BlackBerry | Cybersecurity

CylanceGATEWAY

Rozwiązanie oparte na sztucznej inteligencji, w chmurze, realizujące założenia Zero Trust Network Access

ARKUSZ DANYCH

Solidne bezpieczeństwo sieci ma kluczowe znaczenie w erze, w której polityka pracy z domu i przynoszenia własnych urządzeń do pracy (BYOD) zyskuje szeroką akceptację. Ekspansja pracy zdalnej zatarła tradycyjne granice sieci, powodując znaczny wzrost obszaru powierzchni ataku w organizacji. Każde nowe urządzenie, każda nowa aplikacja i każdy nowy użytkownik łączący się z zasobami biznesowymi wprowadzają dodatkowe zagrożenia dla bezpieczeństwa. Gdy pracownicy zdalni podłączają do sieci firmowej szeroką gamę niezarządzanych urządzeń, ryzyko to szybko rośnie.

Ostatnie szacunki firmy Gartner wskazują, że 74% firm zamierza na stałe przenieść pracowników do bardziej zdalnego środowiska pracy po pandemii COVID-19.1 Ta transformacja siły roboczej oznacza, że więcej zasobów biznesowych będzie zarówno przenoszonych, jak i dostępnych spoza tradycyjnych granic sieci. Pracownicy zdalni będą coraz częściej próbowali uzyskać dostęp do związanych z pracą ofert oprogramowania jako usługi (SaaS) i danych organizacyjnych z różnych urządzeń, co stwarza zagrożenia dla bezpieczeństwa.access work-related software-as-a-service (SaaS) offerings and organizational data from various devices, creating security risks.

CylanceGATEWAY™ to rozwiązanie Zero Trust Network Access (ZTNA), które łagodzi dodatkowe luki w zabezpieczeniach powstałe w wyniku obsługi pracowników mobilnych i zdalnych. Próba wstępnej weryfikacji i ochrony wszystkich możliwych kombinacji technologii domowego biura przed dopuszczeniem ich do sieci firmowej nie jest już opłacalna. Wdrażając opartą na sztucznej inteligencji strukturę Zero Trust, CylanceGATEWAY wykorzystuje ciągłą autoryzację, aby zapewnić dostęp do zasobów biznesowych tylko bezpiecznym i zaufanym urządzeniom. Urządzenia lub aplikacje w domowym biurze mogą nie być bezpieczne, ale każde z nich w momencie łączenia się ze środowiskiem biznesowym musi udowodnić swoją wiarygodność, aby uzyskać dostęp.

