PRZEGLĄD

INSPECT

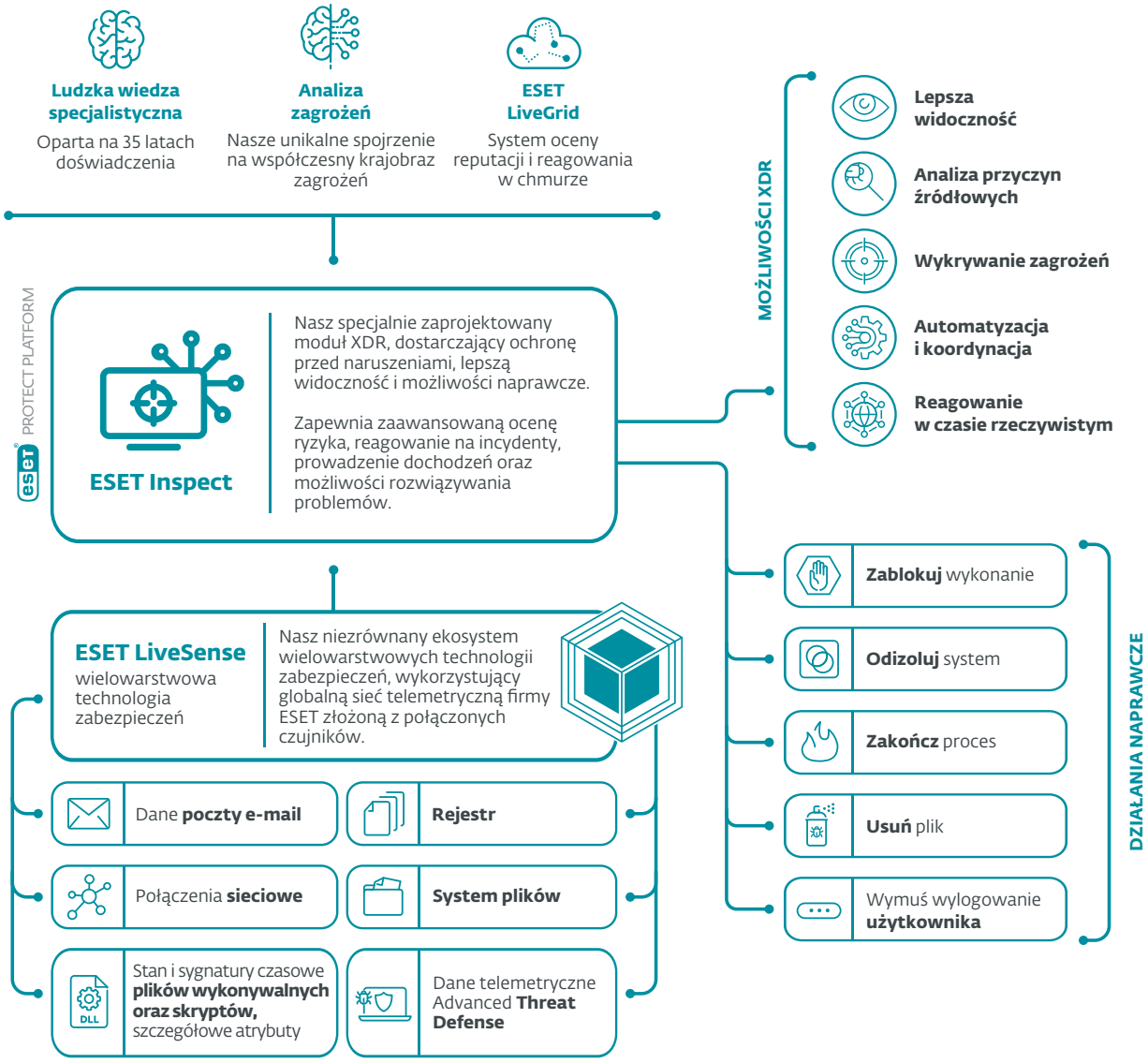
Moduł platformy ESET PROTECT obsługujący standard XDR, zapewniający ochronę przed naruszeniami bezpieczeństwa, lepszy wgląd w sytuację oraz działania naprawcze

Progress. Protected.

