WYPRODUKOWANE
**W UNII EUROPEJSKIEJ**
ROZWIJANE
**W POLSCE**

**4** MILIONY KLIENTÓW W POLSCE

# FILE SECURITY

Bezkompromisowe wielowarstwowe rozwiązanie
do ochrony serwerów plikowych

CYBERSECURITY
EXPERTS ON YOUR SIDE

# Jak działa rozwiązanie **file security?**

**Produkt File Security chroni serwery organizacji przed zagrożeniami. Jest on przeznaczony do instalacji na serwerach w celu ochrony firmowych zasobów przed zainfekowaniem. Współcześnie wiele firm podejmuje bardzo duże ryzyko, pozwalając użytkownikom na zapisywanie plików w sieci firmowej, nie dbając przy tym o odpowiednie zabezpieczenie współdzielonych zasobów firmowych przed złośliwym oprogramowaniem. Wystarczy, że jeden użytkownik zapisze złośliwy plik na dysku sieciowym, żeby narazić na ryzyko infekcji pozostałych pracowników, a nawet doprowadzić do zaszyfrowania przez ransomware wszystkich danych organizacji.**

Rozwiązanie **ESET File Security** zapewnia zaawansowaną ochronę przed zagrożeniami wszystkich serwerów ogólnego przeznaczenia, dysków sieciowych i serwerów wielofunkcyjnych. Pomaga zapewnić ich stabilne i bezkonfliktowe działanie, minimalizując liczbę koniecznych restartów oraz związanych z nimi przerw technicznych. W ten sposób umożliwia utrzymanie ciągłości działania sieci firmowej i samej firmy.

# Dlaczego warto wybrać **rozwiązania File Security?**

## RANSOMWARE

Od pierwszego ataku Cryptolockera w 2013 r. wirusy szyfrujące ransomware stanowią jedno z najpoważniejszych zagrożeń dla sieci firmowych. Chociaż oprogramowanie tego typu istniało już wcześniej, to firmy przez długi czas nie traktowały ryzyka związanego z możliwością ataku z jego wykorzystaniem za wystarczająco poważne. Dzisiaj, kiedy pojedynczy przypadek zaszyfrowania ważnych plików może zatrzymać pracę przedsiębiorstwa, wygląda to zupełnie inaczej. Wiele firm po infekcji spowodowanej ransomware szybko zdaje sobie sprawę, że posiadane przez nie kopie bezpieczeństwa nie są wystarczająco aktualne, by można z nich było skorzystać, w związku z czym decydują się zapłacić okup.

W przypadku serwerów plików ransomware stanowi jeszcze większe niebezpieczeństwo, ponieważ zagrożenie szyfrujące może zostać zapisane na dyskach sieciowych firmy przez samych użytkowników. ESET File Security oferuje wielowarstwową ochronę, która nie tylko zapobiega infekcjom ransomware, ale też wykrywa czy tego typu wirus był kiedykolwiek obecny w sieci firmowej. Zapobieganie, wykrywanie i blokowanie ataków ransomware ma ogromne znaczenie, ponieważ każdy zapłacony przez firmy okup przekonuje cyberprzestępców, że warto korzystać z tego typu wirusów.

## ATAKI UKIERUNKOWANE I NARUSZENIA BEZPIECZEŃSTWA DANYCH

Współczesne cyberzagrożenia i ataki stale ewoluują. Firmy, które padają ofiarą cyberprzestępców, są zazwyczaj albo zaskoczone, że ktoś ominął ich zabezpieczenia, albo zupełnie nieświadome zaistnienia incydentu w ich sieci firmowej. Dopiero po wykryciu ataku zaczynają reaktywnie wprowadzać środki zaradcze, które mają przeciwdziałać podobnym zdarzeniom w przyszłości. W większości przypadków firmy nie chronią się jednak przed kolejnymi typami zagrożeń, które mogą wykorzystać nowe wektory ataku.