MOŻLIWOŚCI CylanceGATEWAY

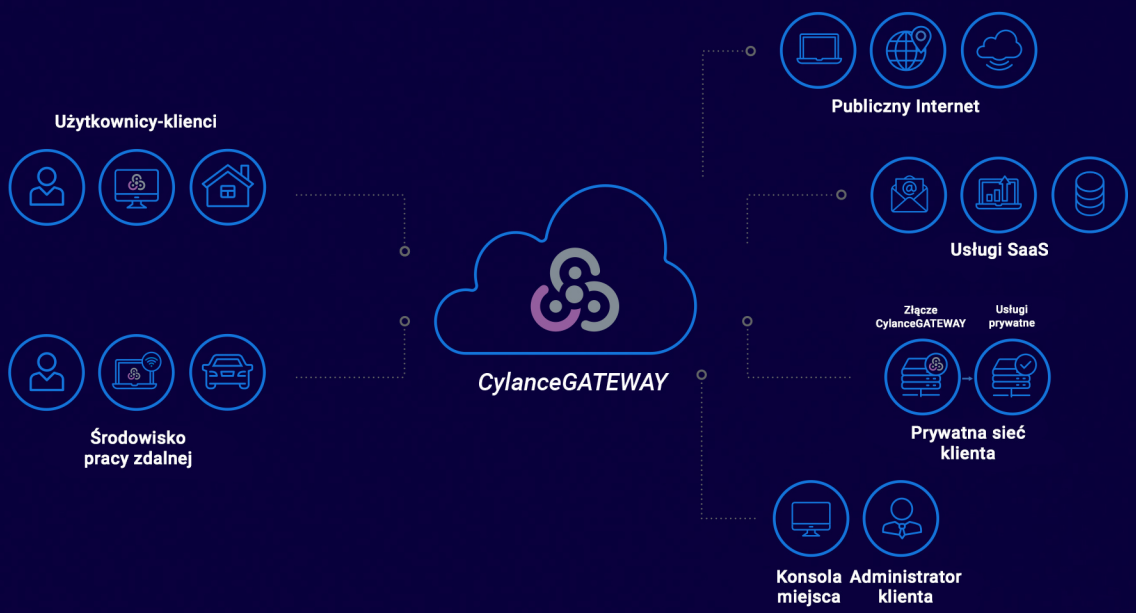
Rozwiązanie CylanceGATEWAY™ łączy kilka zaawansowanych technologii w celu zapewnienia bezpieczeństwa środowisk sieciowych. Jest ono zbudowane w oparciu o solidny stos TCP/IP, zoptymalizowany pod kątem urządzeń mobilnych i zdalnych oraz może wykrywać zagrożenia w zaszyfrowanych pakietach. Wykorzystuje sztuczną inteligencję do wykrywania podejrzanych zachowań i anomalii w całym środowisku, dostosowywania dostępu w czasie rzeczywistym oraz korelowania i kontekstualizowania informacji o zagrożeniach, często pomijanych przez starsze rozwiązania. CylanceGATEWAY chroni sieci, aplikacje i dane bez zakłócania wydajności użytkowników i bez poświęcania prywatności. Funkcje segmentacji ukrywają aplikacje, aby nie były publicznie widoczne, zmniejszając ryzyko ataków DDoS i zapobiegając ruchowi bocznemu. Określanie źródłowych adresów IP (Source IP Pinning) ogranicza łączność aplikacji SaaS tylko do zaufanych i znanych adresów IP, a możliwość korzystania z konfigurowalnych prywatnych adresów IP zapewnia elastyczność pozwalającą uniknąć błędów w routingu z innymi punktami końcowymi. CylanceGATEWAY umożliwia precyzyjne przyznawanie dostępu do zasobów lokalnych i chmurowych wyłącznie wybranym uwierzytelnionym użytkownikom.

OPARTY NA SZTUCZNEJ INTELIGENCJI, ADAPTACYJNY, BEZPIECZNY DOSTĘP

CylanceGATEWAY wykorzystuje sztuczną inteligencję w chmurze do ciągłej analizy szeregu czynników przy określaniu wiarygodności zdalnych uczestników i uprawnień dostępu. Uczestnicy to nie tylko użytkownicy, ale mogą to być również aplikacje lub boty szukające dostępu do środowiska. Podczas oceny dostępu sztuczna inteligencja w chmurze może dostosować poziomy zaufania w oparciu o następujące zmienne:

- Czy adres IP użytkownika jest zaufany?
- Czy uczestnik jest tym, za kogo się podaje?
- Czy uczestnik zachowuje się normalnie?

CylanceGATEWAY w skrócie
Dostęp do sieci wspomagany przez sztuczną inteligencję, realizujący założenia Zero Trust Network Acces



CLOUD AI

CylanceGATEWAY Cloud AI stale analizuje czynniki ryzyka sieciowego dla każdego podłączonego podmiotu i dynamicznie zmienia poziomy dostępu zgodnie z ich wiarygodnością.

- Czy uczestnik ma dostęp do oczekiwanych zasobów?
- Czy zachowanie użytkownika jest zgodne z jego wcześniejszą aktywnością lub innymi użytkownikami pełniącymi podobne role?

Gdy poziom zaufania użytkownika zmienia się, Cloud AI może na bieżąco informować o dynamicznej polityce, aby podejmować różne działania. W przypadku pozytywnych zmian w poziomie zaufania użytkownik może odziedziczyć zmodyfikowane lub ulepszone uprawnienia dostępu. Negatywne zmiany w poziomie zaufania mogą skutkować ograniczonym dostępem, żądaniem ponownego uwierzytelnienia lub uruchomieniem alertów bezpieczeństwa i procedur naprawczych.

