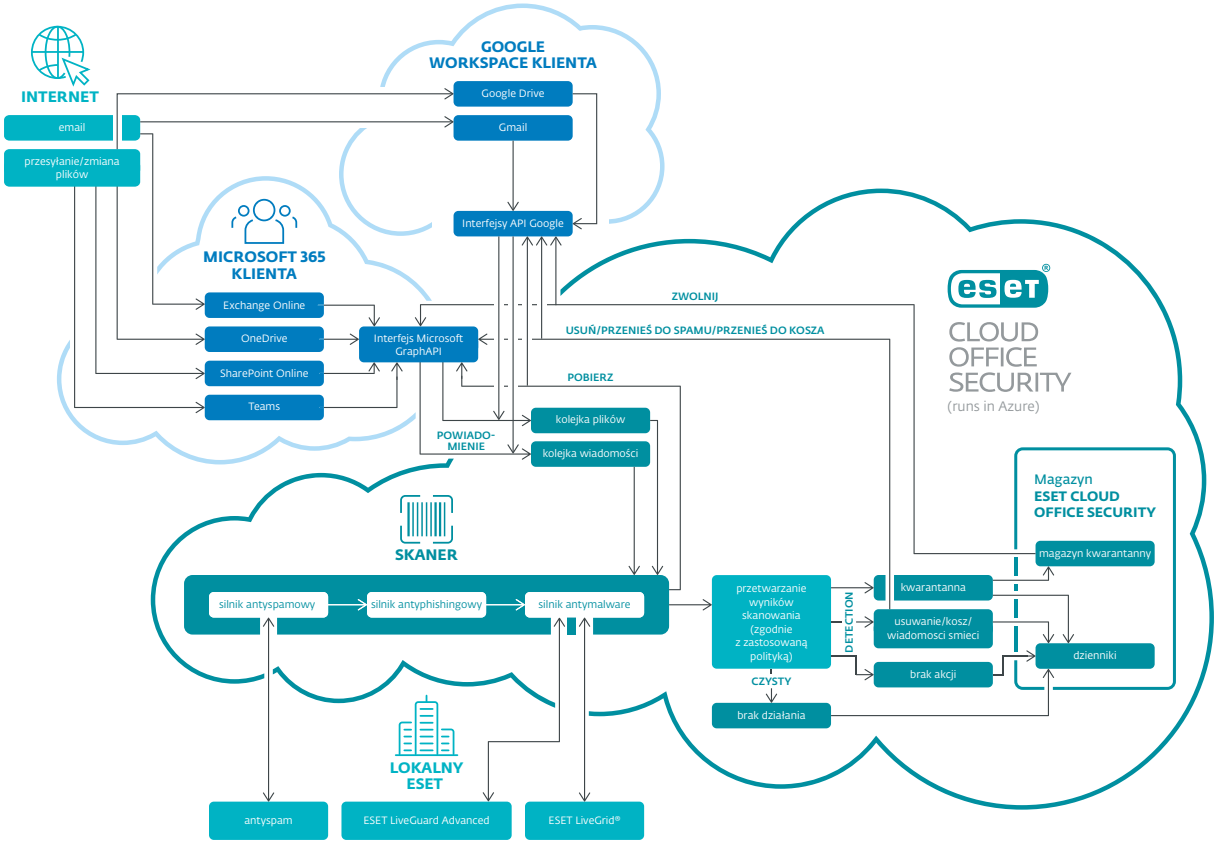
Skuteczność w liczbach*:

- ✓ Wykryto 1 300 000 zagrożeń w wiadomościach e-mail
- ✓ Zablokowano 3 000 000 wiadomości phishingowych
- ✓ Przechwycono 200 000 000 wiadomości spamowych
- ✓ 600 000 zagrożeń innych niż e-mailowe pochodziło z usług OneDrive, SharePoint, Teams i Google Drive

*Dane z 2025 r.

- Pomaga zapewnić wolną od infekcji komunikację oraz współpracę w firmie
- Minimalizuje negatywny wpływ niechcianych wiadomości na codzienną produktywność
- Zapobiega wykorzystywaniu nadchodzących z zewnątrz wiadomości e-mail jako kanału do ataków ukierunkowanych

# Jak to działa




Cybersecurity
Progress. Protected.

