DATA SHEET

FireEye Endpoint Security

Wiele technologii bezpieczeństwa w pojedynczym agencie

Podstawowe Informacje:

- Zapobiega większości cyber-ataków skierowanych przeciwko stacją końcowym.
- Wykrywa i blokuje próby włamań w trakcie ich trwania, aby zmniejszyć obszar ataku.
- Zwiększa produktywność i efektywność, wykrywając faktyczne zagrożenia zamiast skupiać się na pogoni za alertami.
- Wykorzystuje pojedynczego, lekkiego agenta,, w celu jak najmniejszego obciążenia stacji użytkownika.
- Zapewnia zgodność z normą Common Criteria i standardem FIPS.
- Wdrażany zarówno jako fizyczny appliance lub subskrypcja w chmurze.

Tradycyjne platformy do ochrony stacji końcowych dotychczas nie były projektowane do walki z zaawansowanymi ukierunkowanymi atakami (APT – Advanced Persistent Threats). Aby stacja końcowa była gotowa na nowoczesne formy ataków, rozwiązanie do ochrony musi szybko analizować i reagować na takie zagrożenia.

Wykwalifikowani cyberprzestępcy potrafią omijać tradycyjne metody ochrony stacji roboczych, na których wcześniej mogły polegać zespoły ds. bezpieczeństwa. Jeśli nawet jedno z istniejących zabezpieczeń jest w stanie zatrzymać jakieś znane zagrożenie, to nie może ono potwierdzić działania i celu potencjalnego ataku.

Aby chronić przed powszechnym malware'em rozwiązania EPP (Endpoint Protection Platform) korzystają z silników sygnaturowych. Zagrożenia nie opisane jeszcze sygnaturą, Malware Guard wykrywa wykorzystując algorytmy uczenia maszynowego. Algorytmy te zasilone są wiedzą FireEye, pochodzącą z setek tysięcy godzin spędzonych rocznie na świadczeniu usług Incident Response i walce zarówno z malware'em jak i grupami hakerskimi.

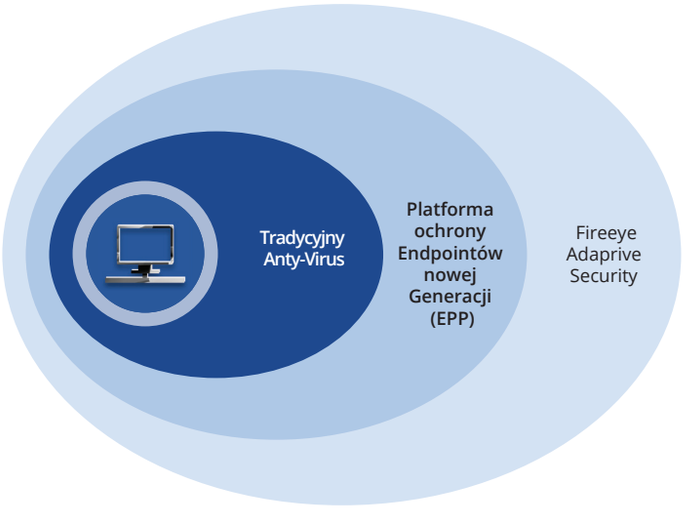
Aby poradzić sobie z zaawansowanymi metodami ataków FireEye Endpoint Security wykorzystuje funkcjonalności Endpoint Detection and Response (EDR) takie, jak silniki analityczne bazujące na zachowaniach. Jako finał analizy Fireeye Endpoint Security odnajduje ukryte zagrożenia, wykorzystując w czasie rzeczywistym silnik monitorujący IOCs (Indicators of Compromise), bazujące na doświadczeniu FireEye w walce z atakami na całym świecie.

Niemniej nawet posiadając najlepszą ochronę włamania, są nieuniknione. Aby zapewnić rzetelną odpowiedź i szybką reakcję na incydenty, minimalizując zakłócenia w działaniu organizacji, Fireeye Endpoint Security daje następujące możliwości:

- Wyszukiwanie w trakcie śledztwa znanych i nieznanych zagrożeń i artefaktów, nawet na dziesiątkach tysięcy stacji w czasie minut.
- Weryfikowanie i uszczegółowianie dróg ataku użytych do infiltracji stacji.
- Potwierdzanie czy atak miał miejsce (i czy nadal trwa) na konkretnej stacji i gdzie rozprzestrzenił się dalej.
- Ustalanie chronologii, czasu trwania ataku na stację i dalsze śledzenie incydentu.
- Dokładna weryfikacja, które stacje wymagają odseparowania od środowiska produkcyjnego w celu zapobiegnięcia dalszemu rozprzestrzenianiu się ataku.

