ENDPOINT SOLUTIONS

Wielowarstwowa ochrona, wykorzystująca metody uczenia maszynowego i wieloletnie doświadczenie ekspertów bezpieczeństwa IT - od jednego z globalnych liderów zabezpieczeń stacji roboczych z siedzibą w Unii Europejskiej.

Progress. Protected.

ESET jest globalnym dostawcą oprogramowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało **ponad 5 milionów Polaków i ponad 110 milionów użytkowników na świecie.**

Produkty ESET są rozwijane w kilkunastu centrach badawczo-rozwojowych na świecie. **Pierwsze takie centrum powstało i działa do dzisiaj w Krakowie.** To, co od lat wyróżnia ESET na tle konkurencji, to metoda wykrywania wirusów i ataków oparta na **sztucznej inteligencji, tj. zaawansowanej heurystyce, która z czasem przerodziła się w uczenie maszynowe.** Rozwiązania ESET wyróżnia także niemal niezauważalne dla wydajności komputerów działanie, co wielokrotnie doceniły w testach niezależne ośrodki badawcze, m.in. AV-Test czy AV-Comparatives.

Czym jest **Endpoint Protection Platform?**

Endpoint Protection Platform (EPP) to oprogramowanie zabezpieczające, instalowane na stacjach roboczych, którego celem jest wykrywanie zagrożeń i dostarczanie wszelkich informacji na temat ewentualnych prób ataków, dając możliwość błyskawicznej reakcji w przypadku wykrycia incydentu.

Rozwiązania typu Endpoint Protection zapewniają wielowarstwową ochronę stacji roboczych, działając w oparciu o wiele technologii. Jako jedyne na rynku umożliwiają skuteczną ochronę przy niemal niezmienionej wydajności chronionego urządzenia i prawidłowym identyfikowaniu zagrożeń.

Dlaczego warto wybrać rozwiązania **Endpoint Protection?**

RANSOMWARE

Ransomware od czasu pojawienia się Cryptolockera w 2013 roku, stanowi spory problem dla wielu firm na całym świecie. Mimo, że złośliwe oprogramowanie szyfrujące dane pojawiło się znacznie wcześniej, nigdy jednak nie było aż tak poważnym i realnym zagrożeniem dla firm jak obecnie. Dziś pojedynczy atak ransomware może doprowadzić do zaszyfrowania kluczowych dla firmy danych, paraliżując w ten sposób funkcjonowanie całego przedsiębiorstwa. Organizacje, które doświadczyły ataku ransomware, szybko zdają sobie sprawę, że posiadanie kopii zapasowej często nie wystarcza do zażegnania problemu. Zdarza się również, że zaatakowane firmy ostatecznie decydują się na zapłacenie okupu za odszyfrowanie danych.

Rozwiązania do ochrony stacji roboczych ESET zapewniają skuteczną obronę przed zagrożeniami ransomware, dzięki ich wielowarstwowej ochronie. Pozwala ona identyfikować zagrożenie na różnych etapach ataku.

ATAKI TARGETOWANE I KRADZIEŻ DANYCH

Współczesne rozwiązania bezpieczeństwa IT nieustannie ewoluują, w odpowiedzi na ciągle zmieniające się zagrożenia i nowe metody ataków. Kiedy w firmie dochodzi do ataku lub naruszenia danych, organizacje są zwykle zaskoczone, że ich mechanizmy obronne zawiodły oraz, że atak w ogóle miał miejsce. Po wykryciu tego typu incydentu, często po czasie, firmy wprowadzają zabezpieczenia, które mają ochronić je przed powtórzeniem się tego typu sytuacji. Takie podejście nie chroni jednak przedsiębiorstwa przed kolejnymi atakami - cyberprzestępcy mogą bowiem wykorzystać kolejnym razem inną podatność.

By zapobiec tego typu sytuacjom rozwiązania Endpoint od ESET wykorzystują mechanizmy sztucznej inteligencji oraz chmurę, by rozpoznawać i gromadzić informacje o wykrytych atakach i infekcjach, jakie na całym świecie zidentyfikowały aplikacje zabezpieczające ESET. Pozwala to na ograniczanie rozprzestrzeniania się zagrożeń i niwelowanie prawdopodobieństwa infekcji kolejnych sieci firmowych.