# Przykłady zastosowania

Właściciel firmy chce wdrożyć konkretne środki, aby zminimalizować ryzyko cyberzagrożeń i utrzymać ciągłość biznesu.

### ROZWIĄZANIE

- ✓ Administrator może sprawdzić liczbę spamu, złośliwego oprogramowania lub phishingu wykrytych przez ESET Cloud Office Security oraz ustalić, którzy użytkownicy są najczęściej celem ataków.
- ✓ Administrator może zauważyć, w jakich porach firma otrzymuje najwięcej spamu.
- ✓ W oparciu o dane administrator może przygotować raport zawierający istotne informacje dla kierownictwa.

Ransomware zazwyczaj dostaje się do skrzynek nieświadomych użytkowników poprzez wiadomości e-mail.

### ROZWIĄZANIE

- ✓ ESET Cloud Office Security automatycznie przesyła podejrzane załączniki wiadomości e-mail do ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced analizuje próbkę w odizolowanym środowisku chmurowej piaskownicy, a następnie przekazuje wynik z powrotem do ESET Cloud Office Security, zazwyczaj w ciągu pięciu minut.
- ✓ ESET Cloud Office Security wykrywa i automatycznie neutralizuje załączniki zawierające złośliwą zawartość.
- ✓ Złośliwy załącznik nie wyrządza szkód użytkownikowi ani firmowej sieci.

Częsta wymiana dużych plików w firmowej chmurze między pracownikami i osobami z zewnątrz.

### ROZWIĄZANIE

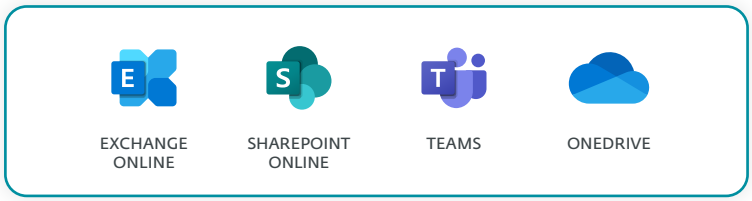
- ✓ Wrażliwe dane firmy przechowywane na OneDrive lub Google Drive wymagają dodatkowej warstwy zabezpieczeń.
- ✓ Administrator może aktywować rozwiązanie bezpieczeństwa w chmurze, takie jak ESET Cloud Office Security, aby chronić aplikacje Microsoft 365 lub Google Workspace.
- ✓ Zaawansowany silnik antywirusowy skanuje wszystkie nowe i modyfikowane pliki, zapobiegając rozprzestrzenianiu się złośliwego oprogramowania za pośrednictwem OneDrive lub Google Drive na wielu urządzeniach.

Potrzeby określonej grupy pracowników muszą być zrównoważone z koniecznością utrzymania bezpieczeństwa firmy.

### ROZWIĄZANIE

- ✓ Administrator może skonfigurować różne ustawienia ochrony dla każdej jednostki lub nawet dla poszczególnych użytkowników.
- ✓ Dzięki temu, jeśli w małym zespole w firmie istnieje potrzeba odbierania specyficznych wiadomości (np. newslettery marketingowe), administrator może przygotować odpowiednią politykę i wyłączyć filtr antyspamowy dla tej grupy.
- ✓ Firma nadal pozostaje chroniona przed złośliwym oprogramowaniem, a większość pracowników nie otrzymuje żadnego spamu.

# Protect emails and files shared or stored in the cloud




## ANTYSPAM

Obecnie wykorzystuje ulepszony, wielokrotnie nagradzany silnik o wyższej wydajności. Ten podstawowy komponent filtruje wszystkie wiadomości spam i utrzymuje skrzynki pocztowe wolne od niepożądanych i niechcianych wiadomości.

