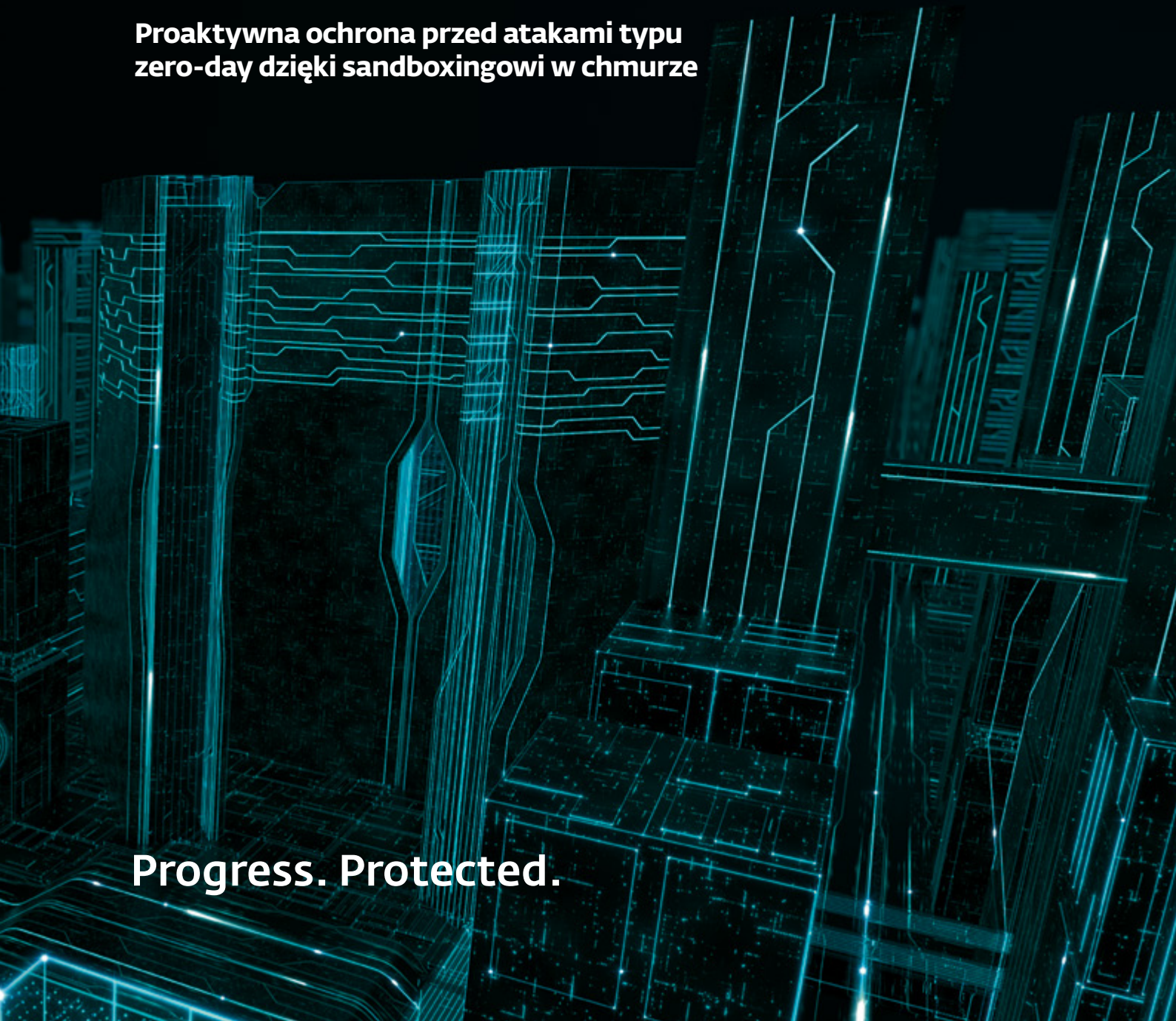
OMÓWIENIE ROZWIĄZANIA

LIVEGUARD ADVANCED

Proaktywna ochrona przed atakami typu zero-day dzięki sandboxingowi w chmurze



Progress. Protected.