ESET File Security wykorzystuje informacje o zagrożeniach zebrane przez swoje rozwiązania, zainstalowane na komputerach użytkowników na całym świecie. W ten sposób możliwe jest priorytetyzowanie i skuteczne blokowanie najnowszych zagrożeń, jeszcze zanim dotrą do firmowej sieci. To istotne, ponieważ cyberprzestępcy chętnie wybierają na swój cel serwery firmowe. Wszystko dlatego, że zawierają one na tyle ważne dla firmy dane, że te często decydują się zapłacić okup. Aby lepiej chronić przed atakami ransomware ESET File Security korzysta ze swojego autorskiego i chmurowego systemu wczesnego ostrzegania, dzięki któremu może błyskawicznie zablokować najnowsze typy zagrożeń, bez konieczności czekania na aktualizację silnika detekcji.

## ATAKI BEZPLIKOWE

Najnowsze typy zagrożeń, tzw. bezplikowe, działają wyłącznie w pamięci komputera, przez co niemożliwym staje się wykrycie ich tradycyjnymi metodami skanowania plików. Dodatkowo niektóre tego typu wirusy wykorzystują do swojego działania aplikacje wbudowane w system operacyjny, przez co są jeszcze trudniejsze do rozpoznania i blokowania. Dla przykładu ataki z wykorzystaniem PowerShell są bardzo popularne.

ESET File Security jest w stanie wykryć zmodyfikowane lub przejęte przez wirusy aplikacje i ochronić w ten sposób sieć firmową przed tego typu atakami. Inne rozwiązania wykorzystują w tym celu specjalnie tworzone skanery, które nieustannie monitorują pamięć pod kątem jakiejkolwiek podejrzanej aktywności. ESET File Security jest stale rozwijane, tak by pozostawać o krok przed najnowszymi typami złośliwego oprogramowania.

ESET File Security oferuje wielowarstwową ochronę, która nie tylko zapobiega infekcjom ransomware, ale też wykrywa czy tego typu wirus był kiedykolwiek obecny w sieci firmowej.

Firmy, które padają ofiarą cyberprzestępców, są zazwyczaj albo zaskoczone, że ktoś ominął ich zabezpieczenia, albo zupełnie nieświadome zaistnienia incydentu w ich sieci firmowej.

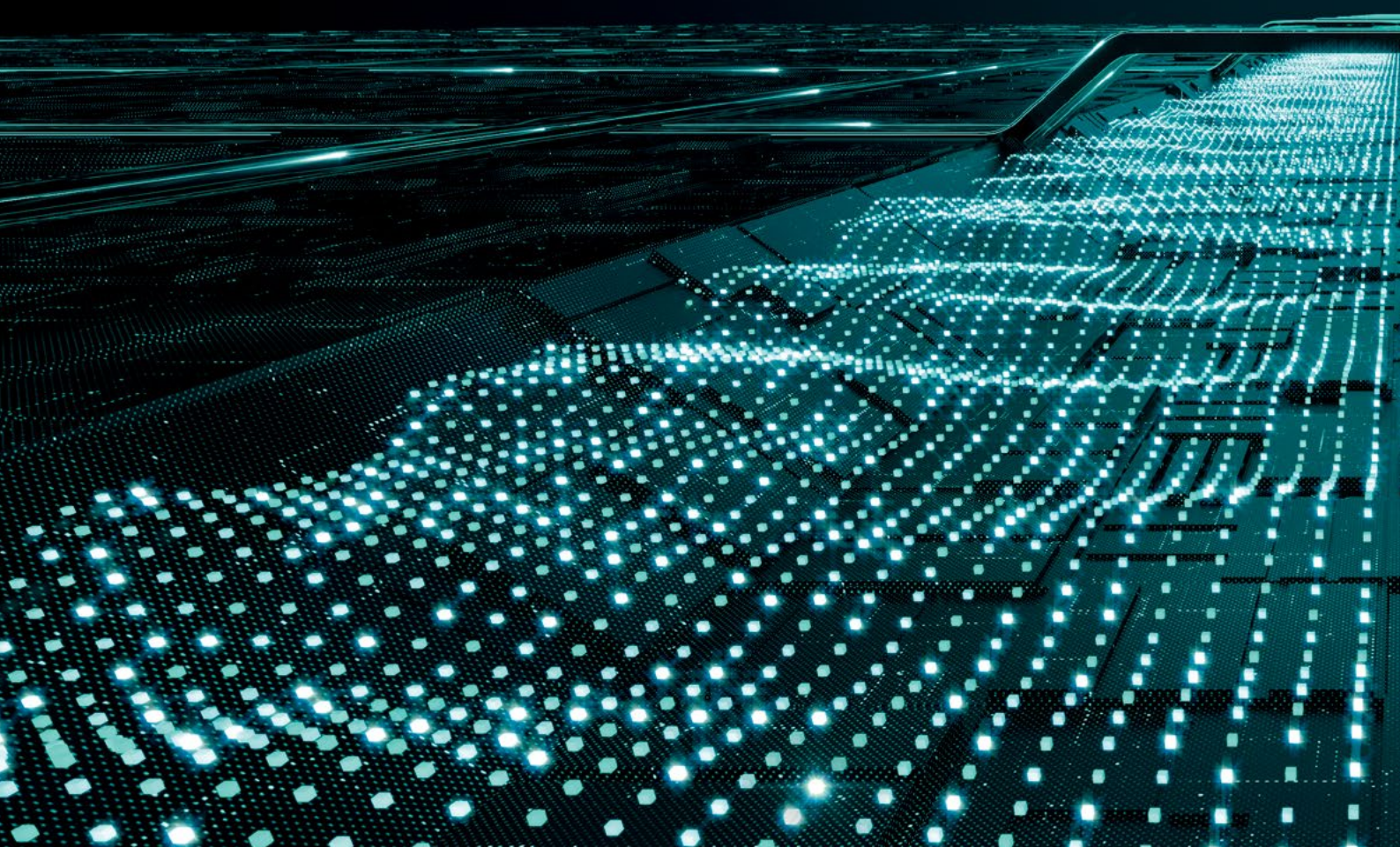
Najnowsze typy zagrożeń, tzw. bezplikowe, działają wyłącznie w pamięci komputera, przez co niemożliwym staje się wykrycie ich tradycyjnymi metodami skanowania plików.