ATAKI BEZPLIKOWE

Istniejące typy zagrożeń bytują wyłącznie w pamięci komputera, co uniemożliwia ich wykrywanie za pomocą tradycyjnego skanowania antywirusowego plików. Niektóre z takich zagrożeń korzystają z zainstalowanych w systemie operacyjnym aplikacji, aby jeszcze trudniej było wykryć ich złośliwe elementy. Często tego typu wirusy wykorzystują również skrypty PowerShell do przeprowadzenia ataku.

Rozwiązania Endpoint firmy ESET posiadają zabezpieczenia przed atakami bezplikowymi - wykrywając zmodyfikowane lub zainfekowane aplikacje. Rozwiązania ESET posiadają specjalny moduł, który nieustannie sprawdza pamięć urządzeń pod kątem wszelkich podejrzanych elementów.

Rozwiązania Endpoint od ESET zapewniają skuteczną obronę, dzięki wykorzystaniu wielu połączonych warstw ochronnych. Pozwala to zarówno zapobiegać przedostaniu się złośliwego oprogramowania ransomware do sieci firmowej, jak również identyfikować je, jeśli znalazło się wcześniej w sieci firmowej.

Kiedy dochodzi do ataku lub naruszenia danych, organizacje są zwykle zaskoczone, że ich mechanizmy obronne zawiodły oraz, że atak w ogóle miał miejsce.

Istniejące zagrożenia bytują wyłącznie w pamięci komputera, co uniemożliwia ich wykrywanie za pomocą tradycyjnego skanowania antywirusowego plików.

„ESET od lat chroni naszą firmę przed zagrożeniami. Robi to, co musi. Nie musimy się niczym martwić. Krótko mówiąc ESET oznacza: niezawodność, jakość i usługę na najwyższym poziomie."

— Jos Savelkoul, team leader ICT-Department
Szpital w Zuyderland, Holandia (licencja dla 10 000 stanowisk)

Poznaj nasze rozwiązania

ESET Endpoint Security for Windows/macOS/Android
ESET Endpoint Antivirus for Windows/macOS/Linux
ESET File Security for Microsoft Windows Server/Linux/FreeBSD/Azure
ESET Mobile Device Management for Apple iOS

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 RÓŻNYCH SYSTEMÓW OPERACYJNYCH

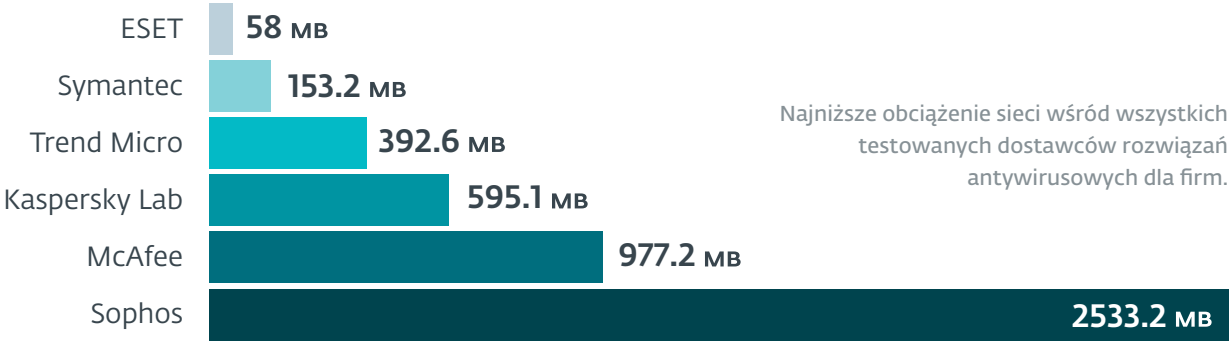
Produkty ESET przeznaczone do ochrony stacji roboczych obsługują popularne systemy operacyjne, w tym: Windows, Mac OS, Linux i Android. Wszystkie produkty firmy ESET mogą być w pełni zarządzane za pomocą konsoli do centralnej administracji.