Czym jest **zaawansowana ochrona przed zagrożeniami?**

Proaktywna technologia ESET LiveGuard Advanced zapewnia kolejną warstwę ochrony dla produktów ESET, takich jak ESET Mail Security, czy rozwiązania Endpoint. Do wykrywania nowych, niezidentyfikowanych wcześniej zagrożeń rozwiązanie wykorzystuje technologię sandboxingu w chmurze. Sam sandbox w swoim działaniu korzysta z kilku typów sensorów, które uzupełniają statyczną analizę kodu. Przeprowadzają one dogłębną analizę próbki z wykorzystaniem uczenia maszynowego, introspekcję wewnątrz pamięci i detekcję zagrożeń opartą na analizie behawioralnej.

Rozwiązanie ESET LiveGuard Advanced stanowi kolejną warstwę zabezpieczeń wspierającą działanie innych produktów ESET, takich jak Mail Security, Endpoint i Cloud Office Security. Zaawansowana technologia wykorzystująca możliwości chmury obliczeniowej opiera się na szeregu zróżnicowanych czujników, które pozwalają na przeprowadzenie statycznej analizy kodu, dokładnej inspekcji próbki z wykorzystaniem uczenia maszynowego, introspekcji w pamięci oraz analizy behawioralnej.

Dlaczego warto korzystać z **proaktywnej ochrony opartej na chmurze?**

RANSOMWARE

Od czasu pojawienia się Cryptolockera w 2013 roku złośliwe oprogramowanie typu ransomware pozostaje ciągłym zagrożeniem dla firm i organizacji na całym świecie. Pomimo tego, że oprogramowanie tego rodzaju istniało znacznie wcześniej, do tamtego momentu firmy nie traktowały go w kategorii poważnego zagrożenia. Obecnie infekcja nawet pojedynczej maszyny może szybko zablokować firmie możliwość prowadzenia dalszej działalności w wyniku zaszyfrowania kluczowych plików i danych. Wiele firm padających ofiarą ataku ransomware zdaje sobie sprawę, że ich kopie zapasowe są nieaktualne – pojawia się wówczas chęć zapłaty okupu na rzecz cyberprzestępców.

Rozwiązanie oparte na chmurze, umożliwiające proaktywne wykrywanie zagrożeń stanowi dodatkową warstwę ochrony znajdującą się poza siecią przedsiębiorstwa, która uniemożliwia uruchomienie próbki oprogramowania ransomware w środowisku produkcyjnym.

ATAKI UKIERUNKOWANE I WYCIEKI DANYCH

Nowe metody ataków i niespotykane wcześniej zagrożenia zmieniają krajobraz cyberbezpieczeństwa na świecie. Kiedy dochodzi do ataku lub wycieku danych, organizacje są zazwyczaj zaskoczone, że ich zabezpieczenia zostały pokonane, a w gorszych przypadkach nie mają w ogóle świadomości, że doszło do ataku. Po wykryciu naruszenia organizacje reagują wdrażając środki zaradcze, by uniemożliwić jego powtórzenie – w żaden sposób nie chroni ich to jednak przed kolejnym atakiem, który może zostać zrealizowany przy pomocy zupełnie innego wektora.

Sandboxing – uruchamianie potencjalnych próbek złośliwego oprogramowania w odizolowanym środowisku – oparty na chmurze jest znacznie skuteczniejszy niż obserwowanie charakterystyki potencjalnego zagrożenia, gdyż pozwala na sprawdzenie zachowania danej próbki. Pozwala to na bardziej jednoznaczne określenie, czy mamy do czynienia z atakiem ukierunkowanym, zaawansowanym zagrożeniem długotrwałym (APT) czy nieszkodliwym plikiem.

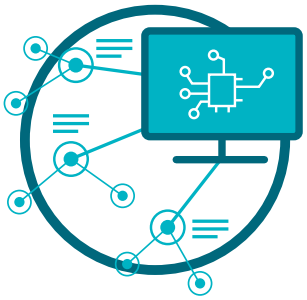
Analiza statyczna i dynamiczna opiera się na szeregu algorytmów uczenia maszynowego wykorzystujących wiele technik takich jak uczenie głębokie.

Sandboxing w chmurze poza siecią przedsiębiorstwa pozwala skutecznie analizować nie tylko charakterystykę próbki, ale także obserwować zachowanie potencjalnego zagrożenia.

Nasze produkty i technologie opierają się na trzech filarach

ESET LIVEGRID®

W przypadku wykrycia nowego zagrożenia typu zero-day, na przykład oprogramowania ransomware, plik jest wysyłany do naszego opartego na chmurze systemu ochrony przed złośliwym oprogramowaniem – LiveGrid®, w którym następuje uruchomienie próbki i monitorowanie jej zachowania. Wyniki tego testu są przekazywane do wszystkich stacji roboczych na całym świecie w ciągu kilku minut – wszystko bez konieczności pobierania aktualizacji.