Czym jest rozwiązanie typu **Extended Detection & Response (XDR)?**

ESET Inspect, moduł platformy ESET PROTECT umożliwiający wdrażanie rozwiązań XDR, to narzędzie służące do wykrywania nietypowych zachowań i naruszeń bezpieczeństwa, oceny ryzyka, reagowania na incydenty, prowadzenia dochodzeń oraz usuwania skutków incydentów.

Rozwiązanie to umożliwia osobom odpowiedzialnym za reagowanie na incydenty monitorowanie i ocenę wszystkich działań w sieci oraz na podłączonych urządzeniach. Pomaga również w automatyzacji natychmiastowych działań naprawczych, jeśli zajdzie taka potrzeba. Ponad 800 (a liczba ta wciąż rośnie) reguł wykrywania firmy ESET umożliwia kompleksowe wykrywanie zagrożeń.



Cybersecurity
Progress. Protected.

Czym wyróżnia się ESET

KOMPLEKSOWA OCHRONA, WYKRYWANIE I REAKCJA

Umożliwia szybką analizę i usunięcie wszelkich problemów związanych z bezpieczeństwem w sieci. Wielowarstwowy system zabezpieczeń firmy ESET, w którym każda warstwa przesyła dane do ESET Inspect, analizuje ogromne ilości danych w czasie rzeczywistym, dzięki czemu żadne zagrożenie nie pozostaje niewykryte.

ROZWIĄZANIE OD LIDERA CYBERBEZPIECZEŃSTWA

ESET od ponad 30 lat walczy z cyberzagrożeniami. Jako firma oparta na badaniach naukowych od dawna przoduje w takich dziedzinach jak uczenie maszynowe, technologie chmurowe, a obecnie także XDR.

LEPIEJ ZAPOBIEGAĆ NIŻ LECZYĆ

Podejście firmy ESET do XDR jest ściśle powiązane z jej wielokrotnie nagradzanymi produktami zapobiegawczymi. Dzięki zaangażowaniu w rozwój wysokiej jakości technologii wykrywania rozwiązania prewencyjne ESET są wiodące na świecie.

SYSTEM REPUTACYJNY

Rozbudowane filtrowanie pozwala inżynierom ds. bezpieczeństwa identyfikować wszystkie aplikacje o potwierdzonym poziomie bezpieczeństwa dzięki solidnemu systemowi reputacyjnemu firmy ESET. System ESET zawiera bazę danych obejmującą setki milionów nieszkodliwych plików, co gwarantuje, że zespoły ds. bezpieczeństwa poświęcają swój czas na analizę nieznanych i potencjalnie złośliwych plików, a nie na fałszywe alarmy.

AUTOMATYZACJA I DOSTOSOWYWANIE

Z łatwością dostosuj ESET Inspect do wymaganego poziomu szczegółowości i automatyzacji. Wybierz pożądany poziom interakcji – oraz rodzaj i ilość danych, które mają być przechowywane – podczas wstępnej konfiguracji oraz przy pomocy gotowych profili użytkowników, a następnie pozwól, aby tryb uczenia się (Learning Mode) zmapował środowisko Twojej organizacji i w razie potrzeby zasugerował wykluczenia zapobiegające fałszywym alarmom.

AUTOMATYCZNE TWORZENIE ZGŁOSZEŃ

Uzyskaj doskonałą widoczność dzięki automatycznie tworzonym i przejrzyście wizualizowanym zgłoszeniom. ESET Inspect koreluje ogromne ilości danych w celu znalezienia zdarzeń będących przyczyną źródłową i kompiluje je w kompleksowe zgłoszenia, dzięki czemu można je natychmiast rozwiązać.

GOTOWOŚĆ DO NATYCHMIASTOWEGO UŻYCIA

Rozwiązanie ESET działa od razu po uruchomieniu, ale jest na tyle zaawansowane, że pozwala doświadczonym specjalistom ds. wykrywania zagrożeń na szczegółowe modyfikacje.

MITRE ATT&CK

ESET Inspect odnosi swoje wykrycia do frameworka MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™), który za pomocą jednego kliknięcia zapewnia kompleksowe informacje nawet o najbardziej złożonych zagrożeniach.