## ANTI-PHISHING

Rozwiązanie ESET Cloud Office Security zapobiega odwiedzaniu przez użytkowników stron phishingowych poprzez skanowanie tematu i treści przychodzących wiadomości e-mail w poszukiwaniu podejrzanych linków (adresów URL). Linki te są porównywane z stale aktualizowaną bazą danych znanych stron phishingowych.

## ANTIMALWARE

Skanuje wszystkie przychodzące wiadomości i załączniki, a także wszystkie nowe i zmienione pliki. Dzięki temu skrzynki pocztowe użytkowników pozostają wolne od złośliwego oprogramowania, a jego rozprzestrzenianie się poprzez chmurowe magazyny danych na wielu urządzeniach jest zablokowane.

## SANDBOXING W CHMURZE

Technologia oparta na chmurze, wykorzystująca zaawansowane skanowanie, najnowocześniejszą sztuczną inteligencję, środowisko testowe w chmurze oraz dogłębną analizę behawioralną w celu zapobiegania ukierunkowanym atakom i nowym, nieznanym dotąd zagrożeniom, zwłaszcza oprogramowaniu ransomware. Rozwiązanie ESET LiveGuard Advanced zapewnia proaktywną ochronę przed atakami typu zero-day wraz z autonomiczną naprawą.

## ANTISPOOFING

Oparte na solidnym silniku reguł rozwiązanie antispoofingowe chroni organizację poprzez wykrywanie i blokowanie fałszywych wiadomości e-mail, które podszywają się pod wiarygodne źródła. Zapewnia bezpieczną komunikację i pomaga zapobiegać atakom phishingowym dzięki zaawansowanej technologii weryfikacji wiadomości e-mail.

## WYKRYWANIE ZŁOŚLIWYCH KODÓW QR

Wykrywa potencjalne ataki typu „quishing" poprzez identyfikację kodów QR w wiadomościach e-mail, wyodrębnianie osadzonych w nich linków oraz skanowanie ich za pomocą silników antyphishingowych, antywirusowych i antyspamowych firmy ESET. Pomaga to blokować złośliwe adresy URL, zanim użytkownicy będą mieli do nich dostęp.

## OCHRONA PRZED ATAKAMI POPRZEZ KALENDARZ

Sprawdza zaproszenia kalendarzowe i powiązane wiadomości e-mail pod kątem spamu, linków phishingowych, złośliwego oprogramowania, podejrzanych załączników oraz osadzonych kodów QR. W przypadku wykrycia zagrożenia zarówno wiadomość e-mail, jak i wydarzenie w kalendarzu są automatycznie usuwane, co zapobiega dotarciu fałszywych zaproszeń na spotkania do użytkowników.

## OCHRONA PRZED HOMOGLYFAMI

Sprawdza wiadomości e-mail pod kątem znaków z innych alfabetów, np. cyrylicy i greckiego, które wyglądają identycznie jak znaki łacińskie, a jednak są inne, co powoduje przekierowanie na złośliwy adres. Dzięki temu Twoja organizacja jest lepiej chroniona przed atakami polegającymi na podszywaniu się pod legalne adresy e-mail, co zwiększa ogólne bezpieczeństwo poczty elektronicznej.

## KONTROLA DOSTĘPU OPARTA NA ROLACH

Umożliwia precyzyjne przypisywanie uprawnień użytkownikom w oparciu o role, co pomaga chronić poufne dane

i zapewnić zgodność z przepisami. Rozwiązanie to, zaprojektowane z myślą o instytucjach rządowych, przedsiębiorstwach i dostawcach usług zarządzanych (MSP), oferuje szczegółową kontrolę dostępu opartą na rolach. Na przykład uniemożliwia młodszemu analitykowi uzyskać dostęp do wiadomości e-mail działu kadr. Poziomy dostępu można dostosować do zakresu obowiązków użytkownika, zapewniając organizacjom pełną kontrolę przy minimalnym stopniu złożoności.

## NATYWNA WIELODOSTĘPNOŚĆ ORAZ WSPARCIE DLA MSP

ESET Cloud Office Security został zaprojektowany od podstaw z myślą o wielodostępowym zarządzaniu nawet dziesiątkami tysięcy użytkowników. Dzięki temu ECOS doskonale sprawdza się nie tylko w małych i średnich firmach, ale także u dostawców usług zarządzanych (MSP).

