www.4sync.pl
sales@4sync.pl tel.: 22 299 17 00

KARTA DANYCH TECHNICZNYCH

Fidelis Endpoint®

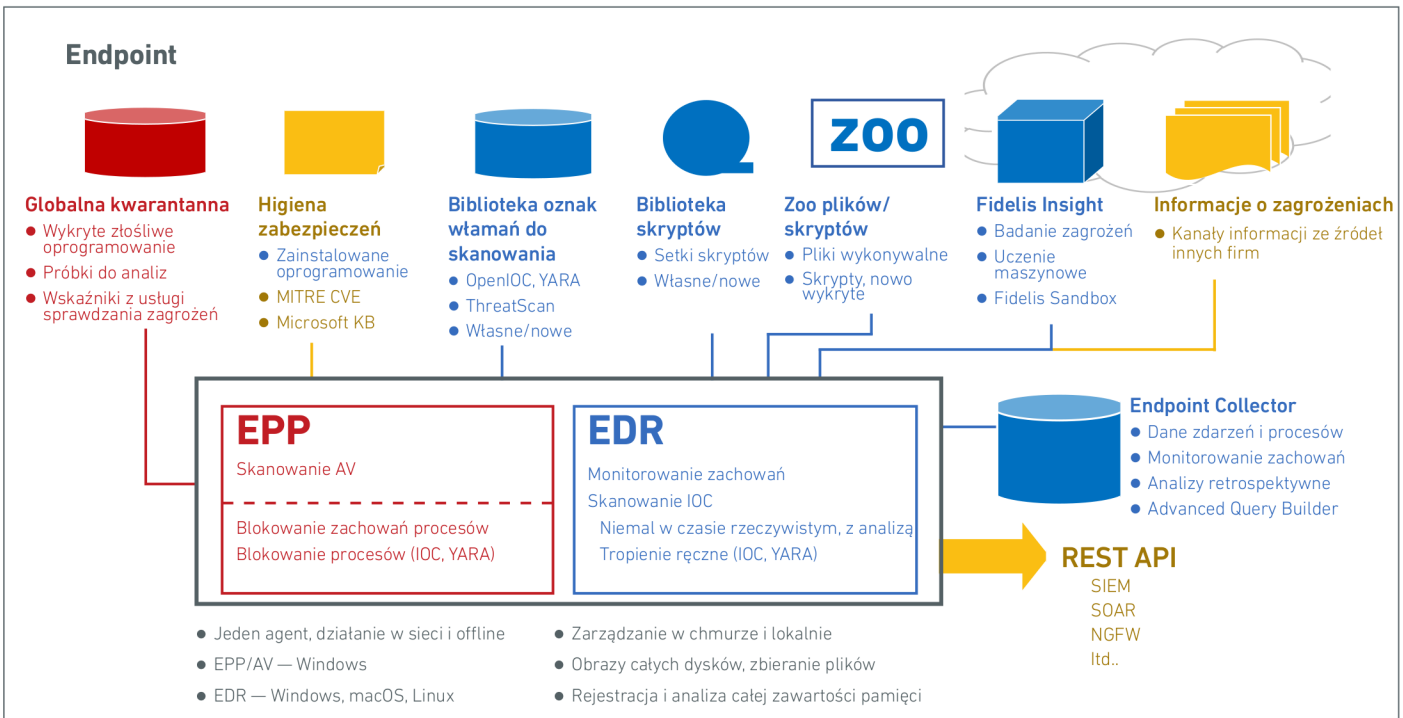
Zapobieganie incydentom i ich wykrywanie, analizy śledcze i reakcje przy użyciu jednego agenta

Fidelis Endpoint łączy w sobie niezawodne funkcje ochrony punktów końcowych, wykrywania związanych z nimi incydentów i reagowania, analiz śledczych i dochodzeń oraz zarządzania systemami, a wszystkie one są dostępne w ramach jednego agenta.

Fidelis Endpoint ma architekturę jednoagentową z zarządzanymi w chmurze lub lokalnie mechanizmami obronnymi, które działają zarówno przy aktywnym połączeniu z siecią, jak i jego braku. Rozwiązanie to udostępnia szereg efektywnych funkcji do najbardziej zaawansowanych i dojrzałych środowisk ochrony bezpieczeństwa, a ponadto można je skalować do obsługi 100 000 punktów końcowych.