*„ESET od lat chroni naszą firmę przed zagrożeniami. Robi dokładnie to, co powinien, a my nie musimy się niczym martwić. Krótko mówiąc, ESET to: jakość i niezawodność."*

—Jos Savelkoul, Team Leader ICT-Department; Szpital w Zuyderland, Holandia
licencja dla ponad 10 000 stanowisk

# Dostępne wersje ESET File Security

ESET File Security dla systemu Microsoft Windows Server
ESET File Security dla systemu Linux
ESET File Security dla platformy Microsoft Azure



# Poczuj różnicę z ESET

## WIELOWARSTWOWA OCHRONA

ESET zapewnia wielowarstwową ochronę, łącząc w sobie wiele technologii, w tym m.in. uczenie maszynowe, rozbudowując je o wiedzę i doświadczenie światowej klasy ekspertów z branży bezpieczeństwa IT. W ten sposób zapewnia swoim klientom najwyższy poziom ochrony. Nasze technologie nieustannie się zmieniają, dostosowując się do wymagań rynku, zapewniając przy tym skuteczność ochrony, przy niemal niezmienionej wydajności chronionego urządzenia i prawidłowym odróżnianiu bezpiecznych plików od zagrożeń.

## WSPARCIE DLA WIELU SYSTEMÓW OPERACYJNYCH

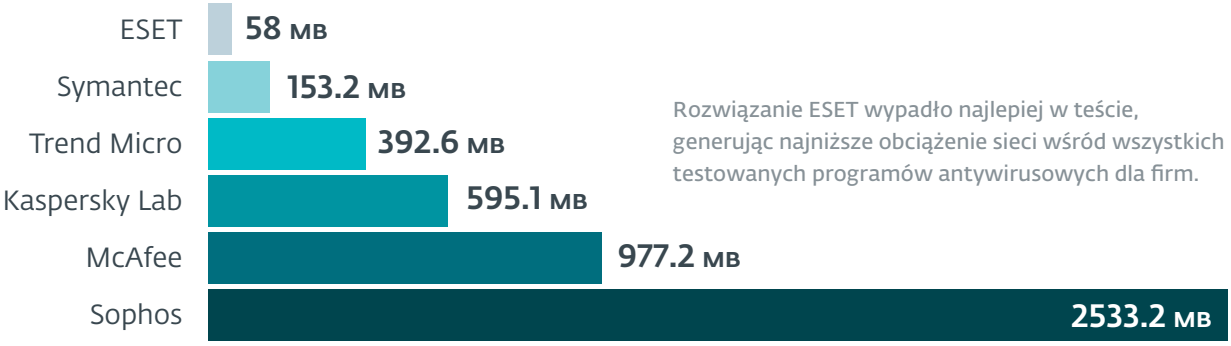
ESET File Security wspiera różne systemy operacyjne i platformy, w tym Windows Server, Office 365, OneDrive, Linux i Microsoft Azure. Wszystkie produkty firmy ESET mogą być w pełni zarządzane za pomocą jednej konsoli do centralnej administracji.