SZCZEGÓŁOWA WIDOCZNOŚĆ SIECI

Dzięki przejrzystym regułom wykrywania (ESET posiada ponad 800 i ta liczba stale rośnie), zaawansowanym wskaźnikom naruszenia bezpieczeństwa (IoC) oraz możliwościom wyszukiwania, dogłębna analiza plików wykonywalnych w sieci pozwoli zidentyfikować wszelkie podejrzane elementy.

ELASTYCZNOŚĆ WDROŻENIA

To Ty decydujesz, w jaki sposób wdrożyć rozwiązanie zabezpieczające: ESET Inspect może działać na własnych serwerach lokalnych lub w chmurze, co pozwala dostosować konfigurację do docelowych kosztów całkowitych posiadania (TCO) oraz możliwości sprzętowych.

Cybersecurity
Progress. Protected.

Możliwości rozwiązania

SYSTEM ZARZĄDZANIA INCYDENTAMI

Grupuj obiekty, takie jak wykrycia, komputery, pliki wykonywalne lub procesy, w logiczne jednostki, aby przeglądać potencjalnie złośliwe zdarzenia na osi czasu wraz z powiązanymi działaniami użytkowników. ESET Inspect automatycznie sugeruje osobie reagującej na incydent wszystkie powiązane zdarzenia i obiekty, które mogą znacznie pomóc na etapach klasyfikacji, badania i rozwiązywania incydentu.

OPCJE REAKCJI W CZASIE RZECZYWISTYM

ESET Inspect oferuje łatwo dostępne działania reagujące jednym kliknięciem, takie jak ponowne uruchomienie lub wyłączenie stacji roboczych, odizolowanie ich od reszty sieci, uruchomienie skanowania na żądanie, zakończenie uruchomionych procesów oraz blokowanie dowolnej aplikacji na podstawie jej wartości skrótu. Ponadto dzięki opcji reakcji w czasie rzeczywistym ESET Inspect, określonej jako Terminal, specjaliści ds. bezpieczeństwa mogą korzystać z pełnego zestawu opcji dochodzeniowych i naprawczych dostępnych w PowerShell.

ANALIZA PRZYCZYN GŁÓWNYCH

Z łatwością przeglądaj analizę przyczyn głównych oraz pełne drzewo procesów dowolnego potencjalnie złośliwego łańcucha zdarzeń, przechodź do pożądanego poziomu szczegółowości i podejmuj świadome decyzje na bazie bogatego kontekstu oraz wyjaśnień przygotowanych przez naszych ekspertów, dotyczących zarówno sytuacji nieszkodliwych, jak i złośliwych.

PUBLICZNE API

ESET Inspect oferuje publiczny interfejs API REST, który umożliwia dostęp do wykrytych zagrożeń i działań naprawczych oraz ich eksportowanie, co pozwala na skuteczną integrację z narzędziami takimi jak SIEM, SOAR, systemy zgłoszeń i wieloma innymi.

WIELE WSKAŹNIKÓW NARUSZENIA BEZPIECZEŃSTWA (IOC)

Przeglądaj i blokuj moduły na podstawie ponad 30 różnych wskaźników, w tym skrótów, modyfikacji rejestru, zmian w plikach oraz połączeń sieciowych.

THREAT HUNTING

Korzystaj z zaawansowanego wyszukiwania IoC opartego na zapytaniach i stosuj filtry do danych surowych w celu sortowania według popularności plików, reputacji, podpisu cyfrowego, zachowania lub innych informacji kontekstowych. Skonfigurowanie wielu filtrów umożliwia zautomatyzowane i łatwe wykrywanie zagrożeń oraz reagowanie na incydenty, w tym wykrywanie i powstrzymywanie zaawansowanych, długotrwałych ataków APT oraz ataków ukierunkowanych.

BEZPIECZNY I PŁYNNY DOSTĘP ZDALNY

Skuteczność reagowania na incydenty i usług bezpieczeństwa zależy od tego, jak łatwy jest do nich dostęp – zarówno pod względem połączenia osoby reagującej na incydent z konsolą, jak i połączenia z punktami końcowymi. Połączenie działa z prędkością zbliżoną do czasu rzeczywistego przy zastosowaniu maksymalnych środków bezpieczeństwa, a wszystko to bez konieczności korzystania z narzędzi innych firm.