Fidelis Endpoint to jedyny produkt, który oferuje:

- Jednego agenta udostępniającego najlepsze w swojej klasie funkcje AV i niezrównane mechanizmy EDR w systemie Windows
- Zaawansowane funkcje EDR oparte na oznakach włamań IOC i YARA dla systemów Windows, macOS i Linux
- Metadane zdarzeń i procesów do analiz w czasie rzeczywistym i retrospektywnych oraz zoo plików i skryptów
- Otwarte kanały informacji o zagrożeniach (Fidelis Insight, open source oraz źródła innych firm i przygotowane we własnym zakresie)
- Automatyzację funkcji zapobiegania incydentom i ich wykrywania, analiz śledczych i reakcji oraz obsługa własnych skryptów
- Opcjonalne usługi zarządzanego wykrywania i reagowania (MDR), które zapewniają całodobowe czuwanie na środowiskiem oraz realizację niezbędnych operacji wykrywania i reakcji, a także kontakt z analitykami



Fidelis Endpoint oferuje zapobieganie incydentom (kolor czerwony), ich wykrywanie i reagowanie na nie (kolor niebieski), udostępnianie informacji o zagrożeniach ze źródeł innych firm i integrację (kolor brązowy) w ramach jednego agenta z mechanizmami obronnymi działającymi zarówno przy aktywnym połączeniu z siecią, jak i jego braku.