NIEZRÓWNANA WYDAJNOŚĆ

Największym wyzwaniem dla firmy jest znalezienie rozwiązania typu Endpoint Protection, które chroniąc stację roboczą, utrzyma jej wydajność na niemal niezmienionym poziomie. Produkty ESET wielokrotnie doceniono w testach niezależnych organizacji badawczych, właśnie z uwagi na niezauważalne działanie na chronionych urządzeniach.

ESET MARKĄ GLOBALNĄ

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.



Najniższe obciążenie sieci wśród wszystkich testowanych dostawców rozwiązań antywirusowych dla firm.

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

„Dlaczego polecam produkty ESET? Bardzo mało obciążają komputery, są proste w instalacji, a administracja nie wymaga wiele czasu. W poprzednich firmach miałem styczność z wieloma rozwiązaniami antywirusowymi i faktycznie na ich tle ESET zawsze wypadał najlepiej."

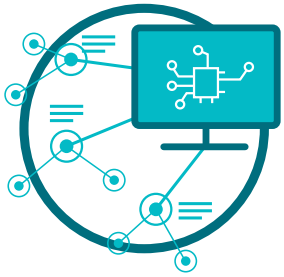
— Grzegorz Pawłowski, Administrator IT
Gremi Media, Polska (licencja dla 500 stanowisk)

Technologia

Działanie naszych rozwiązań opiera się na trzech filarach

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.



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.

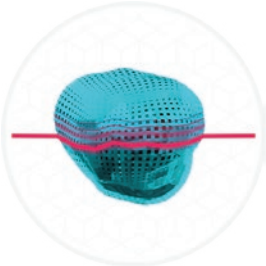
WIEDZA EKSPERTÓW

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 ochronna 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

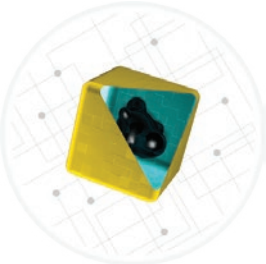
Zaawansowany skaner pamięci ESET monitoruje zachowanie procesów skanując je w bezpiecznym, odizolowanym środowisku. Skaner ten pozwala wykrywać nowe zagrożenia bezplikowe w przypadku, kiedy konwencjonalne skanery antywirusowe pozostają bezradne.

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.

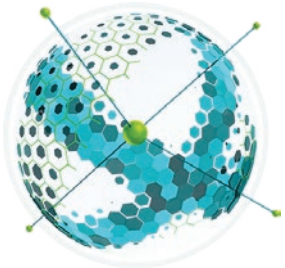


SANDBOXING

Dzisiejsze zagrożenia często kamuflują swoje działania, starając się w ten sposób uniknąć wykrycia. Aby sprawdzić ich rzeczywiste zachowanie, rozwiązania ESET wykorzystują tzw. sandboxing, który symuluje działanie potencjalnego zagrożenia w wirtualnym, izolowanym 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

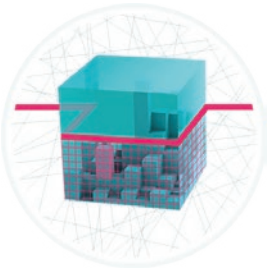
Kolejna warstwa ochrony programów ESET identyfikuje luki w protokołach sieciowych i blokuje ich wykorzystanie, dzięki czemu uniemożliwia rozprzestrzenianie się zagrożeń (m.in. ransomware) wewnątrz sieci firmowej i poza nią.

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 działającym na hoście (HIPS) monitoruje aktywność wszystkich procesów systemu Windows i wykorzystuje predefiniowane reguły do rozpoznawania podejrzanego działania systemu. W razie wykrycia takiej aktywności HIPS automatycznie unieszkodliwia działanie złośliwego procesu.