## NIEZRÓWNANA WYDAJNOŚĆ

Wyzwaniem dla wielu firm jest znalezienie rozwiązania typu Endpoint Protection, które chroniąc stacje robocze, utrzyma ich wydajność na niemal niezmienionym poziomie. Produkty ESET wielokrotnie doceniono w testach niezależnych organizacji badawczych, właśnie z uwagi na niezauważalny wpływ na wydajność chronionych urządzeń.

## GLOBALNY ZASIĘG

Rozwiązania ESET są obecne w ponad 200 krajach. Firma posiada 13 laboratoriów badawczo-rozwojowych, w tym jedno w Krakowie, oraz 22 biura rozlokowane na całym świecie. Globalna obecność ESET pomaga w skutecznym powstrzymywaniu złośliwego oprogramowania przed rozprzestrzenianiem się na całym świecie, a także w opracowywaniu technologii wykrywania nowych zagrożeń i podatności.




Rozwiązanie ESET wypadło najlepiej w teście, generując najniższe obciążenie sieci wśród wszystkich testowanych programów antywirusowych dla firm.

Źródło: AV-Comparatives: Network Performance Test, Business Security Software

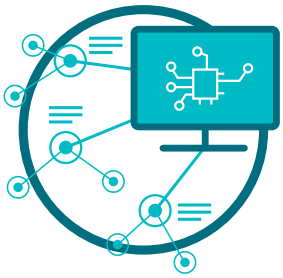
*„...najlepszy dowód? Statystyki naszej pomocy technicznej: po wdrożeniu rozwiązania ESET nasz dział wsparcia nie rejestruje już żadnych zgłoszeń – nie muszą rozwiązywać żadnych problemów z działaniem antywirusa czy złośliwym oprogramowaniem!"*

— Adam Hoffman, Kierownik ds. Architektury IT; Mercury Engineering, Irlandia

1 300 stanowisk

# Technologia

## Działanie naszych rozwiązań opiera się na trzech filarach



### UCZENIE MASZYNOWE

ESET wykorzystuje efekt synergii jaki wynika z połączenia możliwości zaawansowanych sieci neuronowych i starannie dobranych algorytmów sztucznej inteligencji do prawidłowego identyfikowania i oznaczania otrzymywanych plików jako bezpieczne, potencjalnie niechciane lub złośliwe.

### ESET LIVEGRID®

Za każdym razem, gdy zagrożenie typu zero-day, takie jak ransomware, zostanie wykryte przez nasze rozwiązanie gdzieś na świecie, jest ono przesyłane do naszego chmurowego systemu wczesnego ostrzegania przed złośliwym oprogramowaniem – ESET LiveGrid®. Wewnątrz niego następuje symulacja działania zagrożenia i sprawdzenie w jaki sposób zachowuje się podejrzany plik po jego uruchomieniu. Wyniki takiej analizy są dostarczane do komputerów chronionych rozwiązaniami ESET na całym świecie, bez konieczności dodatkowej aktualizacji silnika detekcji.

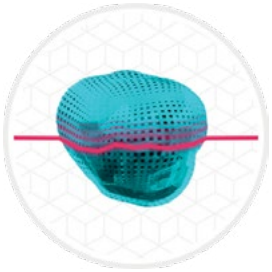
### WIEDZA EKSPERTÓW

Światowej klasy eksperci ds. bezpieczeństwa z ESET dzielą się swoim doświadczeniem i unikatową wiedzą, aby zapewnić użytkownikom ESET najlepszą ochronę przez całą dobę, każdego dnia tygodnia.