IZOLACJA JEDNYM KLIKNIĘCIEM

Zdefiniuj zasady dostępu do sieci, aby szybko powstrzymać ruch boczny złośliwego oprogramowania. Izoluj zainfekowane urządzenie od sieci jednym kliknięciem w interfejsie ESET Inspect i z łatwością usuwaj urządzenia ze stanu izolacji.

WYKRYWANIE ANOMALII I ZACHOWAŃ

Sprawdzaj działania wykonywane przez pliki wykonywalne i korzystaj z systemu reputacji ESET LiveGrid®, aby szybko ocenić, czy uruchomione procesy są bezpieczne, czy też budzą podejrzenia. Monitorowanie nietypowych zdarzeń związanych z użytkownikami jest możliwe dzięki specjalnym regułom zaprogramowanym tak, by uruchamiały się na podstawie zachowania, a nie tylko wykrywania złośliwego oprogramowania lub sygnatur. Grupowanie komputerów według użytkowników lub działów pozwala zespołom ds. bezpieczeństwa ustalić, czy użytkownik ma uprawnienia do wykonania konkretnej czynności, czy też nie.

INTERAKTYWNE RAPORTY ZACHOWAŃ

Natknąłeś się na podejrzany plik? Prześlij go do dogłębnej analizy do ESET LiveGuard Advanced, wyposażonego w potężną piaskownicę w chmurze. W ciągu kilku chwil wyświetl interaktywny raport dotyczący zachowań pliku, zmian w systemie, wywołań API itp. i zablokuj go całkowicie.

TAGOWANIE

Przypisuj i usuwaj tagi w celu szybkiego filtrowania obiektów, takich jak komputery, alarmy, wykluczenia, zadania, pliki wykonywalne, procesy i skrypty. Tagi są udostępniane wszystkim użytkownikom, a po utworzeniu można je przypisywać w ciągu kilku sekund.

FIRMOWA POLITYKA WYKRYWANIE NARUSZEŃ

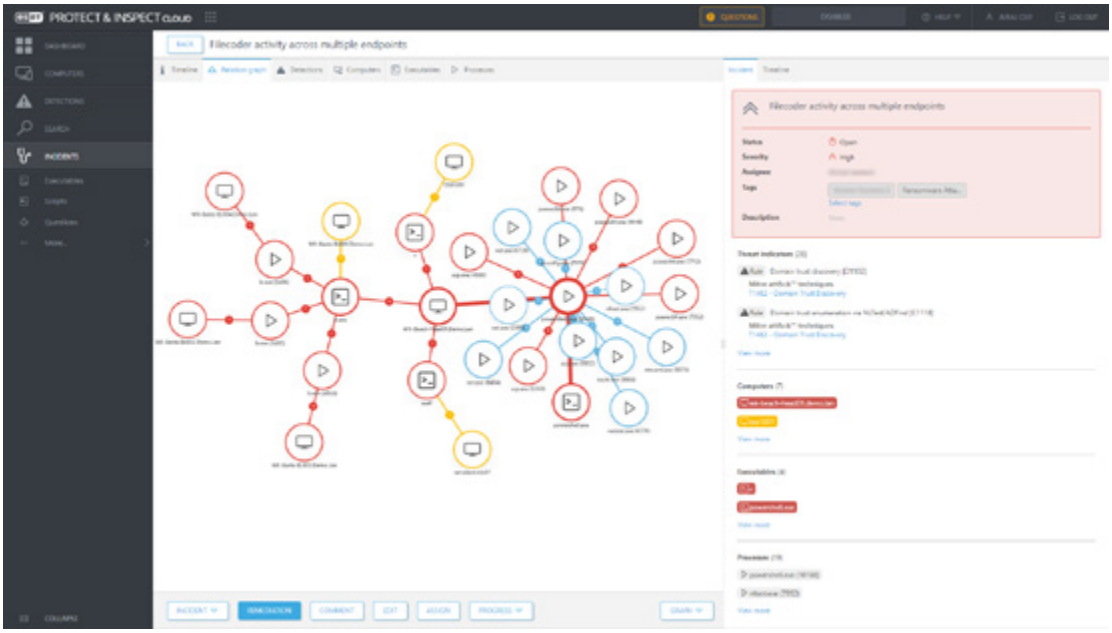
Zablokuj uruchamianie złośliwych modułów na dowolnym komputerze w sieci Twojej organizacji. Otwarta architektura ESET Inspect zapewnia elastyczność w wykrywaniu naruszeń zasad dotyczących korzystania z określonego oprogramowania, takiego jak aplikacje torrentowe, pamięć w chmurze, przeglądanie w sieci Tor lub inne niepożądane oprogramowanie.

