

*„Fundamentalną wadą dzisiejszej infrastruktury cyberbezpieczeństwa jest fakt, że detekcja zachodzi PRZED zatrzymaniem. Sygnatury wytwarzane przez ludzi bazują głównie na poprzednio wykrytych próbkach. To niewystarczające rozwiązanie, ponieważ złośliwe oprogramowanie typu „Zero-Day” działa cicho i bez żadnych przeszkód.” - Stuart McClure, założyciel i CEO Cylance®*

## Bezpieczeństwo przygotowane na przyszłość

---

CylancePROTECT przez wykorzystanie sztucznej inteligencji do wykrywania i powstrzymywania w czasie rzeczywistym złośliwych ataków na komputery na nowo określa co program antywirusowy robi i powinien robić dla firmy.

Stosowanie przez CylancePROTECT podejścia matematycznego do wykrywania złośliwego oprogramowania z użyciem technik nauki maszynowej (oczekującej na opatentowanie) w miejsce sygnatur i reaktywnych Sandboxów sprawia, że nowe złośliwe oprogramowanie, wirusy, boty i inne nieznanne, przyszłe warianty, stają się bezużyteczne.

Firma Cylance stworzyła najcelniejsze, najbardziej efektywne i wydajne rozwiązanie do powstrzymywania zaawansowanych zagrożeń oraz złośliwego kodu przed wykonaniem na urządzeniach końcowych.

W sercu niespotykanej dotąd technologii identyfikacji firmy Cylance leży rewolucyjna platforma samoucząca się, wykorzystująca moc nauk o algorytmach i sztucznej inteligencji. Analizuje i klasyfikuje ona setki tysięcy cech na jeden plik, sprowadzając je do poziomu atomowego, aby określić w czasie rzeczywistym, czy dany obiekt jest "dobry" czy „zły”.

## Jak to działa?

---

Architektura CylancePROTECT składa się z małego agenta integrowanego z istniejącymi systemami zarządzania oprogramowaniem lub konsolą Cylance. Na urządzeniu końcowym wykrywanie i powstrzymywanie złośliwych procesów odbywa się poprzez użycie przetestowanych modeli matematycznych po stronie hosta, niezależnie od chmury czy sygnatur. Możliwa jest detekcja oraz kwarantanna złośliwego oprogramowania zarówno w otwartych jak i odizolowanych sieciach bez konieczności ciągłego aktualizowania sygnatur.

Obrona wymaga stosowania najlepszej ochrony w miejscach najbardziej wystawionych na ataki - punktach końcowych. Matematyczne podejście Cylance zatrzymuje wykonanie groźnego kodu, nieważne, czy zagrożenie te było wcześniej znane, czy jest to nowy rodzaj złośliwej technologii. Żadne inne oprogramowanie tego typu nie może równać się z CylancePROTECT pod względem precyzji, łatwości obsługi oraz efektywności działania.

## Kompatybilność z systemami operacyjnymi Microsoft Windows® i Mac OS® X

CylancePROTECT jest kompatybilny z obecnymi wersjami systemów operacyjnych Microsoft Windows i Mac OS.

Microsoft Windows (32 lub 64 bity)	Mac OS
Windows XP SP3 Windows Vista Windows 7 Windows 8 i 8.1 Windows 10 Windows Server 2008 / 2008 R2 Windows Server 2012 / 2012 R2	Mac OS X 10.9 (Mavericks) Mac OS X 10.10 (Yosemite) Mac OS X 10.11 (El Capitan)
2 GB pamięci	2 GB pamięci
500 MB wolnego miejsca na dysku	500 MB wolnego miejsca na dysku
Wymaga: .NET Framework 3.5 SP1 Przeglądarki internetowej Połączenie internetowe do rejestracji produktu Lokalne uprawnienia administracyjne do instalacji	Wymaga: Przeglądarki internetowej Połączenie internetowe do rejestracji produktu Lokalne uprawnienia administracyjne do instalacji

### O Cylance:

Cylance to pierwsza firma, która wykorzystwała sztuczną inteligencję, algorytmy naukowe i naukę maszynową w dziedzinie cyberbezpieczeństwa, aby wesprzeć firmy, rządy i użytkowników końcowych w aktywnym rozwiązywaniu najtrudniejszych zagadnień dotyczących bezpieczeństwa. Poprzez użycie przełomowego procesu analizy predyktywnej Cylance może szybko i skutecznie identyfikować, co jest bezpieczne, a co stanowi zagrożenie, a nie to, czy dopuścić coś do działania lub nie. Połączenie zaawansowanej nauki maszynowej ze sztuczną inteligencją oraz unikalnym zrozumieniem mentalności hakerów sprawia, że Cylance dostarcza technologię, która reagują przeciwko zaawansowanym zagrożeniom predyktywnie i podczas ataków.

**VIDA**

Teatralna 8/13, 40-003 Katowice

+48 32 252 13 10

+48 32 350 00 50

cylance@vida.pl



**CYLANCE™**