Zapobieganie

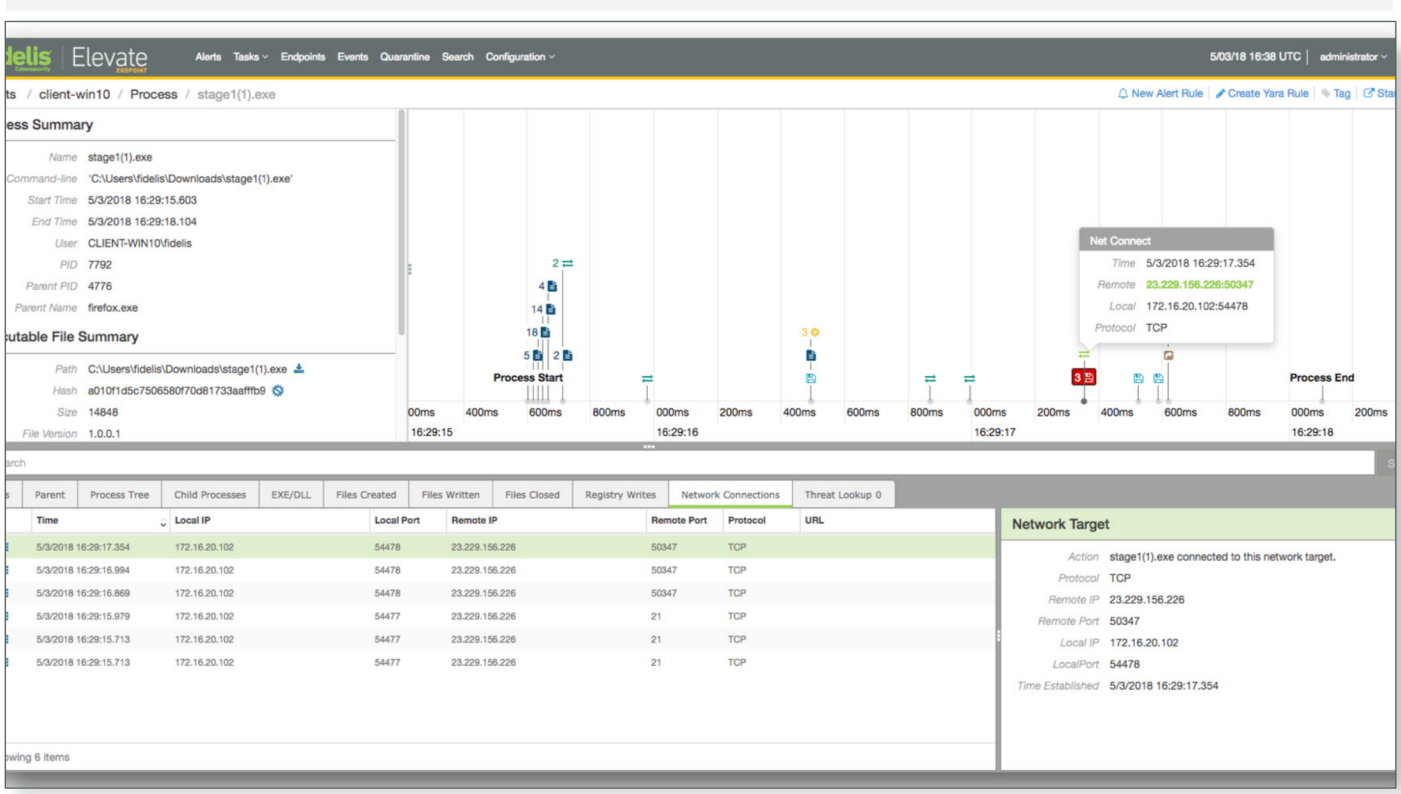
- **Najlepsza w swojej klasie ochrona antywirusowa** do systemu Windows wspomagana przez narzędzie BitDefender i oparta na behawioralnych i heurystycznych mechanizmach obronnych oraz sygnaturach — obejmuje również ochronę sektora rozruchowego i globalną kwarantannę wykrytego złośliwego oprogramowania na potrzeby analizy
- **Usługa sprawdzania zagrożeń** udostępnia ustalane w chmurze wskaźniki wykrywania na podstawie informacji z różnych skanerów
- **Aktualne informacje o zagrożeniach** z uwzględnieniem modeli zachowań ML i symptomów ataku wykrywanych w plikach przez oprogramowanie antywirusowe, co zapewnia ochronę punktów końcowych zarówno przy aktywnym połączeniu z siecią, jak i jego braku
- **Blokowanie zachowań procesów** oraz stosowanie reguł IOC i YARA do blokowania procesów w odniesieniu do punktów końcowych w całej firmie (działają niezależnie od wybranego przez klienta mechanizmu AV)
- **Raporty o zainstalowanym oprogramowaniu**, umożliwiające identyfikację punktów końcowych ze znanymi lukami w zabezpieczeniach oraz udostępniające linki do raportów MITRE CVE lub Microsoft KB
- **Higiena zabezpieczeń punktów końcowych**, w tym statusy systemów operacyjnych i zastosowanych poprawek, możliwość raportowania oraz zmian statusów zapory i ochrony antywirusowej hosta, a także alerty o podłączaniu urządzeń do portów USB
- **Szybkie przechodzenie od alertów ochrony antywirusowej do drzewa procesów** ze szczegółami zdarzeń udostępniającymi kontekst dla źródła złośliwego oprogramowania przy wykorzystaniu potencjału, jakie daje połączenie funkcji zapobiegania i wykrywania
- **Ograniczenie fałszywych alertów i ręcznego dostosowywania** białych list, kontenery izolacyjne oraz autonomiczne, oparte na uczeniu maszynowym mechanizmy wykrywania anomalii w celu zapobiegania zagrożeniom