Pojedyncza warstwa ochrony w oprogramowaniu zabezpieczającym dla firm nie jest wystarczająca. Aby zapewnić skuteczną ochronę przed dynamicznie rozwijającymi się zagrożeniami, produkty ESET Endpoint korzystają z licznych technologii, które potrafią wykrywać zagrożenia przed ich aktywowaniem, w momencie inicjalizacji ich działania oraz po zakończeniu pracy złośliwego kodu. Możliwość detekcji zagrożenia w dowolnej fazie cyklu jego życia pozwala zapewnić klientom ESET najwyższy poziom ochrony.

## UCZENIE MASZYNOWE

Wszystkie produkty biznesowe ESET od 1997 roku pracują w oparciu o zaawansowane algorytmy uczenia maszynowego, które wspierają wszystkie obecne w produktach ESET warstwy ochrony. Uczenie maszynowe ma istotny udział w procesie analizy nieznanych próbek, pozwalając błyskawicznie ocenić czy stanowi ona zagrożenie, czy też jest bezpiecznym plikiem.



## ZAAWANSOWANY SKANER PAMIĘCI

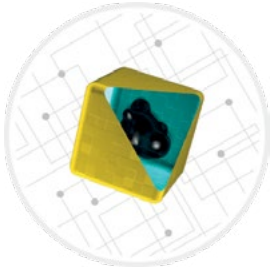
Zaawansowany skaner pamięci ESET monitoruje zachowanie podejrzanych procesów i skanuje je w momencie, gdy ujawnią się w pamięci komputera. Skaner ten pozwala na wykrycie zagrożenia, którego nie da się wykryć konwencjonalnymi metodami. Jedynie tego typu skaner może z powodzeniem wykryć i zneutralizować ataki bezplikowe.

## RANSOMWARE SHIELD

ESET Ransomware Shield to dodatkowa warstwa chroniąca użytkowników przed złośliwym oprogramowaniem ransomware. Ta technologia pozwala monitorować i weryfikować wszystkie uruchamiane aplikacje w oparciu o ich zachowanie i reputację. Jest przeznaczona do wykrywania i blokowania procesów przypominających swoim zachowaniem działanie oprogramowania ransomware.

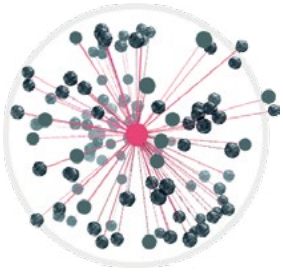
## EXPLOIT BLOCKER

ESET Exploit Blocker monitoruje aplikacje narażone na ataki exploitów (m.in. przeglądarki, czytniki dokumentów, programy pocztowe, Flash, Java i inne) i zamiast skupiać się tylko na identyfikatorach luk CVE, koncentruje się na rozpoznawaniu technik wykorzystywanych przez exploity. W momencie wykrycia przez ESET próby wykorzystania exploitu, zagrożenie jest natychmiast blokowane.



## SANDBOXING

Dzisiejsze zagrożenia często kamuflują swoje działania, starając się w ten sposób uniknąć wykrycia. W celu sprawdzenia ich rzeczywistego zachowania, rozwiązania ESET wykorzystują tzw. sandboxing, który symuluje ich działanie w wyizolowanym od systemu operacyjnego środowisku.

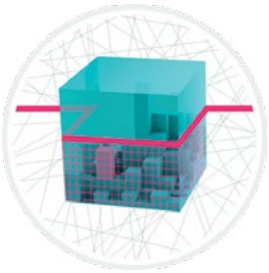


## OCHRONA PRZED BOTNETAMI

ESET Botnet Protection to funkcjonalność, która wykrywa złośliwą komunikację wykorzystywaną przez sieci komputerów zombie, czyli tzw. botnety. Każda zidentyfikowana podejrzana próba komunikacji jest blokowana i zgłaszana użytkownikowi.

## OCHRONA PRZED ATAKAMI SIECIOWYMI

Kolejna warstwa ochrony programów ESET identyfikuje luki w protokołach sieciowych i blokuje ich wykorzystanie. Dzięki temu zapewniona jest ochrona przed atakami, na które nie powstała jeszcze stosowna poprawka do systemu operacyjnego.



## AMSI/SKANOWANIE SKRYPTÓW

Rozwiązania ESET wykorzystują Antimalware Scan Interface (AMSI) by zapewnić jeszcze wyższy poziom ochrony przed złośliwym oprogramowaniem dla użytkowników, danych, aplikacji i procesów. Dodatkowo programy ESET wspierają interfejs usług chronionych, czyli nowy moduł wbudowany w system Windows, pozwalający na uruchomienie wyłącznie zaufanego, podpisanego certyfikatem kodu, przeciwdziałając tym samym atakom typu „code injection".

