**Cisco redefiniuje bezpieczeństwo centrów danych i chmury w erze AI**

*Cisco Hypershield oferuje przedsiębiorstwom hiperskalowalny poziom zabezpieczeń i łączności*

**Najważniejsze informacje:**

* Cisco wspiera i chroni filar rewolucji AI – centra danych i chmury obliczeniowe w skali AI – aby zapewnić bezpieczeństwo każdej aplikacji i urządzenia bez względu na to, jak są rozproszone i połączone.
* We współczesnym wysoce rozproszonym świecie czas od wykrycia podatności do wykorzystania jej skraca się – a obrona przed coraz bardziej wyrafinowanymi i złożonymi zagrożeniami w centrach danych wykracza poza skalę ludzkich możliwości.
* Cisco Hypershield pozwala klientom wdrażać mechanizmy zabezpieczające wszędzie tam, gdzie są potrzebne – w chmurze, w centrum danych, w hali produkcyjnej lub w szpitalnej pracowni.
* Dzięki bezpieczeństwu AI-native klienci mogą autonomicznie segmentować swoje sieci, korzystać z rozproszonej i niemal natychmiastowej ochrony przed exploitami bez łat bezpieczeństwa oraz aktualizacji oprogramowania bez przestojów.

**WARSZAWA, 18 kwietnia, 2024** — Cisco, lider w dziedzinie bezpieczeństwa i sieci, w odpowiedzi na rosnące wymagania, jakie przed infrastrukturą IT stawia rewolucja AI, zaprezentował zupełnie nowe podejście do ochrony centrów danych i chmur obliczeniowych. Firma zmienia sposób, w jaki wykorzystujemy i zabezpieczamy sztuczną inteligencję i inne nowoczesne przepływy pracy za pomocą Cisco Hypershield, pierwszego w branży rozwiązania w swojej klasie.

**Hypershield przechyla szalę na korzyść obrońców**

Cisco Hypershield chroni aplikacje, urządzenia i dane w publicznych oraz prywatnych centrach danych, chmurach i lokalizacjach fizycznych. Rozwiązanie, od samego początku projektowane i budowane z myślą o sztucznej inteligencji, umożliwia organizacjom osiągnięcie wyników w zakresie bezpieczeństwa wykraczających poza możliwości człowieka.

– Cisco Hypershield to jedna z najważniejszych innowacji w zakresie bezpieczeństwa w naszej historii – powiedział **Chuck Robbins, prezes i dyrektor generalny Cisco**. – Dzięki przewadze naszych danych i sile w obszarach platform bezpieczeństwa, infrastruktury i obserwowalności, Cisco osiągnęło wyjątkową pozycję umożliwiającą niesienie pomocy klientom w wykorzystaniu mocy sztucznej inteligencji.

Hypershield to nowa, rewolucyjna architektura zabezpieczeń. Została zbudowana w oparciu o technologię opracowaną pierwotnie dla hiperskalowych chmur publicznych, a teraz jest dostępna dla zespołów IT w przedsiębiorstwach każdej wielkości. Hypershield jest bardziej „tkaniną” niż „ogrodzeniem”, umożliwiając egzekwowanie polityk bezpieczeństwa w każdej usłudze aplikacyjnej w centrum danych, w każdym klastrze Kubernetes w chmurze publicznej, w każdym kontenerze i maszynie wirtualnej. Hypershield może nawet przekształcić każdy port sieciowy w wysokowydajny punkt egzekwowania polityk bezpieczeństwa, wprowadzając zupełnie nowe możliwości bezpieczeństwa nie tylko w chmurach, ale także w centrum danych, hali produkcyjnej lub w szpitalnej pracowni. Nowa technologia blokuje exploity aplikacji w przeciągu minut i zatrzymuje ruchy boczne w obrębie sieci.

– Sztuczna inteligencja ma potencjał, aby 8 miliardów ludzi na świecie miało taki sam wpływ jak 80 miliardów. Przy tej obfitości musimy na nowo wyobrazić sobie rolę centrum danych – to, w jaki sposób centra danych są połączone, zabezpieczone, obsługiwane i skalowane - powiedział **Jeetu Patel, wiceprezes wykonawczy i dyrektor generalny ds. bezpieczeństwa i współpracy w Cisco**. - Siła Cisco Hypershield polega na tym, że może ono zapewnić bezpieczeństwo wszędzie tam, gdzie jest to potrzebne – w oprogramowaniu, na serwerze, a w przyszłości nawet w przełączniku sieciowym. W przypadku systemu rozproszonego, który może obejmować setki tysięcy punktów egzekwowania polityk, kluczowe znaczenie ma uproszczone zarządzanie. A my musimy być o rzędy wielkości bardziej autonomiczni zachowując o rzędy wielkości niższe koszty.