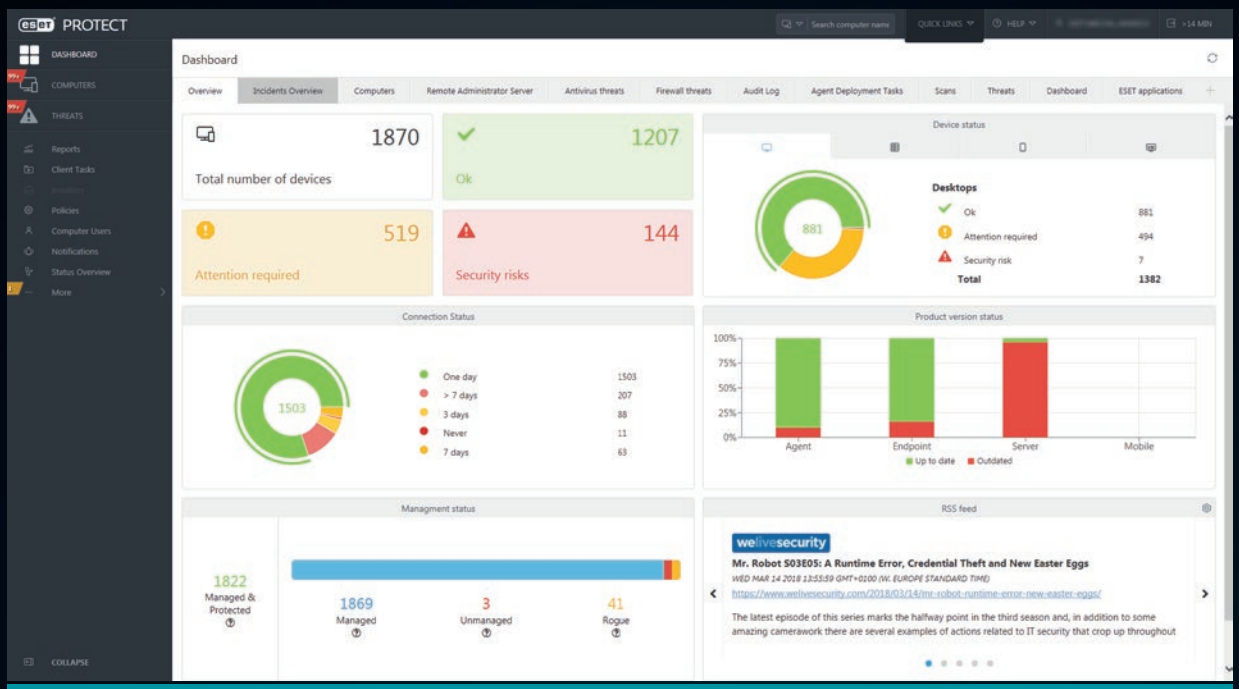


SKANER UEFI

ESET jest pierwszym dostawcą zabezpieczeń dla stacji roboczych, którego rozwiązania posiadają dedykowany skaner UEFI (Unified Extensible Firmware Interface), który chroni przed zagrożeniami, aktywującymi się jeszcze przed uruchomieniem systemu operacyjnego. W razie wykrycia nieprawidłowości program blokuje zagrożenie i powiadamia o tym użytkownika.