## ANALIZA DNA ZAGROŻEŃ

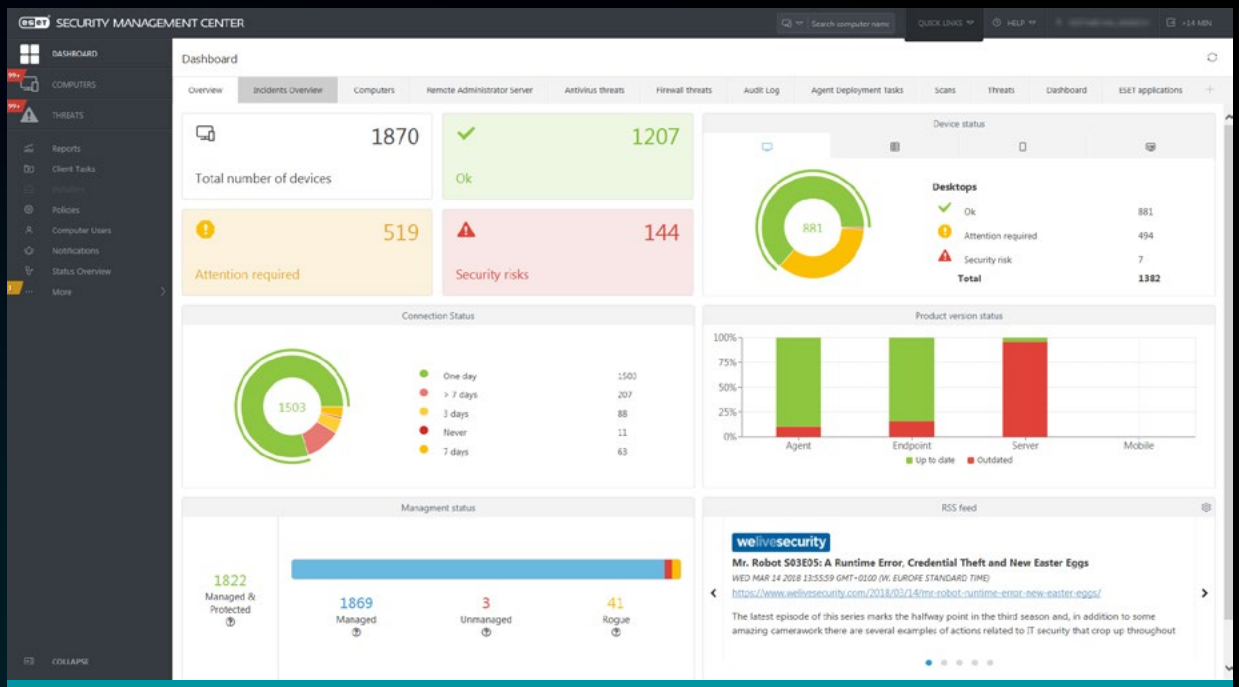
Rozwiązania ESET korzystają z różnych mechanizmów wykrywania zagrożeń, począwszy od porównywania tzw. hashy, aż po analizę DNA zagrożeń. Ta ostatnia metoda pozwala rozpoznać niebezpieczny kod po jego zachowaniu. Same złośliwe oprogramowanie można bowiem łatwo modyfikować i zaciemniać jego kod, uniemożliwiając w ten sposób jego wykrycie. Dzięki identyfikacji zagrożenia na podstawie jego DNA, tego typu sztuczki nie wpływają na możliwość wykrywania złośliwej zawartości.

## SYSTEM HIPS

System zapobiegania włamaniom działający na hoście (HIPS) monitoruje zachowanie systemu operacyjnego i wykorzystuje predefiniowane reguły pod kątem rozpoznania podejrzanego zachowania. W razie wykrycia takiej aktywności HIPS od razu ją blokuje.