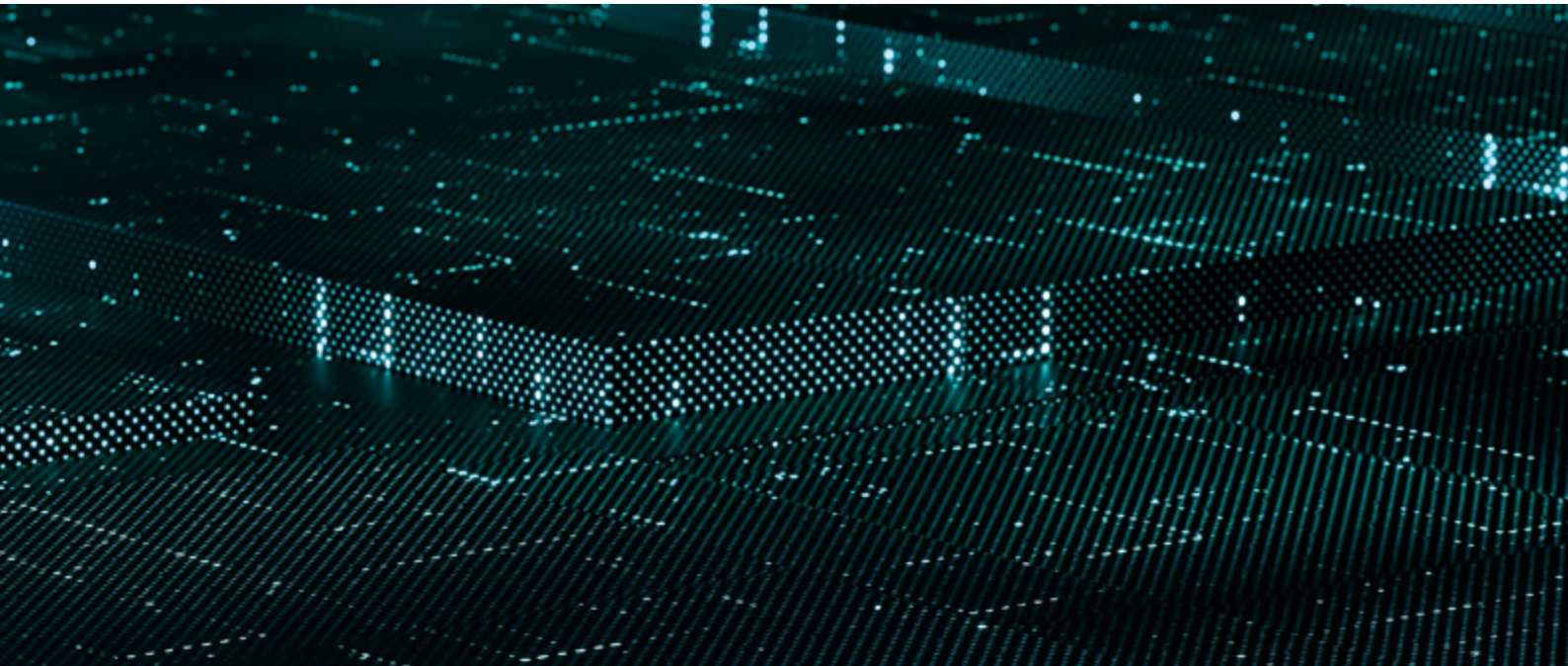


UCZENIE MASZYNOWE

Dzięki połączonej mocy sieci neuronowych i specjalnie dobranych algorytmów rozwiązanie automatycznie oznacza nowe próbki jako czyste, potencjalnie niechciane lub złośliwe.

SPECJALISTYCZNA WIEDZA

Światowej klasy specjaliści zajmujący się bezpieczeństwem dzielą się swoją wiedzą i informacjami, by zapewnić stały przepływ informacji o zagrożeniach 24 godziny na dobę, 7 dni w tygodniu.