OTWARTA ARCHITEKTURA I INTEGRACJE

ESET Inspect zapewnia unikalne wykrywanie oparte na zachowaniu i reputacji, które jest w pełni przejrzyste dla zespołów ds. bezpieczeństwa. Wszystkie reguły można łatwo edytować za pomocą plików XML, co pozwala na ich precyzyjne dostosowanie, lub łatwo tworzyć w celu dopasowania do potrzeb konkretnych środowisk korporacyjnych, w tym integracji z systemami SIEM.

ZAAWANSOWANY SCORING

Ustal priorytety alarmów dzięki funkcji scoringu, która przypisuje wartość ważności do incydentów i pozwala administratorom szybko zidentyfikować komputery o wyższym prawdopodobieństwie wystąpienia potencjalnych incydentów.



Przykłady zastosowań

Wykrywanie behawioralne i powtarzające się przypadki zakażeń

PROBLEM

W Twojej sieci znajdują się użytkownicy, którzy wielokrotnie padają ofiarą złośliwego oprogramowania. Ci sami użytkownicy są zarażani raz po raz. Czy wynika to z ryzykownych zachowań? A może są oni atakowani częściej niż inni użytkownicy?

ROZWIĄZANIE

- ✓ Łatwe wyświetlanie problemowych użytkowników i urządzeń.
- ✓ Szybkie przeprowadzenie analizy przyczyn źródłowych w celu znalezienia źródła infekcji.
- ✓ Usuwanie wykrytych wektorów infekcji, takich jak poczta elektroniczna, Internet lub urządzenia USB.

Łatwa konfiguracja i prosta reakcja - nie jest wymagany zespół ds. bezpieczeństwa

PROBLEM

Nie wszystkie firmy dysponują zespołami ds. bezpieczeństwa, a wprowadzanie i wdrażanie zaawansowanych reguł wykrywania może stanowić wyzwanie.

ROZWIĄZANIE

- ✓ Ponad 300 wbudowanych, wstępnie skonfigurowanych reguł.
- ✓ Łatwa reakcja poprzez jedno kliknięcie przycisku w celu zablokowania, wyłączenia lub poddania kwarantannie urządzeń.
- ✓ Sugerowane działania naprawcze i kolejne kroki są wbudowane w alarmy.
- ✓ Reguły można edytować za pomocą języka XML, co pozwala na łatwe dostosowywanie lub tworzenie nowych reguł.

Wykrywanie i blokowanie zagrożeń

PROBLEM

Twój system wczesnego ostrzegania lub SOC generuje nowe ostrzeżenie o zagrożeniu. Jakie są Twoje kolejne kroki?

ROZWIĄZANIE

- ✓ Wykorzystaj system wczesnego ostrzegania, aby uzyskać dane dotyczące nadchodzących lub nowych zagrożeń.
- ✓ Przeszukaj wszystkie komputery pod kątem obecności nowego zagrożenia.
- ✓ Przeszukaj wszystkie komputery pod kątem wskaźników naruszenia bezpieczeństwa (IoC), które mogłyby świadczyć o istnieniu zagrożenia przed pojawieniem się ostrzeżenia.
- ✓ Zablokuj zagrożenie, uniemożliwiając mu infiltrację sieci lub działanie w organizacji.

Widoczność sieci

PROBLEM

Niektóre firmy martwią się o aplikacje uruchamiane przez użytkowników w systemach. Trzeba zwracać uwagę nie tylko na tradycyjnie instalowane aplikacje, ale także na aplikacje przenośne, które w rzeczywistości nie są instalowane. Jak zachować nad nimi kontrolę?

ROZWIĄZANIE

- ✓ Łatwe przeglądanie i filtrowanie wszystkich zainstalowanych aplikacji na wszystkich urządzeniach.
- ✓ Przeglądanie i filtrowanie wszystkich skryptów na wszystkich urządzeniach.
- ✓ Łatwe blokowanie uruchamiania nieautoryzowanych skryptów lub aplikacji.
- ✓ Podejmuj działania naprawcze, powiadamiając użytkowników o nieautoryzowanych aplikacjach i automatycznie je odinstalowując.