## MENEDŻER KWARANTANNY

Administratorzy mogą sprawdzać obiekty w tym obszarze magazynu kwarantanny i decydować, czy je usunąć, czy przywrócić. Ta funkcja pozwala łatwo zarządzać wiadomościami i plikami poddanymi kwarantannie przez nasze rozwiązanie. Dodatkowo administratorzy mogą pobierać te elementy i analizować je przy użyciu innych narzędzi lokalnie.

## AUTOMATYCZNA OCHRONA

Dzięki włączeniu tej opcji administratorzy mogą mieć pewność, że nowi użytkownicy tworzeni w dzierżawach Microsoft 365 i Google Workspace zostaną automatycznie objęci ochroną, bez konieczności osobnego dodawania ich w konsoli.

## REGUŁY E-MAILOWE Z GOTOWYMI SZABLONAMI

Oszczędzają czas i usprawniają zarządzanie regułami e-mailowymi dzięki gotowym do użycia szablonom, które można natychmiast włączyć i dostosować do własnych potrzeb – nie ma potrzeby zaczynać od zera. Inteligentne reguły oferują zaawansowane zmienne wykraczające poza standardowe opcje, zapewniając większą elastyczność i kontrolę przy minimalnym wysiłku. Idealne rozwiązanie dla użytkowników poszukujących zaawansowanej automatyzacji bez dodatkowej złożoności.

## POWIADOMIENIA

Kiedy ESET Cloud Office Security wykryje nową, podejrzaną aktywność, może natychmiast wysłać wiadomość e-mail do administratorów lub użytkowników, aby poinformować ich o zagrożeniu.

## FUNKCJA ODZYSKIWANIA MAILI

Szybko i łatwo izoluje potencjalnie złośliwe wiadomości e-mail, chroniąc organizację przed zagrożeniami przenoszonymi za pośrednictwem poczty elektronicznej i minimalizując przestoje. Wycofane wiadomości e-mail można przywrócić jednym kliknięciem.

## ZAWIESZENIE KONTA UŻYTKOWNIKA

Umożliwia administratorom natychmiastowe zawieszenie kont, co do których istnieje podejrzenie włamania, poprzez wylogowanie użytkowników i zablokowanie dalszego dostępu do czasu zakończenia dochodzenia. Żadne dane nie są usuwane, ale dostęp do wiadomości e-mail i plików zostaje zablokowany, co pomaga zapobiegać naruszeniom bezpieczeństwa lub wyciekom danych w trakcie opanowywania incydentu.

# WYPRÓBUJ ZANIM KUPISZ

Wypróbuj nasze zaawansowane rozwiązanie zapewniające dodatkową warstwę ochrony dla usług Microsoft 365 i Google Workspace. Przekonaj się, jak szybko i łatwo można je wdrożyć. Sprawdź jego niezawodność, wygodę i łatwość zarządzania. Skontaktuj się z naszymi ekspertami, aby zamówić bezpłatną subskrypcję próbną obejmującą do 25 stanowisk.