Poczuj różnicę z ESET

WIELOWARSTWOWA OCHRONA

ESET LiveGuard Advanced to oparte na chmurze rozwiązanie do obrony przed zagrożeniami, które umożliwia przesyłanie wszystkich podejrzanych próbek do bezpiecznego środowiska testowego w siedzibie firmy ESET, gdzie ich zachowanie jest badane na podstawie informacji na temat zagrożeń, wielu wewnętrznych narzędzi firmy ESET do analizy statycznej i dynamicznej oraz danych dotyczących reputacji próbek, co pozwala na skuteczne wykrywanie zagrożeń typu zero-day. Każda z próbek jest analizowana przy pomocy czterech warstw zabezpieczeń, które mogą być stosowane dynamicznie w zależności od wyników. ESET LiveGuard Advanced łączy wyniki wszystkich analiz i ocenia status każdej próbki. Wyniki przeprowadzonych badań trafiają w pierwszej kolejności do produktów ESET zabezpieczających urządzenia użytkownika oraz infrastrukturę przedsiębiorstwa.

PEŁNA WIDOCZNOŚĆ

Każda analizowana próbka jest opatrzona kompletem wyników, które można wyświetlić w konsoli ESET PROTECT. Ponadto klienci posiadający licencję na więcej niż 100 stanowisk otrzymują pełne sprawozdanie z analizy behawioralnej, zawierające szczegółowe informacje o próbkach i ich zachowaniu zaobserwowanym podczas analizy w piaskownicy – wszystkie informacje są podawane w łatwej do zrozumienia formie. Oprogramowanie nie tylko wyświetla informacje na temat próbek wysyłanych do programu ESET LiveGuard Advanced, ale także wszystkie informacje przesłane do systemu ochrony przed złośliwym oprogramowaniem w chmurze firmy ESET – ESET LiveGrid®.

MOBILNOŚĆ

W dzisiejszych czasach pracownicy organizacji coraz częściej pracują zdalnie, a nie w siedzibie firmy. Dlatego nasze rozwiązanie ESET LiveGuard Advanced może analizować pliki bez względu na to, gdzie znajdują się użytkownicy. W przypadku wykrycia złośliwego oprogramowania cała firma jest natychmiast chroniona przed jego działaniem.

PRYWATNOŚĆ

Firma ESET bardzo poważnie traktuje kwestie prywatności i zgodności z obowiązującymi przepisami. Za pomocą szeregu ustawień użytkownik może nakazać firmie ESET usuwanie próbek natychmiast po przeprowadzeniu analizy.

NIEZRÓWNANA SZYBKOŚĆ

W walce z zagrożeniami liczy się każda minuta, dlatego rozwiązanie ESET LiveGuard Advanced jest w stanie przeanalizować większość przesyłanych próbek w czasie krótszym niż 5 minut. Jeśli próbka została wcześniej przeanalizowana, wystarczy kilka sekund, aby wszystkie urządzenia w organizacji zostały objęte ochroną.

SPRAWDZONE I GODNE ZAUFANIA ROZWIĄZANIE

Firma ESET działa w branży zabezpieczeń od ponad 30 lat i stale rozwija swoje technologie, by pozostawać o krok przed cyberprzestępcami i opracowywanymi przez nich zagrożeniami. W rezultacie nasze rozwiązania chronią obecnie przeszło miliard użytkowników Internetu na całym świecie. Nasza technologia jest nieustannie sprawdzana i testowana przez niezależnych testerów, którzy weryfikują skuteczność naszego podejścia w zakreise powstrzymywania najnowszych zagrożeń.

PROAKTYWNA OCHRONA

Jeśli próbka zostanie uznana za podejrzaną, jej wykonanie zostanie zablokowane w oczekiwaniu na analizę przez rozwiązanie ESET LiveGuard Advanced. Takie podejście zapobiega infekcji przez złośliwe oprogramowanie, które może dokonać spustoszenia w systemie użytkownika. Ponadto, po zakończeniu analizy i wykryciu zagrożenia na pojedynczym urządzeniu użytkownika, informacja trafia w ciągu kilku minut do wszystkich urządzeń w sieci organizacji, zapewniając natychmiastową ochronę każdemu użytkownikowi i każdemu systemowi, który mógł paść ofiarą zagrożenia.

Zastosowania

Ransomware

ZASTOSOWANIE

Złośliwe oprogramowanie typu ransomware zwykle trafia do skrzynek pocztowych nieświadomych użytkowników za pośrednictwem wiadomości poczty elektronicznej.

ROZWIĄZANIE

- ✓ Rozwiązanie ESET Mail Security automatycznie przesyła podejrzane załączniki wiadomości e-mail do programu ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced analizuje próbkę, a następnie przesyła wynik z powrotem do programu Mail Security – zwykle zajmuje to zaledwie 5 minut.
- ✓ ESET Mail Security wykrywa i automatycznie usuwa załączniki, które zawierają złośliwą zawartość.
- ✓ Dzięki temu złośliwy załącznik nigdy nie dociera do odbiorcy.