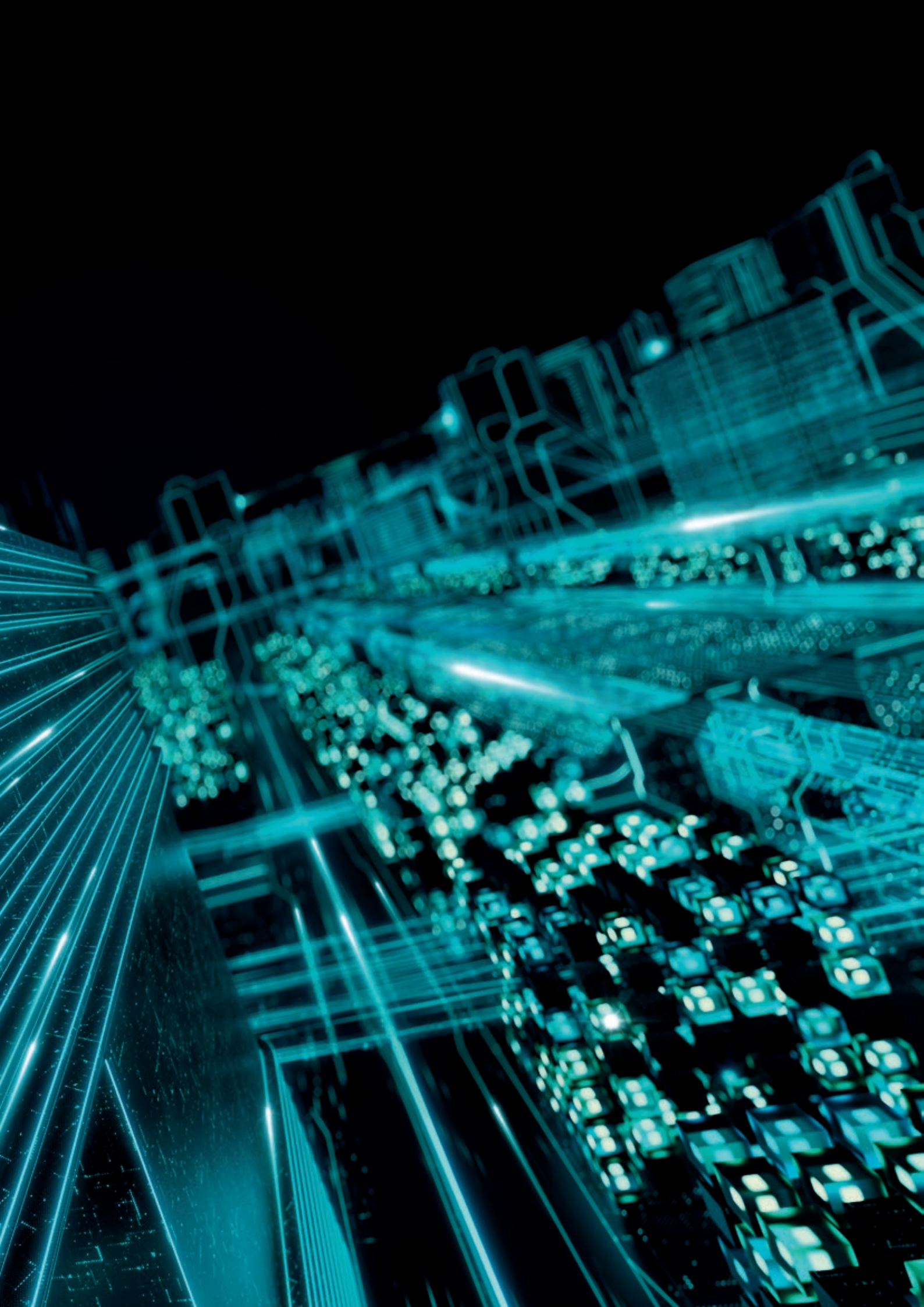
„Największą zaletą rozwiązania jest jego duża przewaga techniczna nad innymi produktami na rynku. ESET zapewnia nam niezawodne zabezpieczenia, co oznacza, że mogę pracować nad dowolnym projektem w dowolnym momencie, wiedząc, że nasze komputery są chronione w 100 proc."

— Fiona Garland, Business Analyst Group IT
Mercury Engineering, Irlandia (licencja dla 1 300 stanowisk)



ESET PROTECT

Produkty ESET do ochrony stacji roboczych, urządzeń mobilnych i serwerów są zarządzane za pośrednictwem konsoli ESET PROTECT (dostępnej w wersji chmurowej i lokalnej) instalowanej w systemie Windows lub Linux. Konsola dostępna jest również jako obraz maszyny wirtualnej, który możesz zaimportować, by przyśpieszyć i ułatwić proces konfiguracji rozwiązania.



Zastosowanie

Ransomware

Niektóre firmy wymagają dodatkowego zabezpieczenia, które ochroni organizację przed atakami ransomware.

ROZWIĄZANIE

- ✓ Ochrona przed atakami sieciowymi pozwala zapobiegać rozprzestrzenianiu się szkodliwego oprogramowania i rozwojowi infekcji systemu, zatrzymując exploity zanim zostaną wykorzystane na danej stacji roboczej.
- ✓ Funkcja sandboxingu ułatwia wykrycie zagrożeń próbujących zaciemnić swój kod, poprzez weryfikację w odizolowanym od systemu środowisku.
- ✓ Chmurowy system wczesnego ostrzegania Live Grid zapewnia ochronę przed nowymi infekcjami, zanim jeszcze powstaną stosowne aktualizacje dla silnika detekcji.
- ✓ Kompletną ochronę uzupełnia Ransomware Shield, eliminujący ryzyko infekcji firmowych komputerów zagrożeniami szyfrującymi.