Wykrywanie

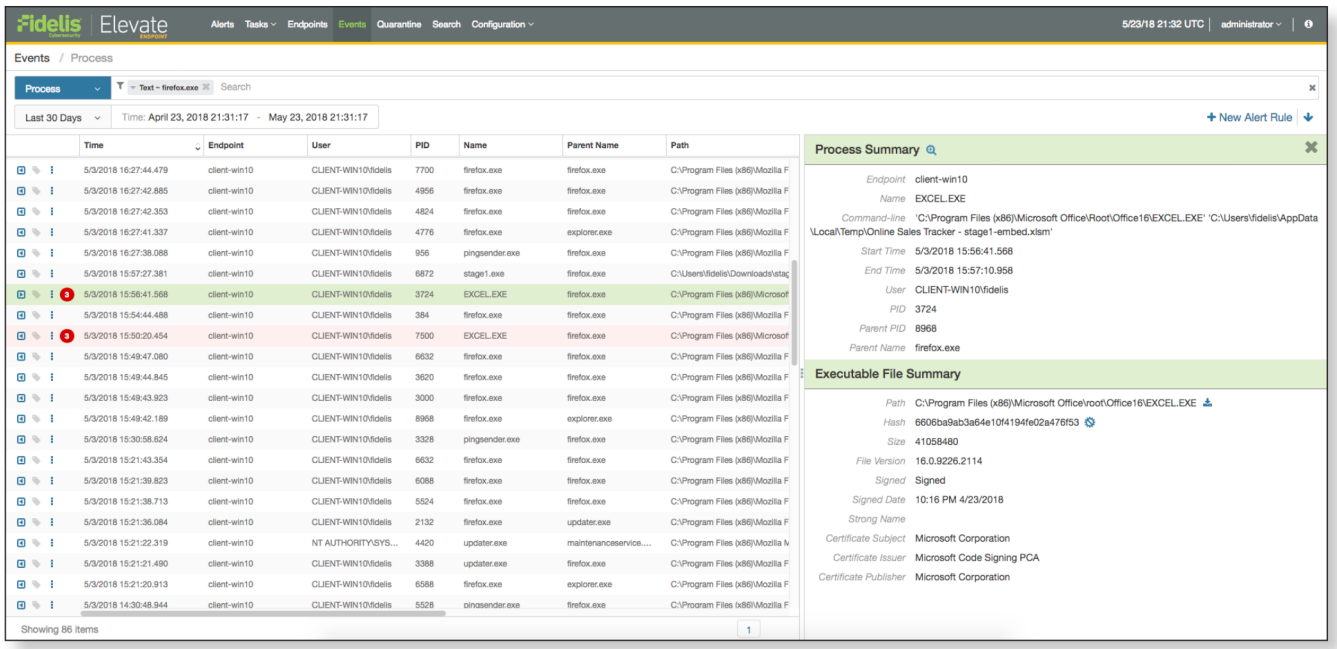
- **Zaawansowane funkcje EDR** w systemach Windows, macOS i Linux
- **Otwarte kanały informacji o zagrożeniach** ze źródeł innych firm, opracowywanych wewnętrznie oraz z Fidelis Insight (w tym sandboxing, uczenie maszynowe i badania zagrożeń)
- **Własne, niestandardowe reguły zachowań** z zastosowaniem oznak behawioralnych — uzupełnienie reguł zachowań wbudowanych w rozwiązanie Fidelis
- **Biblioteka oznak włamań do skanowania**, wyposażona w pełne zestawienia oznak IOC i YARA, a także umożliwiająca dodawanie nowych oznak OpenIOC i YARA
- **Szczegółowe metadane zdarzeń i procesów z 30, 60 lub 90 dni** do analiz w czasie rzeczywistym i retrospektywnych z uwzględnieniem pozyskiwanych informacji o zagrożeniach oraz obsługa niestandardowych operacji wyszukiwania i tropienia
- **Automatyczne uwzględnianie informacji o zagrożeniach** w celu wykrywania zagrożeń związanych ze zdarzeniami systemowymi Windows
- **Analizy z odtwarzaniem** umożliwiają rejestrowanie kluczowych zdarzeń i automatyczne prezentowanie osi czasu związanej z podejrzewanymi incydentami oraz alertów z przypisanymi priorytetami
- **Wykonywane na żądanie skanowanie** systemów plików i pamięci przy użyciu biblioteki oznak włamań do skanowania
- **Obsługa przy połączeniu z siecią i jego braku** — w takich przypadkach operacje analiz i wykrywania są wykonywane lokalnie, a dane przechowywane w pamięci podręcznej do czasu przywrócenia połączenia z siecią i wznowienia zadań

NOWOŚĆ: zoo plików wykonywalnych i skryptów

- Repozytorium pierwszych egzemplarzy plików wykonywalnych i skryptów z punktu końcowego
- Rozwiązanie problemu złośliwego oprogramowania usuwającego pliki w celu ukrycia śladów swojej aktywności



Oś czasu zdarzeń udostępnia obraz i kontekst wszystkich działań związanych z punktami końcowymi — np. alertów, procesów nadrzędnych, drzewa procesów, procesów podrzędnych, załadowanych bibliotek DLL i plików exe, utworzonych plików, zapisanych plików, zamkniętych plików i połączeń sieciowych — a także funkcje sprawdzania zagrożeń.