Ochrona pracowników na wszystkich stanowiskach

ZASTOSOWANIE

Pracownicy na różnych stanowiskach wymagają różnych poziomów ochrony. Programiści lub pracownicy działów IT wymagają innych zabezpieczeń niż pracownicy obsługi biura czy dyrektor generalny całego przedsiębiorstwa.

ROZWIĄZANIE

- ✓ Rozwiązanie ESET LiveGuard Advanced pozwala na ustalenie wyjątkowych zasad dla każdego komputera lub serwera.
- ✓ Takie rozwiązanie umożliwia automatyczne stosowanie zasad w oparciu o grupę użytkowników lub grupę Active Directory.
- ✓ Takie podejście pozwala także na automatyczne dostosowanie ustawień poprzez proste przeniesienie użytkownika pomiędzy grupami.

Nieznane lub podejrzane pliki

ZASTOSOWANIE

Czasami pracownicy lub dział IT mogą otrzymać podejrzany plik, by zweryfikować jego bezpieczeństwo.

ROZWIĄZANIE

- ✓ Każdy użytkownik może przesłać próbkę do analizy – jest to to możliwe z poziomu każdego produktu firmy ESET.
- ✓ Każda przesłana próbka jest następnie błyskawicznie analizowana przez rozwiązanie ESET LiveGuard Advanced.
- ✓ Jeśli plik zostanie uznany za złośliwy, wszystkie komputery w organizacji zostaną automatycznie objęte ochroną.
- ✓ Administrator IT otrzymuje dostęp do informacji na temat użytkownika, który przesłał próbkę oraz dowiaduje się, czy dany plik był bezpieczny, czy jednak stanowił zagrożenie.

Funkcjonalności ESET LiveGuard Advanced

AUTOMATYCZNA OCHRONA

Po skonfigurowaniu rozwiązania, administrator lub użytkownik nie muszą podejmować żadnych działań. Rozwiązanie automatycznie podejmuje decyzję o tym, czy dana próbka jest bezpieczna, niebezpieczna bądź nieznana. Te ostatnie są przesyłane w celu analizy do rozwiązania ESET LiveGuard Advanced. Po zakończeniu analizy wynik jest przekazywany do wszystkich produktów, które na jego podstawie podejmują stosowne działania.

OCHRONA DOSTOSOWANA DO POTRZEB

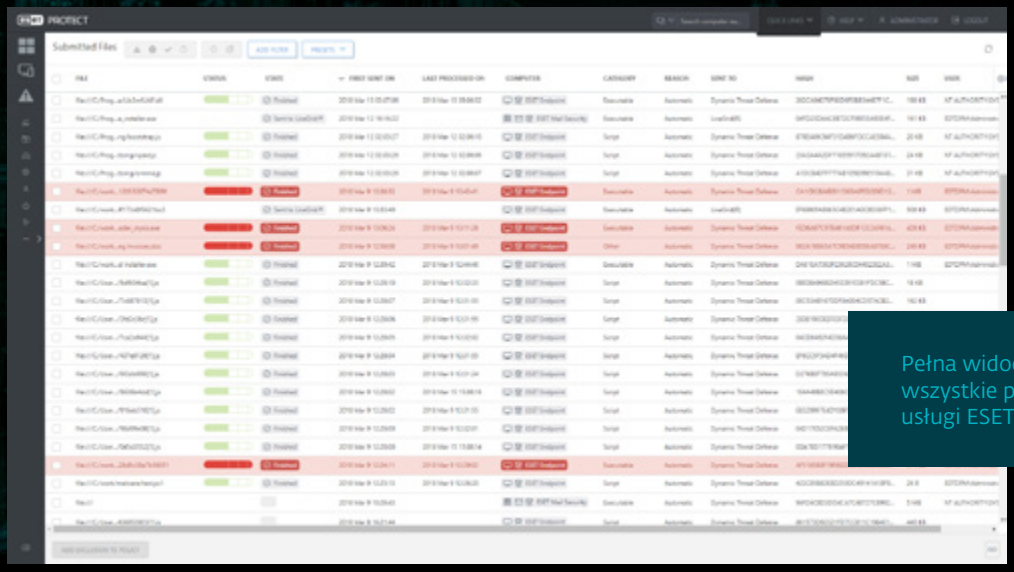
Rozwiązania ESET umożliwiają szczegółową konfigurację zasad ESET LiveGuard Advanced dla każdego komputera, dzięki czemu administrator może kontrolować rodzaj przesyłanych próbek oraz reakcję na wynik analizy. Ponadto ustawienia mogą być stosowane nie tylko dla poszczególnych komputerów, ale także dla grup urządzeń.