Zagrożenia typu zero-day

Zagrożenia zero-day są szczególnie niebezpieczne dla firm, ponieważ nie są one przygotowane na walkę z nimi.

ROZWIĄZANIE

- ✓ Produkty biznesowe ESET wykorzystują mechanizmy heurystyczne i uczenie maszynowe, zapobiegając przed infekcjami i atakami nieznanych wcześniej zagrożeń.
- ✓ 13 globalnych laboratoriów badawczo-rozwojowych, w tym jedno w Krakowie pomaga szybko reagować na zagrożenia identyfikowane w dowolnym miejscu na ziemi.
- ✓ Chmurowy system wczesnego ostrzegania ESET Live Grid rozbudowuje ochronę przed nowymi wirusami, która nie wymaga oczekiwania na kolejną aktualizację baz sygnatur detekcji.

Zagrożenia bezplikowe

Wirusy bezplikowe są stosunkowo nowym zagrożeniem i ze względu na to, że działają tylko w pamięci komputera, wymagają innego podejścia, niż w przypadku ich tradycyjnych odpowiedników.

ROZWIĄZANIE

- ✓ Unikalna technologia zaawansowanego skanera pamięci ESET chroni przed zagrożeniami bezplikowymi, monitorując zachowanie podejrzanych procesów i skanując je po wcześniejszym wyizolowaniu z pamięci.
- ✓ W razie wątpliwości próbki podejrzanego obiektu przesyłane są bezpośrednio do systemu ESET Threat Intelligence i administrator informowany jest o wynikach w raporcie.
- ✓ Wielowarstwowa ochrona, uczenie maszynowe oraz wiedza ekspertów z firmy ESET zapewniają naszym klientom najwyższy poziom ochrony.

„Największą zaletą ESET dla mnie jako szefa IT jest to, że po wdrożeniu tego oprogramowania moi ludzie mają więcej czasu na inne obowiązki."

— Tomasz Witkowski,
CIO, Gremi Media, Polska
(licencja dla 500 stanowisk)

O ESET

ESET jest globalnym dostawcą oprogra-mowania zabezpieczającego komputery firm oraz użytkowników indywidualnych, któremu zaufało ponad 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.

Od wielu lat ESET jest pionierem w dziedzinie uczenia maszynowego i technologii chmurowych, które skutecznie zapobiegają infekcjom złośliwym oprogramowaniem, wykrywają je i pozwalają je skutecznie zwalczać.

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

ESET W LICZBACH

110 mln+
użytkowników na całym świecie

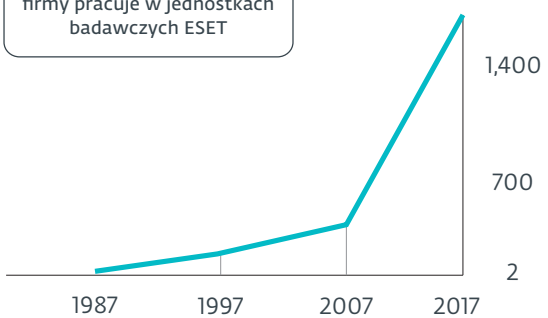
5 mln+
użytkowników w Polsce

400 tys.+
klientów biznesowych

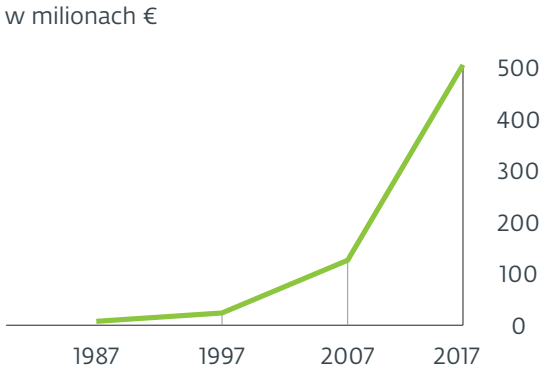
13
globalnych ośodków rozwojowo-badawczych – w tym laboratorium w Krakowie

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 badań, 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 WYRÓŻNIENIA

CRN

Gartner peerinsights customers' choice 2019

AV comparatives APPROVED Business Security JUL 2019

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


Digital Security
Progress. Protected.