Fidelis Endpoint rejestruje i przechowuje dane zdarzeń i alertów, aby umożliwić łatwe poszukiwanie, identyfikację oraz analizy śledcze zagrożeń i metod działania hakerów.

Analizy śledcze

- **Integralność sprawdzana metodą analiz śledczych** przez zapisywanie obrazów całych dysków w kontenerach śledczych oraz zbieranie plików i folderów, rejestrację zawartości pamięci i jej analizy na żywo
- **Kontekst zdarzeń**, czyli informacje o wszystkim, co miało miejsce w wybranym punkcie końcowym w każdym punkcie czasu mieszczącym się w przedziale określonym w narzędziu Endpoint Collector, z uwzględnieniem zdarzeń systemowych, plików lub znanych złych procesów
- **Endpoint Collector** zapewnia analizy śledcze w czasie rzeczywistym i retrospektywne oraz obsługuje niestandardowe operacje wyszukiwania i tropienia
- **Kreator zaawansowanych zapytań** wykracza poza aspektowe wyszukiwanie z zastosowaniem wyrażeń boolowskich na potrzeby analiz śledczych, tworzenia reguł zachowań i tropienia zagrożeń
- **Raporty o zainstalowanym oprogramowaniu**, umożliwiające identyfikację punktów końcowych ze znanymi lukami w zabezpieczeniach oraz udostępniające linki do raportów MITRE CVE lub Microsoft KB
- **Izolacja systemów punktów końcowych** na potrzeby analiz śledczych z dostępem przy użyciu konsoli lub wyznaczonego do tego celu innego systemu
- **Biblioteka skryptów** zawiera gotowe skrypty do zbierania artefaktów na potrzeby automatyzacji analiz śledczych, a także obsługuje niestandardowe skrypty, dzięki którym można zautomatyzować zadania analiz

Reagowanie

- **Gotowe i definiowane przez użytkownika zautomatyzowane reakcje na alerty** umożliwiają izolację punktów końcowych z zachowaniem możliwości dostępu z konsoli i uruchamiania gotowych procedur lub uruchamiania zadań klasyfikacji alertów w celu gromadzenia materiału dowodowego i zrzutów pamięci
- **Skrypty** umożliwiają przywracanie ostatniej znanej dobrej konfiguracji punktu końcowego
- **Wbudowane mechanizmy reakcji** obejmują przerywanie procesów, zbieranie lub usuwanie plików, jeśli biblioteka skryptów udostępnia wbudowane skrypty reakcji, a także obsługę nowych, własnych skryptów reakcji
- **Wbudowana integracja** z FireEye, Palo Alto Networks oraz wybranymi systemami SIEM i NGFW przy użyciu interfejsu REST API

Zarządzanie

- ✓ Grupy dynamiczne tworzone na podstawie cech są automatycznie aktualizowane i umożliwiają lepszą segmentację oraz łatwiejsze zarządzanie zasadami
- ✓ Możliwość konfigurowania subskrypcji alertów według poziomu istotności w przypadku poczty e-mail, aplikacji Microsoft Teams, komunikatora Slack itd.
- ✓ Skrypty do zarządzania systemami oferują profile sprzętu i systemów operacyjnych, inwentaryzację oprogramowania, sprawdzanie zainstalowanych aktualizacji i poprawek oraz wymuszanie aktualizacji
- ✓ Funkcja sprawdzania statusów podłączenia agentów oferuje profil punktów końcowych będących w trybie online i aktywnych lub dawno nie widzianych
- ✓ Strona stanu systemu udostępnia statusy usług, serwerów i kontenerów oraz możliwość zbierania dzienników i uruchamiania bądź zatrzymywania usług
- ✓ Mechanizmy kontroli dostępu na podstawie ról umożliwiają określanie uprawnień użytkowników na poziomie punktów końcowych, skryptów i systemu
- ✓ Punkty końcowe korzystają z bezpiecznych kanałów komunikacji z agentem przy użyciu połączenia WebSocket z szyfrowaniem TLS v1.2, co pozwala na nieobciążające połączenia oraz szybkie interakcje i reakcje

Opcje wdrożeń

Lokalne:

- Klient zajmuje się utrzymaniem wszystkich programów oraz zarządzaniem nimi
- Profesjonalne usługi Fidelis stanowią pomoc we wdrożeniu i szkoleniach
- Opłaty za utrzymanie obejmują aktualności o zagrożeniach dostarczane przez zespół firmy Fidelis ds. badania zagrożeń
- Licencje na dodatkowych agentów w miarę wzrostu potrzeb

W chmurze:

- DInfrastruktura jest utrzymywana przez firmę Fidelis, dzięki czemu klient może się skupić na kwestiach bezpieczeństwa
- Szybkie wdrożenie i błyskawiczna implementacja
- Skalowanie stosownie do wzrostu potrzeb — z udostępnieniem dowolnej wymaganej liczby agentów punktów końcowych
- Niezakłócone działanie podczas przejścia ze środowiska testowego do produkcyjnego
- Ceny w uproszczonym modelu subskrypcyjnym zgodnie z zapotrzebowaniem klienta na liczbę agentów i pamięć masową

Zalety integracji z platformą Fidelis Elevate

- Rozwiązania Fidelis Endpoint i Network są w pełni zintegrowane, co oznacza jedną konsolę do weryfikacji alertów z sieci do punktów końcowych, a także obraz szerszego zakresu zagrożeń dzięki analizom obejmującym wszystkie sesje z punktów końcowych do sieci i analizom wieloaspektowym
- Alerty generowane przez Fidelis Deception są płynnie przekazywane do rozwiązania Fidelis Endpoint w celu zbadania hostów, których zabezpieczenia zostały naruszone, a „okruszki chleba" (ang. breadcrumb) rozmieszczone w punktach końcowych pełnią rolę przynęt prowadzących do wabików (ang. decoy), umożliwiając wykrycie zagrożenia po włamaniu
- Fidelis Endpoint automatyzuje też dystrybucję „okruszków chleba" i cykle ich odświeżania, zapewniając determinizm i skuteczność dezinformacji

Opcjonalne usługi zarządzanego wykrywania i reagowania (MDR)

Fidelis Endpoint jest zaawansowanym, precyzyjnym narzędziem do zapobiegania incydentom i ich wykrywania, analiz śledczych i reagowania, obsługującym wysoki stopień automatyzacji przy użyciu skryptów, a także otwarte kanały informacji o zagrożeniach i funkcje dostosowywania. Przy nielicznym i mocno obciążonym zespole ds. bezpieczeństwa zapewnienie obsługi non stop może być trudne. Dlatego właśnie oferujemy usługi MDR, świadczone przez naszych ekspertów ds. bezpieczeństwa, którzy mają duże doświadczenie zdobyte podczas reakcji w ponad 4000 przypadków.

Firma Fidelis oferuje zaawansowane rozwiązania, informacje o zagrożeniach i usługi zarządzane, w tym proaktywne umowy o dyspozycyjności do reagowania na incydenty.

„Największą korzyścią z wdrożenia rozwiązania Fidelis Endpoint jest to, że wreszcie jesteśmy w stanie własnymi siłami reagować na złamania zabezpieczeń. Dzięki temu znacznie skróciliśmy nasz czas reakcji na cyberprzestępstwa: z 10 dni do zaledwie 5 godzin".

— Dyrektor ds. informatyki śledczej i eDiscovery jednego z pięciu największych banków świata

Aby dowiedzieć się więcej, skontaktuj się z nami

Fidelis Cybersecurity | 800 652 4020 | info@fidelissecurity.com

Fidelis Cybersecurity jest czołowym dostawcą rozwiązań do wykrywania i tropienia zagrożeń oraz reagowania na nie. Fidelis zwalcza całą gamę cyberprzestępstw, w tym kradzież danych i szpiegostwo, zapewniając pełny obraz środowisk hybrydowych z infrastrukturą chmurową i lokalną, automatyzując wykrywanie zagrożeń i kradzieży danych, wspomagając tropienie zagrożeń i optymalizując reakcje na incydenty dzięki kontekstom, szybkości i dokładności. Rozwiązania Fidelis są używane jako ostatnia linia obrony przez wiele firm z grupy Global 1000 oraz władz państwowych. Zapraszamy na wspólne łowy. Więcej informacji: www.fidelissecurity.com.

 Fidelis-Endpoint-1902 PL