RĘCZNE PRZESYŁANIE PRÓBEK

W każdej chwili użytkownik lub administrator może przesłać próbki do analizy za pomocą kompatybilnego produktu ESET i uzyskać kompleksowe sprawozdanie. Administratorzy mają dostęp do danych i wyników analiz bezpośrednio w konsoli ESET PROTECT.

OCHRONA POCZTY

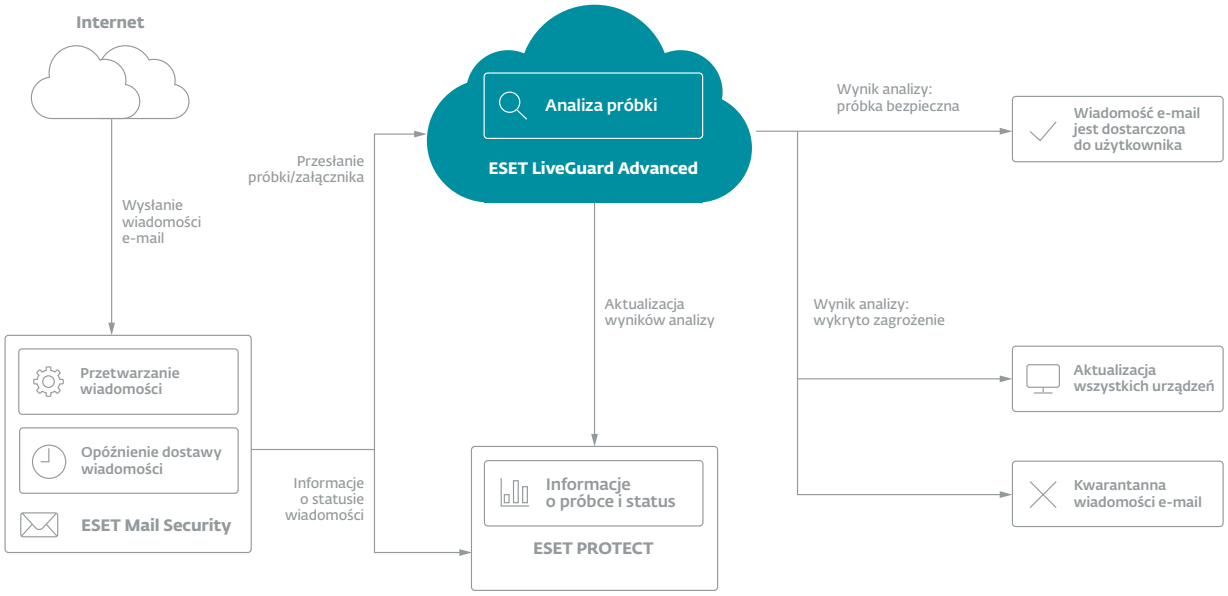
Rozwiązanie ESET LiveGuard Advanced pozwala na analizę plików, a także może zostać połączone z programem ESET Mail Security, aby zagwarantować, że złośliwe wiadomości e-mail nie trafią nigdy do skrzynek twojej organizacji. Aby zapewnić ciągłość działania, do programu ESET LiveGuard Advanced



Pełna widoczność - zobacz wszystkie pliki wysłane do usługi ESET LiveGrid®

Jak działa rozwiązanie ESET LiveGuard Advanced?

Rozwiązanie ESET Mail Security



Rozwiązanie ESET LiveGuard Advanced jest kompatybilne z produktami ESET Endpoint, Server i Cloud App Security (Microsoft 365) i jest w pełni zintegrowane z konsolami centralnego zarządzania ESET.