**Trzy filary hiper-tarczy Cisco**

Egzekwowanie polityk bezpieczeństwa za pomocą Cisco Hypershield odbywa się w trzech różnych warstwach: w oprogramowaniu, maszynach wirtualnych oraz w serwerach i urządzeniach sieciowych i obliczeniowych. Cisco Hypershield wykorzystuje te same potężne akceleratory sprzętowe, które są szeroko stosowane w systemach obliczeniowych wysokiej wydajności i hiperskalowych chmurach publicznych.

Hypershield zostało zbudowane na trzech filarach:

* **AI-Native: r**ozwiązanie od samego początku zaprojektowano i zbudowano tak, aby działało autonomicznie i predykcyjnie. Hypershield jest samozarządzalne i zapewnia hiper-rozproszone podejście do bezpieczeństwa na dużą skalę.
* **Cloud-Native:** Hypershield zostało zbudowane w oparciu o otwartą maszynę wirtualną eBPF, domyślny mechanizm łączenia i ochrony natywnych chmurowo przepływów pracy w chmurze hiperskalowej. Na początku kwietnia br. Cisco przejęło wiodącego dostawcę eBPF dla przedsiębiorstw, firmę Isovalent.
* **Hyper-rozproszoność:** Cisco całkowicie zmienia sposób działania tradycyjnych zabezpieczeń sieciowych, wbudowując zaawansowaną kontrolę bezpieczeństwa w serwery i samą strukturę sieci. Hypershield obejmuje wszystkie chmury i wykorzystuje akcelerację sprzętową, taką jak jednostki przetwarzania danych (DPU) do analizowania anomalii w zachowaniu aplikacji i sieci i reagowania na nie. Pozwala to przenieść bezpieczeństwo bliżej tych przepływów, które wymagają ochrony.

Cisco, dzięki wiodącej w branży wiedzy specjalistycznej w zakresie sieci i bezpieczeństwa oraz rozległemu ekosystemowi partnerów, wraz z firmą NVIDIA, jest zaangażowane w tworzenie i optymalizację rozwiązań bezpieczeństwa AI-native w celu ochrony i skalowania centrów danych przyszłości. Współpraca firm obejmuje wykorzystanie opartej na sztucznej inteligencji, natywnej platformy cyberbezpieczeństwa NVIDIA Morpheus do szybszego wykrywania anomalii sieciowych, a także platformy mikroserwisowej NVIDIA NIM na potrzeby tworzenia niestandardowych asystentów AI w obszarze bezpieczeństwa. Klasa konwergentnych akceleratorów NVIDIA łączy moc obliczeniową GPU i DPU zwiększając możliwości Cisco Hypershield o solidne zabezpieczenia od chmury po brzeg sieci.

– Przedsiębiorstwa ze wszystkich branż poszukują zabezpieczeń, które ochronią je przed stale rosnącą liczbą cyberzagrożeń – powiedział **Kevin Deierling, starszy wiceprezes ds. sieci w firmie NVIDIA**. – Cisco i NVIDIA wspólnie wykorzystują moc sztucznej inteligencji, aby zapewnić potężną, niezwykle bezpieczną infrastrukturę centrów danych, która umożliwi przedsiębiorstwom transformację i przyniesie korzyści klientom na całym świecie.

**Wyzwania bezpieczeństwa**

Jako rewolucyjna, nowa architektura bezpieczeństwa, Hypershield rozwiązuje trzy kluczowe wyzwania, z jakimi mierzą się klienci w kontekście obrony przed dzisiejszym wyrafinowanym krajobrazem zagrożeń:

* **Rozproszona ochrona przed exploitami:** atakujący są biegli w wykorzystywaniu nowo wykrywanych luk w zabezpieczeniach szybciej, niż obrońcy są w stanie je załatać. Według Cisco Talos Threat Intelligence każdego dnia pojawia się niemal 100 nowych podatności, co może prowadzić do katastrofalnych skutków. Hypershield zapewnia ochronę w przeciągu minut, automatycznie testując i wdrażając zabezpieczenia kompensacyjne w rozproszonej strukturze punktów egzekwowania polityk.
* **Autonomiczna segmentacja:** gdy atakujący znajdzie się w sieci, do powstrzymania jego bocznych ruchów w obrębie sieci kluczowa jest segmentacja. Hypershield nieustannie monitoruje, automatycznie uzasadnia i ponownie ocenia istniejące polityki w celu autonomicznej segmentacji sieci, rozwiązując problem w dużych i złożonych środowiskach.
* **Samokwalifikujące się aktualizacje:** Hypershield automatyzuje niezwykle żmudny i czasochłonny proces testowania i wdrażania aktualizacji wykorzystując podwójną płaszczyznę danych. Ta całkowicie nowa architektura oprogramowania umożliwia umieszczanie aktualizacji i zmian polityk w cyfrowym bliźniaku, który sprawdza je za pomocą unikatowej dla klienta kombinacji ruchu, polityk i funkcji, a następnie wdraża je bez przestojów.