Dogłębne wykrywanie zagrożeń - ransomware

PROBLEM

Firma potrzebuje dodatkowych narzędzi do proaktywnego wykrywania oprogramowania ransomware, a także natychmiastowych powiadomień w przypadku wykrycia w sieci zachowań charakterystycznych dla tego typu złośliwego oprogramowania.

ROZWIĄZANIE

- ✓ Wprowadź reguły wykrywania aplikacji uruchamianych z folderów tymczasowych.
- ✓ Wprowadź reguły wykrywania plików pakietu Office (Word, Excel, PowerPoint) w przypadku uruchamiania przez nie dodatkowych skryptów lub plików wykonywalnych.
- ✓ Generuj alerty w przypadku wykrycia na urządzeniu któregokolwiek z najczęściej spotykanych rozszerzeń oprogramowania ransomware.
- ✓ Wyświetlaj alerty funkcji Ransomware Shield z rozwiązań ESET Endpoint Security w tej samej konsoli.

Analiza i naprawa z uwzględnieniem kontekstu

PROBLEM

Dane są tak dobre, jak kontekst, w jakim się znajdują. Aby podejmować właściwe decyzje, musisz wiedzieć, jakie są te alerty, na jakich urządzeniach się pojawiają i którzy użytkownicy je wywołują.

ROZWIĄZANIE

- ✓ Identyfikuj i sortuj wszystkie komputery zgodnie z usługą Active Directory, automatycznymi grupami lub grupami utworzonymi ręcznie.
- ✓ Zezwalaj na działanie lub blokuj aplikacje lub skrypty w zależności od przynależności komputera do grupy.
- ✓ Zezwalaj na działanie lub blokuj aplikacje lub skrypty w zależności od użytkownika.
- ✓ Otrzymuj powiadomienia wyłącznie dotyczące określonych grup.

ESET Cybersecurity
Progress. Protected.

To jest ESET

Proaktywna ochrona. Minimalizuj ryzyko dzięki prewencji.

Zachowaj przewagę nad znanymi i nowo pojawiającymi się zagrożeniami cybernetycznymi, stosując nasze podejście oparte na prewencji. Łączymy moc sztucznej inteligencji z wiedzą ekspercką, aby zapewnić skuteczną i łatwą w obsłudze ochronę.

ECiesz się najwyższej klasy zabezpieczeniami, które dzięki analizom zagrożeń i wywiadowi cybernetycznemu opracowywane są od ponad 30 lat. To właśnie one zasilają naszą sieć ośrodków badawczo-rozwojowych prowadzonych przez uznanych na świecie ekspertów. ESET PROTECT – nasza oparta na chmurze platforma XDR – łączy zaawansowaną prewencję, detekcję oraz proaktywne wyszukiwanie zagrożeń z szerokim zakresem usług bezpieczeństwa.

Nasze rozwiązania oferują minimalny wpływ na wydajność przy najwyższym poziomie wykrywanie i neutralizowania zarówno znanych, jak i nowych zagrożeń. Wspierają ciągłość działania i redukują koszty wdrożenia oraz utrzymania, dzięki wsparciu technicznemu, której jest prowadzone w języku polskim.

ESET chroni Twoją firmę, abyś mógł w pełni wykorzystać potencjał technologii.

ESET W LICZBACH

1 mld+
chronionych użytkowników Internetu

500k+
klientów biznesowych

178
krajów i terytoriów

11
globalnych ośrodków badań i rozwoju

NASI KLIENCI

MITSUBISHI MOTORS
Drive your Ambition

zabezpieczamy ponad 9 000 stacji roboczych od 2017 roku

BVB 09

chronimy od 2019 r. 1 200 urządzeń i 2 700 skrzynek pocztowych

Canon
Canon Marketing Japan Group

chronimy ponad 32 000 stacji roboczych od 2016 roku

T

partner ISP od 2008 roku baza ponad 2 milionów 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 serwisie Gartner® Peer Insights™. „**Voice of the Customer**" Endpoint Protection Platforms report 2026

FROST & SULLIVAN

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