*„Największą zaletą rozwiązania jest jego duża przewaga techniczna nad innymi produktami na rynku. ESET zapewnia nam niezawodne zabezpieczenia, co oznacza, że mogę pracować nad dowolnym projektem w dowolnym momencie, wiedząc, że nasze komputery są chronione w 100 proc."*

— Fiona Garland, Business Analyst Group IT; Mercury Engineering, Irlandia
1 300 stanowisk




## ESET Security Management Center

Produkty ESET do ochrony stacji roboczych, urządzeń mobilnych i serwerów są zarządzane za pośrednictwem konsoli ESET Security Management Center, instalowanej w systemie Windows lub Linux. Konsola dostępna jest również w postaci obrazu maszyny wirtualnej, dzięki czemu można ją szybko wdrożyć bez potrzeby instalacji.

*"Kiedy odkryliśmy ESET, wiedzieliśmy, że to dobry wybór: niezawodna technologia, skuteczne wykrywanie, obecność na lokalnym rynku i świetne wsparcie techniczne, czyli wszystko to, czego potrzebowaliśmy."*

— Ernesto Bonhoure, Kierownik ds. infrastruktury IT; Szpital Alemán, Argentyna, 1 500+ stanowisk

# Zastosowanie

## Ataki bezplikowe

**Przypadek zastosowania:** Ataki bezplikowe to stosunkowo nowe zagrożenia, które funkcjonują wyłącznie w pamięci systemu lub komputera. To sprawia, że wymagają one innego podejścia od tego stosowanego dla tradycyjnych zagrożeń opartych na plikach.

### ROZWIĄZANIE

- ✓ Zaawansowany skaner pamięci, zaimplementowany w rozwiązaniach ESET, chroni system przed takimi atakami, monitorując zachowanie procesów, blokując złośliwe działania, kiedy ujawnią się w pamięci komputera.
- ✓ W przypadku braku pewności czy dany element stanowi zagrożenie, próbka może zostać wysłana do usługi sandboxingu w chmurze (ESET Dynamic Threat Defense) gdzie poddawana jest specjalistycznej analizie pod kątem złośliwego charakteru
- ✓ W przypadku potwierdzenia złośliwego charakteru danego procesu informacje na ten temat zostają przekazane do chmurowego systemu reputacyjnego ESET Threat Intelligence, aby skrócić czas potrzebny na jego dokładną analizę.

## Ataki zero-day

**Przypadek zastosowania:** Ataki zero-day, a więc infekcje nowymi, nierozpoznanymi dotąd zagrożeniami, to poważny problem dla firm.

### ROZWIĄZANIE

- ✓ ESET Threat Intelligence daje wszystkim programom ESET dostęp do danych o najnowszych zagrożeniach, trendach i atakach ukierunkowanych, dzięki czemu firmy mogą przewidywać ataki nowych zagrożeń i im przeciwdziałać.
- ✓ Produkty ESET, wykorzystują metody heurystyczne i uczenie maszynowe, w ramach wielowarstwowej ochrony przed niespotykanym dotąd złośliwym oprogramowaniem.
- ✓ Oparty o chmurę system ochrony przed złośliwym oprogramowaniem automatycznie zabezpiecza przed nowymi zagrożeniami bez konieczności aktualizacji silnika detekcji.

## Ransomware

**Przypadek zastosowania:** Niektóre firmy wymagają zwiększonej ochrony przed atakami ransomware, chcąc mieć pewność, że ich dyski sieciowe są zabezpieczone przed zaszyfrowaniem.

### ROZWIĄZANIE

- ✓ Ochrona przed atakami sieciowymi, wbudowana w rozwiązania ESET, uniemożliwia wirusom typu ransomware zainfekowanie systemu. Tego typu ataki są neutralizowane na poziomie sieciowym.
- ✓ Wielowarstwowa ochrona ESET składa się m.in. z sandboxingu, dzięki czemu możliwe jest wykrywanie złośliwego oprogramowania, które maskuje swoją obecność, próbując uniknąć wykrycia.
- ✓ Chmurowy system wczesnego ostrzegania automatycznie chroni przed najnowszymi zagrożeniami bez konieczności czekania na aktualizację silnika detekcji.
- ✓ Wszystkie produkty ESET posiadają wbudowaną technologię Ransomware Shield, chroniącą przed infekcjami wirusów szyfrujących.
- ✓ W przypadku braku pewności czy dany element stanowi zagrożenie, próbka może zostać wysłana do usługi sandboxingu w chmurze (ESET Dynamic Threat Defense), gdzie poddawana jest specjalistycznej analizie pod kątem złośliwego charakteru.