IT is a strategic enabler that drives our ability to effectively educate our students. Utilizing FireEye Endpoint Security ensures that our IT assets are available, highly functioning, and secure, which is critical to achieving our mission.

— James D. Perry II
Chief Information Security Officer, University of South Carolina



Often, management thinks any virus is almost the end of the world. With FireEye, I can bring real evidence to display about the nature of the issue and that we've been able to manage and contain it. Making all of those unknowns known quickly helps to take the pressure down for everybody in the organization.

— Michael Hennessy, Director Technology Services
Alpha Grainer Manufacturing, Inc

Podstawowe funkcjonalności:

- Pojedynczy agent z trzema silnikami detekcji, aby zminimalizować ilość konfigurowania, a zmaksymalizować możliwości wykrywania i blokowania ataków.
- Pojedynczy zintegrowany workflow do analizy i reakcji na zagrożenia w ramach jednego rozwiązania.
- W pełni zintegrowana ochrona na bazie silników anty-wirusowych, analizy zachowań, uczenia maszynowego i wskaźników (IOCs) oraz pełna widoczność działania stacji.
- Triage Summary i Audit Viewer jako narzędzia do dokładnego śledztwa i analizy zagrożeń.
- Izolacja zagrożeń i zainfekowanych hostów za pomocą pojedynczego kliknięcia przy zachowaniu możliwości dokładniejszego zbadania problemu.

Dodatkowe funkcjonalności:

- Enterprise Security Search do wykonywania szybkiego oraz dokładnego wyszukiwania IoC na komputerach w i poza siecią LAN organizacji.
- Data Acquisition do zdalnego badania stacji i gromadzenia dowodów ataku.
- Produkt rozszerza analizę zagrożeń od warstwy sieci do stacji końcowych zapewniając wszechstronną i zintegrowaną ochronę przed zaawansowanymi zagrożeniami.
- Błyskawiczna detekcja, analiza i izolacja zagrożeń na dziesiątkach tysięcy hostów (podłączonych lub nie do sieci firmowej).
- Przyjazny interfejs, pozwalający na szybką interpretację i reakcję na jakąkolwiek podejrzaną aktywność stacji.

Wspierane Systemy Operacyjne	
Windows	XP SP3, 2003 SP2, Vista SP1 and up, 2008, Win7, 2012, 8, 8.1, 10, Server 2016
Mac	OS X 10.9+
Linux	Red Hat Enterprise Linux 6.8+, 7.2 + CentOS 6.9+, 7.4+

Opcje wdrożenia: Fizyczny appliance w środowisku użytkownika, Wirtualny appliance w środowisku użytkownika, Subskrypcja w chmurze Fireeye.

ICSA labs CERTIFIED ANTI-VIRUS

vb 100 VIRUS virusbtn.com

Aby dowiedzieć się więcej, odwiedź stronę: **www.FireEye.com**

Autoryzowany Dystrybutor rozwiązań FireEye w Polsce:

Arrow ECS Sp. z o.o., ul. Sosnowiecka 79, 31-345 Kraków
tel. +48 12 616 43 00, e-mail: fireeye.ecs.pl@arrow.com
www.arrowecs.pl

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

DLACZEGO FIREEYE?

SPECJALISTYCZNA WIEDZA. TECHNOLOGIA. INTELIGENCJA.

FireEye dysponuje unikalną w branży zabezpieczeń IT kombinacją specjalistycznej wiedzy, technologii oraz praktycznego doświadczenia z realizacji usług Incident Response.Specjaliści ds. zabezpieczeń FireEye współpracują ze wszystkimi klientami, aby zrozumieć i rozwiązać określone problemy z zabezpieczeniami, zapewniając szybkie odpowiedzi najwyższej klasy ekspertów. Platforma ochrony przed zagrożeniami zapewnia firmie FireEye wgląd w unikalne informacje o świecie zaawansowanych zagrożeń, atakach kierowanych, ciągłych zagrożeniach i cyberprzestępczości, umożliwiając firmie FireEye udostępnianie klientom branżowej i dynamicznej analizy zagrożeń. FireEye dostarcza specjalistyczną wiedzę i analitykę niezbędne organizacjom do ochrony przed współczesnymi zagrożeniami.

FIREEYE™