# Funkcje

| | | |
|---|---|---|
| **OCHRONA USŁUGI EXCHANGE ONLINE I GMAIL** | OCHRONA PRZED SPAMEM | ✓ |
| | OCHRONA PRZED PHISHINGIEM | ✓ |
| | OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM | ✓ |
| | ANTISPOOFING | ✓ |
| | KWARANTANNA | ✓ |
| | DYNAMICZNA OCHRONA PRZED ZAGROŻENIAMI | ✓ |
| **OCHRONA DLA APLIKACJI TEAMS I SHAREPOINT ONLINE** | OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM | ✓ |
| | KWARANTANNA | ✓ |
| | DYNAMICZNA OCHRONA PRZED ZAGROŻENIAMI | ✓ |
| **OCHRONA USŁUGI ONEDRIVE FOR BUSINESS I GOOGLE DRIVE** | OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM | ✓ |
| | KWARANTANNA | ✓ |
| | DYNAMICZNA OCHRONA PRZED ZAGROŻENIAMI | ✓ |
| **CHMUROWA KONSOLA ZARZĄDZAJĄCA** | ZARZĄDZANIE LICENCJAMI | ✓ |
| | AUTOMATYCZNA OCHRONA | ✓ |
| | PANEL ZE STATYSTYKAMI BEZPIECZEŃSTWA | ✓ |
| | POWIADOMIENIA E-MAILOWE O WYKRYTYCH ZAGROŻENIACH | ✓ |
| | ZAAWANSOWANE FILTROWANIE WYKRYTYCH ZAGROŻEŃ | ✓ |
| | ZARZĄDZANIE KWARANTANNĄ | ✓ |
| | USTAWIENIA OCHRONY OPARTE NA ZASADACH | ✓ |
| | KONTROLA DOSTĘPU OPARTA NA ROLACH | ✓ |
| | OBSŁUGA WIELU UŻYTKOWNIKÓW | ✓ |
| | MOŻLIWOŚĆ KONFIGURACJI RAPORTÓW | ✓ |
| | REGUŁY E-MAILOWE Z GOTOWYMI SZABLONAMI | ✓ |
| | LOKALIZACJA NA 21 JĘZYKÓW | ✓ |
| | DOSTĘPNY TRYB CIEMNY | ✓ |
| | PANELE NADZORU Z MOŻLIWOŚCIĄ DOSTOSOWANIA | ✓ |

# To jest ESET

## Proaktywna ochrona. Minimalizuj ryzyko dzięki podejściu prewencyjnemu.

Bądź o krok przed znanymi i pojawiającymi się cyberzagrożeniami, takimi jak ukierunkowane ataki, zagrożenia typu zero-day, oprogramowanie ransomware, phishing i inne. To możliwe, dzięki naszemu podejściu opartemu na sztucznej inteligencji, które stawia na pierwszym miejscu zapobieganie. ESET łączy sztuczną inteligencję i ludzką wiedzę specjalistyczną, aby zapewnić łatwą i skuteczną ochronę.

Skorzystaj z najlepszych w swojej klasie, opartych na badaniach naukowych zabezpieczeniach, popartych ponad 30-letnim doświadczeniem w zakresie globalnej analizy cyberzagrożeń. Rozległa sieć badawczo-rozwojowa, kierowana przez uznanych w branży naukowców, stanowi podstawę naszej wielokrotnie nagradzanej platformy cyberbezpieczeństwa opartej na chmurze. Rozwiązania ESET są wysoce konfigurowalne, obejmują lokalne wsparcie techniczne i mają minimalny wpływ na wydajność.

ESET chroni Twój biznes, dzięki czemu możesz w pełni wykorzystać możliwości nowoczesnych technologii.

## ESET W LICZBACH

**1 mld+**
**chronionych użytkowników internetu**

**500 tys.+**
**klientów biznesowych**

**178**
**krajów**

**11**
**globalnych centrów badawczo-rozwojowych**

## WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

chroniony przez ESET od 2017 roku; ponad 9 500 stacji roboczych

BVB 09

chroniony przez ESET od 2019 roku; ponad 1 200 stacji roboczych & 2 700 skrzynek pocztowych

Canon
Canon Marketing Japan Group

chroniony przez ESET od 2016 roku; ponad 23 000 stacji roboczych

Partner ISP w zakresie bezpieczeństwa od 2008 r. 2 miliony klientów

## WYRÓŻNIENIA

SE LABS ®
AWARDS
Enterprise Endpoint (Windows)
WINNER 2025

Zwycięzca nagród SE LABS Awards 2025 w kategorii **najlepszego rozwiązania dla przedsiębiorstw** i **najlepszego rozwiązania dla małych firm**

Gartner
Peer Insights
**Customers' Choice** 2026

Wyróżniony jako **Wybór Konsumentów** w raporcie Gartner® Peer Insights™ „**Voice of the Customer" Endpoint Protection Platforms** w 2026 roku

FROST & SULLIVAN

Uznany za **lidera** we Frost Radar: Endpoint Security 2025, wykazując się doskonałością w zakresie wzrostu i innowacji