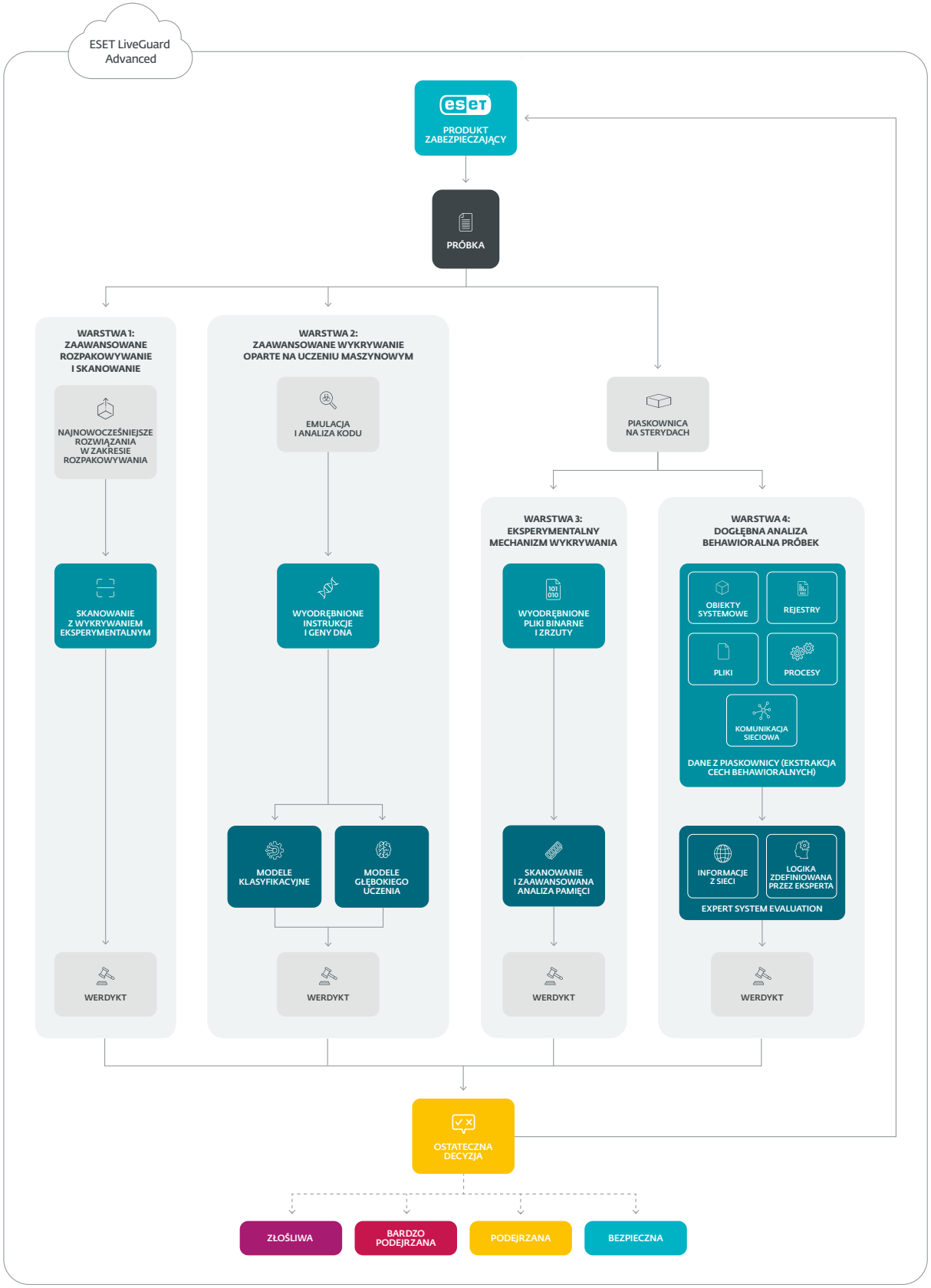
"Niesamowity produkt!"

Jakie aspekty podobają się Panu najbardziej?

"Podoba mi się łatwość wdrożenia rozwiązania na wszystkich stacjach roboczych i szybkość działania – zabezpieczenia zadziałały z wyjątkową szybkością. Znalazłem niechciane oprogramowanie i codziennie otrzymuję wiadomości e-mail z informacjami o zatrzymanych zagrożeniach sieciowych zanim wyrządziły szkody. Mogę spać spokojnie wiedząc, że moja sieć jest chroniona przez rozwiązania ESET."

— Michael P. / administrator sieci / średnie przedsiębiorstwo (51-1000 pracowników)

Jak działa nasza zaawansowana analiza?



Rozwiązanie ESET LiveGuard Advanced wykorzystuje 4 oddzielne warstwy wykrywania, aby zapewnić najwyższy współczynnik wykrywalności. Każda warstwa opiera się na innym podejściu i skutkuje oddzielną opinią na temat próbki. Ocena końcowa obejmuje wyniki wszystkich informacji o próbce.