# O ESET

**ESET jest globalnym dostawcą oprogramowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało blisko 5 milionów Polaków i ponad 110 milionów osób na świecie. Producent został uznany jedynym Challengerem w raporcie Gartner Magic Quadrant dla platform Endpoint Protection 2018[1].**

Od 30 lat ESET w swoich centrach badawczo-rozwojowych, m.in. od ponad dekady w Krakowie, rozwija najlepsze w branży oprogramowanie i usługi bezpieczeństwa informatycznego, dostarczając firmom i użytkownikom indywidualnym kompleksowe rozwiązania do ochrony przed stale ewoluującymi zagrożeniami.

ESET jest firmą o wysokiej płynności finansowej, od początku pozostającą w rękach prywatnych przedsiębiorców. Dzięki temu ESET ma pełna swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom.

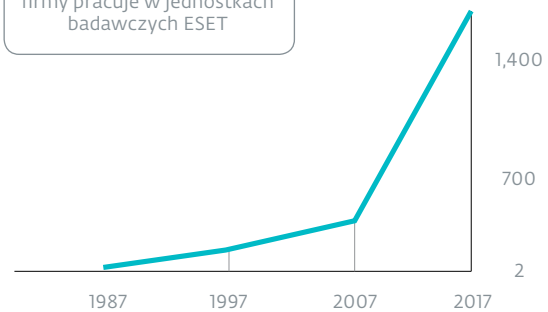
Produkty ESET dostępne są w ponad 200 krajach świata. W Polsce za dystrybucje rozwiązań ESET odpowiada firma DAGMA.

## ESET W LICZBACH

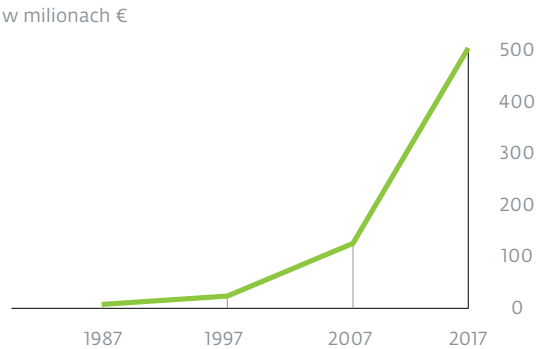
| 110 mln+ | 4 mln+ | 400 tys.+ | 13 |
|---|---|---|---|
| użytkowników na całym świecie | użytkowników w Polsce | klientów biznesowych | centrów badawczo-rozwojowych |

## PRACOWNICY ESET

Więcej niż 1/3 pracowników firmy pracuje w jednostkach badawczych ESET




## PRZYCHODY ESET




[1] Gartner nie promuje żadnego sprzedawcy, produktu ani usług przedstawionych w publikacjach badawczych. Publikacje badawcze Gartnera zawierają opinie organizacji badawczej Gartnera i nie powinny być interpretowane jako stwierdzenia faktów. Gartner zrzeka się wszelkich gwarancji wyrażonych lub domniemanych, w odniesieniu do tych badan, w tym wszelkich gwarancji przydatności handlowej lub jakości do określonego celu.

## WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

Od 2017 roku ESET chroni ponad
14 tysięcy stanowisk.

Canon
Canon Marketing Japan Group

Od 2016 roku ESET chroni ponad
9 tysięcy stanowisk.

Allianz Suisse

Chroniony przez ESET od 2016 roku.
Ponad 4 000 skrzynek pocztowych.

T-Mobile jest partnerem ISP od 2008 roku.
W swojej bazie posiada 2 mln klientów.

## WYBRANE NAGRODY

CRN

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

AV comparatives Approved Business Product 2017

PRODUKT ROKU 2018 WYBÓR CZYTELNIKÓW IT professional

*„Biorąc pod uwagę cechy produktu, zarówno w zakresie ochrony przed złośliwym oprogramowaniem, możliwościami zarządzania, jak również w zakresie globalnego zasięgu klientów i wsparcia technicznego, ESET powinien być brany pod uwagę w zapytaniach ofertowych i przetargach dotyczących wdrożenia rozwiązań antywirusowych."*

— KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018


ENJOY SAFER
TECHNOLOGY™