USŁUGI SIECIOWE W TRYBIE FULL/SPLIT TUNNEL

CylanceGATEWAY™ zapewnia bezpieczny tunel komunikacyjny pomiędzy zdalnymi lub mobilnymi użytkownikami a środowiskiem biznesowym. Bezpieczny tunel działa w trybie pełnego lub dzielonego dostępu w zależności od potrzeb organizacji. Tryb pełnego dostępu zabezpiecza całą komunikację między użytkownikiem a siecią firmową. Tryb dzielonego dostępu pozwala administratorom wyznaczyć określone zasoby do bezpiecznej komunikacji, pozostawiając inny ruch otwarty. Podejście w trybie split tunnel jest przydatne do oddzielania aplikacji służbowych od osobistych, które są dostępne na tym samym własnym urządzeniu przyniesionym do pracy lub używanym podczas pracy z domu. CylanceGATEWAY można również skonfigurować w trybie tunelu dla poszczególnych aplikacji, aby dalej zarządzać dostępem do aplikacji.

OKREŚLANIE ŹRÓDŁOWYCH ADRESÓW IP

Niektóre usługi internetowe i aplikacje w chmurze odrzucają ruch sieciowy pochodzący z dowolnego miejsca innego niż adresy IP wyraźnie zarejestrowane przez organizację. Niektóre organizacje reagują na to ograniczenie po prostu omijając środki cyberbezpieczeństwa, które modyfikują lub ukrywają adresy IP. Wysyłają one ruch bezpośrednio do dostawców usług, co stwarza lukę w zabezpieczeniach.

Określanie źródłowych adresów IP (Source IP Pinning) pozwala organizacjom kontrolować adresy IP urządzeń komunikujących się z dostawcami usług bez pomijania środków bezpieczeństwa.

Organizacje mogą również używać opcji określania źródłowych adresów IP do ukrywania wewnętrznych zasobów przed zewnętrznymi agitatorami, którzy chcą przeniknąć do sieci i poruszać się po niej.

DOSTĘP DO APLIKACJI, A NIE DO SIECI

CylanceGATEWAY™ różni się od VPN sposobem, w jaki zapewnia dostęp do zasobów biznesowych. VPN uwierzytelnia się w sieci, oferując skutecznym atakującym szeroki dostęp do środowiska. CylanceGATEWAY zapewnia segmentowany dostęp do autoryzowanych aplikacji za pośrednictwem połączeń wychodzących połączonych ze sobą na krawędzi usługi, zapewniając, że użytkownicy nigdy nie są umieszczani w sieci. Segmentacja ta ukrywa aplikacje, aby nie były publicznie widoczne, zapobiega ruchowi bocznemu i drastycznie zmniejsza powierzchnię ataku. Zapewnia również administratorom sieci lepszy wgląd w aktywność użytkowników i ruch w sieci.

Możliwości ciągłego uwierzytelniania dostępne w rozwiązaniu CylanceGATEWAY odróżniają je również od sieci VPN, które przyjmują statyczne podejście do uwierzytelniania i autoryzacji. Gdy podmiot przejdzie wstępny proces weryfikacji, VPN deklaruje, że jest bezpieczny na czas trwania połączenia. CylanceGATEWAY stale uwierzytelnia każdego uczestnika sieci, eliminując nadmierne domniemane zaufanie. Analizuje wiele czynników, w tym zachowanie użytkownika, wiarygodność urządzenia oraz wzorce dostępu do sieci i aplikacji w trakcie zaangażowania. Gdy sztuczna inteligencja w chmurze wykryje anomalię, natychmiast podejmuje odpowiednie kroki w celu ochrony środowiska w oparciu o wagę wykrycia. CylanceGATEWAY może nawet wykrywać ataki tunelowania DNS, aby uniemożliwić przeciwnikom komunikację za pomocą protokołu DNS.

SOLIDNE ZABEZPIECZENIA TCP/IP

Rozwiązanie CylanceGATEWAY jest zbudowane na solidnym stosie TCP/IP z warstwą bezpieczeństwa IP, aby umożliwić bezpieczną łączność za pośrednictwem urządzeń z systemami Windows®, macOS®, iOS® i Android™.