WARSTWA 1

Zaawansowane rozpakowywanie i skanowanie

Próbki są poddawane analizie statycznej i nowoczesnym procesom rozpakowywania, a następnie są dopasowywane do rozległej bazy danych na temat zagrożeń.

WARSTWA 2

Zaawansowane wykrywanie oparte na uczeniu maszynowym

Analiza statyczna i dynamiczna oparta na szeregu algorytmów uczenia maszynowego wykorzystujących wiele technik takich jak uczenie głębokie.

WARSTWA 3

Eksperymentalny mechanizm wykrywania

Próbki są umieszczane w „piaskownicach na sterydach", przypominających urządzenia użytkownika. Są one następnie monitorowane pod kątem wszelkich oznak złośliwego zachowania.

WARSTWA 4

Dogłębna analiza behawioralna próbek

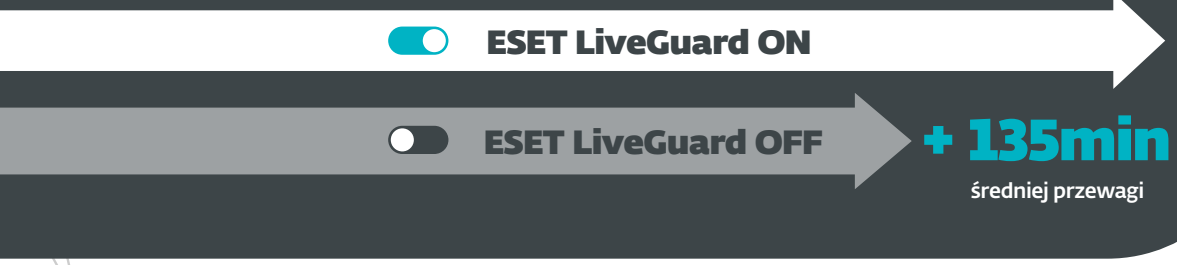
Wszystkie dane wyjściowe z piaskownicy są poddawane dogłębnej analizie behawioralnej, która identyfikuje znane złośliwe wzorce i łańcuchy działań.

ROZWIĄZANIE ŁĄCZY WSZYSTKIE DOSTĘPNE WYNIKI ANALIZ I OCENIA STATUS KAŻDEJ PRÓBKI. WYNIKI TRAFIAJĄ W PIERWSZEJ KOLEJNOŚCI DO PRODUKTÓW ESET ZABEPIECZAJĄCYCH URZĄDZENIA ORAZ INFRASTRUKTURĘ FIRMY UŻYTKOWNIKA.

NIEZRÓWNANA SZYBKOŚĆ

Sandboxing w chmurze umożliwia analizę większości nowych próbek w czasie krótszym niż 5 minut

ZALETA WYKRYWANIA



O firmie ESET

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 pełną swobodę działania i może zapewnić najlepszą ochronę wszystkim swoim klientom. Produkty ESET dostępne są w ponad 200 krajach świata. W Polsce za dystrybucję rozwiązań ESET odpowiada firma DAGMA Bezpieczeństwo IT.

ESET W LICZBACH

1mld+
chronionych użytkowników Internetu

400k+
klientów biznesowych

200+
krajów i terytoriów

13
globalnych ośrodków badań i rozwoju

NASI WYBRANI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

korzysta z ochrony ESET od 2017 roku, ponad 9 000 urządzeń

Allianz Suisse

korzysta z ochrony ESET od 2016 roku, ponad 4 000 skrzynek pocztowych

Canon
Canon Marketing Japan Group

korzysta z ochrony ESET od 2016 roku, ponad 32 000 urządzeń

T

partner ISP w zakresie bezpieczeństwa od 2008 roku, 2 miliony klientów

WYBRANE NAGRODY I WYRÓŻNIENIA

AV comparatives APPROVED Business Security DEC 2021

Firma ESET otrzymała nagrodę Business Security APPROVED od AV - Comparatives w teście bezpieczeństwa biznesowego w grudniu 2021 r.

G2 Leader WINTER 2022

Firma ESET konsekwentnie zajmuje czołowe miejsca na globalnej platformie recenzji użytkowników G2, a jej rozwiązania są doceniane przez klientów na całym świecie.

FORRESTER®

Rozwiązania ESET są regularnie doceniane przez wiodące firmy analityczne, w tym w „The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" jako przykładowy sprzedawca.

eset® Digital Security
Progress. Protected.