Cisco Hypershield jest wbudowane w Security Cloud, ujednoliconą, opartą na sztucznej inteligencji, międzydomenową platformę bezpieczeństwa Cisco. Spodziewana data jego udostępnienia to sierpień 2024 roku. Dzięki niedawnemu przejęciu przez Cisco firmy Splunk klienci zyskają niezrównaną widoczność i wgląd w cały swój cyfrowy ślad w celu zapewnienia niespotykanej dotąd ochrony.

– Sztuczna inteligencja to nie tylko korzyści, ale także narzędzie wykorzystywane do niecnych celów, pozwalające hakerom na inżynierię wsteczną łatek i tworzenie exploitów w rekordowo krótkim czasie. Cisco stara się rozwiązać ten problem za pomocą rozwiązania opartego na sztucznej inteligencji, ponieważ Cisco Hypershield ma na celu przechylenie szali na korzyść obrońcy poprzez ochronę nowych podatności przed exploitami w ciągu kilku minut, a nie dni, tygodni, czy nawet miesięcy, w trakcie których czekamy na faktyczne wdrożenie łatek – powiedział **Frank Dickson, wiceprezes ds. produktów cyberbezpieczeństwa w IDC**. – Ponieważ liczba luk w zabezpieczeniach stale rośnie, a czas, w którym atakujący mogą je wykorzystać na dużą skalę ciągle się skraca, oczywiste jest, że samo łatanie nie wystarcza. Narzędzia takie jak Hypershield są niezbędne do walki z coraz sprytniejszymi cyberprzestępcami.

– Zadaniem Cisco Hypershield jest sprostanie złożonym wyzwaniom związanym z bezpieczeństwem nowoczesnych centrów danych w skali AI. Wizja Cisco dotycząca struktury samozarządzającej się i płynnie integrującej na poziomie od sieci do punktu końcowego pomoże na nowo zdefiniować możliwości w zakresie bezpieczeństwa na dużą skalę – powiedział **Zeus Kerravala, założyciel i główny analityk ZK Research**. – Na przykład dzięki unikatowemu, autonomicznemu i wysoce skutecznemu podejściu do segmentacji poziom widoczności i kontroli w hiper-rozproszonym środowisku zapobiega przemieszczaniu się atakujących w sieci. Choć może to brzmieć jak fantastyka, nadszedł na to właściwy czas, biorąc pod uwagę ostatnie postępy w dziedzinie sztucznej inteligencji w połączeniu z dojrzałością technologii natywnych dla chmury, takich jak eBPF.

Cisco chroni 100 proc. firm z listy Fortune 100. Dowiedz się więcej: [cisco.com/go/security](http://cisco.com/go/security).

**Dodatkowe zasoby**

* Blog: [Cisco Hypershield: Security reimagined — hyper-distributed security for the AI-scale data center](https://blogs.cisco.com/news/cisco-hypershield-security-reimagined-hyper-distributed-security-for-the-ai-scale-data-center)
* Blog: [Cisco Hypershield: A New Era of Distributed, AI-Native Security](https://blogs.cisco.com/security/cisco-hypershield-a-new-era-of-distributed-ai-native-security)
* Informacja prasowa: [Cisco and NVIDIA to Help Enterprises Quickly and Easily Deploy and Manage Secure AI Infrastructure](https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m02/cisco-nvidia-ai-collaboration.html)

**O Cisco**

Cisco (NASDAQ: CSCO) jest światowym liderem technologicznym, który bezpiecznie łączy wszystko ze światem. Naszym celem jest zapewnienie inkluzywnej przyszłości dla każdego i pomaganie naszym klientom w tworzeniu nowych aplikacji, umożliwianiu pracy hybrydowej, transformacji i zabezpieczaniu ich infrastruktury oraz osiąganiu celów zrównoważonego rozwoju. Dowiedz się więcej na polskim lub globalnym biurze prasowym.

Cisco i logo Cisco są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej podmiotów stowarzyszonych w Stanach Zjednoczonych i innych krajach. Listę znaków towarowych Cisco można znaleźć na stronie www.cisco.com/go/trademarks. Wymienione znaki towarowe innych firm są własnością ich odpowiednich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a jakąkolwiek inną firmą.