Oferuje szeroką obsługę protokołów, w tym VoIP, architekturę w chmurze oraz tryby dostępu full/split tunnel. Organizacje polegające na CylanceGATEWAY mogą korzystać z identyfikacji aplikacji SaaS, aby zapobiec błędom w usługach takich jak O365. CylanceGATEWAY chroni przed niebezpiecznymi domenami i adresami za pomocą funkcji reputacji i klasyfikacji adresów IP i URL, uniemożliwiając użytkownikom celowy lub niezamierzony dostęp do nich.

WYKRYWANIE ZAGROŻEŃ SIECIOWYCH

CylanceGATEWAY wykrywa zagrożenia występujące w ruchu sieciowym, w tym w zaszyfrowanych pakietach, i kontekstualizuje informacje o zagrożeniach zidentyfikowane w całej sieci. Zdolność do analizowania i korelowania informacji w różnych środowiskach pozwala CylanceGATEWAY identyfikować złożone i wieloetapowe zagrożenia niewidoczne dla innych form analizy. Podejście CylanceGATEWAY charakteryzuje się wysoką wydajnością, nie wymagając odszyfrowywania/ponownego szyfrowania pakietów, a zatem jest mniej wymagające dla zasobów sieciowych. Wykrywając zagrożenia w zaszyfrowanych pakietach, CylanceGATEWAY chroni środowisko bez naruszania prywatności uczestników sieci.

TYPOWE PRZYPADKI UŻYCIA CylanceGATEWAY

Wykorzystując oparte na sztucznej inteligencji podejście Zero Trust do bezpieczeństwa sieci, CylanceGATEWAY rozwiązuje wiele rzeczywistych problemów, z którymi borykają się dziś organizacje. Przykładowe funkcje CylanceGATEWAY poprawiające środowisko biznesowe obejmują:

PRZYJĘCIE KONCEPCJI ZERO TRUST

Poprawa ogólnej odporności na ryzyko poprzez wdrożenie dynamicznego modelu dostępu do sieci o najmniejszych uprawnieniach i adaptacyjne mechanizmy kontroli oparte na tożsamości, które są kluczowymi elementami architektury Zero Trust.

BEZPIECZNY DOSTĘP DLA WSZYSTKICH UŻYTKOWNIKÓW

Zabezpieczenie hybrydowego modelu biznesowego i pracowników zdalnych dzięki elastycznemu dostępowi do krytycznych zasobów lokalnie lub w chmurze.

BEZPIECZEŃSTWO PUNKTÓW KOŃCOWYCH I SIECI

Zapewnienie ochrony wszystkich punktów końcowych i sieci dzięki zintegrowanym rozwiązaniom, które działają inteligentniej, a nie mocniej, zapewniając lepszą widoczność i lepsze zabezpieczenie przed obecnymi i przyszłymi cyberzagrożeniami.

USPRAWNIONA WSPÓŁPRACA

Zapewnienie szybszego i bezpieczniejszego dostępu osobom innym niż etatowi pracownicy. Kontrahenci, dostawcy i partnerzy strategiczni mogą bezpiecznie uzyskiwać dostęp do zasobów w celu promowania wydajności zarówno na urządzeniach zarządzanych, jak i niezarządzanych.

WYMIANA VPN

Poprawa szybkości i agilności w związku ze zdarzeniami transformacyjnymi bez konieczności integracji sieci w celu zwiększenia wydajności. Zapewnienie w łatwy sposób bardziej ujednoliconego, stabilnego i bezpiecznego środowiska.

FUZJE, PRZEJĘCIA I ZBYCIA

Poprawa szybkości i agilności w związku ze zdarzeniami transformacyjnymi bez konieczności integracji sieci w celu zwiększenia wydajności. Zapewnienie w łatwy sposób bardziej ujednoliconego, stabilnego i bezpiecznego środowiska.

WIDOCZNOŚĆ W CZASIE RZECZYWISTYM

Administratorzy sieci i personel ds. bezpieczeństwa mogą uzyskać dostęp do szczegółowych informacji o aktywności użytkowników i korzystać z wykrywania aplikacji w celu podejmowania świadomych decyzji dotyczących ryzyka w sieci.

GRANULARNE ZARZĄDZANIE ZASADAMI

Przejęcie kontroli nad swoimi sieciami i aplikacjami dzięki bezpiecznemu tylko wychodzącemu dostępowi i adaptacyjnemu zarządzaniu polityką najmniejszych uprawnień, egzekwowanemu przez silnik ryzyka sztucznej inteligencji w chmurze.

DLACZEGO WARTO WYBRAĆ CylanceGATEWAY

Adaptacja i konfiguracja
Konfiguracja jednym kliknięciem dla wielu najpopularniejszych aplikacji SaaS usprawnia pracę administratorów sieci. Szybkie wdrożenie poprawia doświadczenia użytkowników końcowych.

Redukcja ryzyka w sieci
Zapobieganie dostępowi nieautoryzowanych użytkowników do sieci dzięki technologii określania źródłowych adresów IP (Source IP Pinning). Korzystanie z konfigurowalnych prywatnych adresów IP zapewnia elastyczność pozwalającą uniknąć błędów w routingu z innymi punktami końcowymi.

Widoczność sieci i aktywności
Szybki dostęp do szczegółowych informacji dzięki przyjaznemu dla użytkownika pulpitowi nawigacyjnemu i wglądowi w czasie rzeczywistym w ruch sieciowy, zdarzenia związane z naruszeniem bezpieczeństwa i wskaźniki naruszenia bezpieczeństwa. Wyświetlanie statusów, historii dostępu i najpopularniejszych miejsc docelowych.

Łączność z dowolnym miejscem i urządzeniem
Umożliwienie rozproszonym pracownikom pracę z domu lub z dowolnego miejsca na zarządzanych i niezarządzanych urządzeniach. Dostępne dla systemów macOS, Windows, iPhone i Android.

DOWIEDZ SIĘ WIĘCEJ

CylanceGATEWAY™ to tylko jedno z opartych na sztucznej inteligencji, prewencyjnych, światowej klasy rozwiązań bezpieczeństwa oferowanych przez BlackBerry. Dowiedz się więcej o naszej pełnej ofercie pakietów bezpieczeństwa zaprojektowanych, aby pomóc Twojej organizacji przygotować się na cyberataki, zapobiegać im, wykrywać je i reagować na nie.

Poznaj:

---

[1] https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

Szybka i niezawodna wydajność

Wykorzystanie akceleratora brzegowego do optymalizacji ścieżek sieciowych, co poprawia wydajność i szybkość. Solidna i odporna technologia tunelowa zapewnia wysoką jakość połączeń dla dowolnej aplikacji i VoIP.

Zintegrowane wykrywanie zagrożeń

CylanceGATEWAY przeprowadza wspomagane przez sztuczną inteligencję wykrywanie zagrożeń sieciowych poprzez analizę telemetrii sieci bez odszyfrowywania. Natywna integracja CylanceGATEWAY z BlackBerry Spark® Unified Endpoint Security Suite zapewnia, że tylko urządzenia w dobrym stanie otrzymują dostęp do sieci.

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) zapewnia przedsiębiorstwom i rządom na całym świecie inteligentne oprogramowanie i usługi w zakresie bezpieczeństwa. Firma zabezpiecza ponad 500 milionów punktów końcowych, w tym ponad 195 milionów pojazdów. Firma z siedzibą w Waterloo, Ontario wykorzystuje uczenie SI i maszynowe do dostarczania innowacyjnych rozwiązań w dziedzinach cyberbezpieczeństwa, bezpieczeństwa i ochrony danych oraz jest liderem w dziedzinie bezpieczeństwa punktów końcowych, zarządzania punktami końcowymi, szyfrowania i systemów wbudowanych. Wizja BlackBerry jest jasna — zapewnić skomunikowaną przyszłość, której można ufać.

BlackBerry. Intelligent Security. Everywhere.

Aby uzyskać więcej informacji, odwiedź witrynę BlackBerry.com i obserwuj @BlackBerry.

BB23 | 220627