BlackBerry
Intelligent Security. Everywhere.

bakotech

BlackBerry Persona

Nieprzerwane uwierzytelnianie i analiza zachowań oparte na sztucznej inteligencji

Organizacje, które chcą stosować podejście Zero Trust w swojej polityce cyberbezpieczeństwa uważają, że BlackBerry Persona dla urządzeń stacjonarnych jest elementem fundamentalnym.

Persona w wersji desktopowej | Przegląd

BlackBerry® Persona to oparte na sztucznej inteligencji rozwiązanie do ciągłego uwierzytelniania i analizy zachowań, zaprojektowane w celu identyfikacji podejrzanych użytkowników w czasie rzeczywistym, aby zapobiec naruszeniom bezpieczeństwa. Kluczowe funkcje:

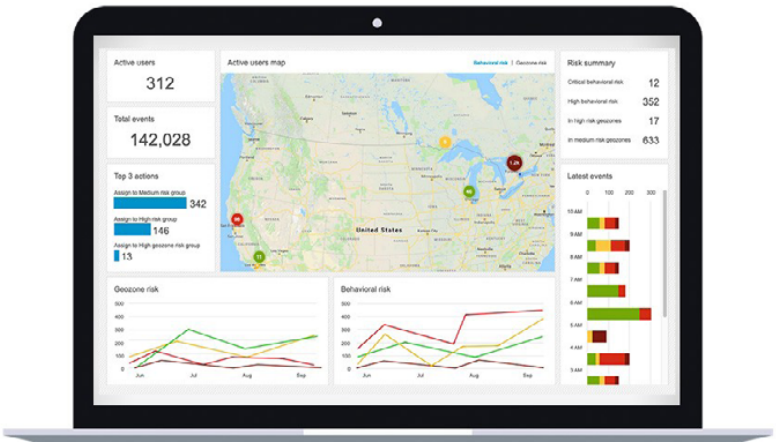
- Ochrona przed niewłaściwym wykorzystaniem skradzionych danych uwierzytelniających przy użyciu silników analizy zachowań i analizy postępowania.
- Ochrona przed zagrożeniami pochodzącymi od osób niepowołanych za pomocą silników analizy złośliwych zachowań.
- Proaktywne działania na urządzeniu końcowym, takie jak weryfikacja 2FA, ograniczanie dostępu do sieci, zawieszanie kont użytkowników.
- Cała analiza użytkownika i ocena punktowa może odbywać się w czasie rzeczywistym na urządzeniu końcowym, co znacznie zmniejsza ilość danych, które muszą być przesyłane i przechowywane w chmurze.
- Integracja z dostawcami zewnętrznymi, takimi jak Ping i OKTA, w celu zapewnienia ciągłego uwierzytelniania dla aplikacji internetowych.

BlackBerry. Persona

Organizacje dążące do stosowania podejścia Zero Trust w swojej polityce cyberbezpieczeństwa uznają BlackBerry Persona za element fundamentalny. Tak jak w przypadku BlackBerry Persona dla urządzeń mobilnych, BlackBerry Persona dla komputerów stacjonarnych wykorzystuje analizę zachowań i modele ML w celu stworzenia wyniku zaufania użytkownika w czasie rzeczywistym. Informacje te będą wykorzystywane do uruchamiania automatycznych działań, umożliwiając powstrzymanie ataków dotyczących danych uwierzytelniających w ciągu kilku minut. Po wdrożeniu, BlackBerry Persona natychmiast rozwiązuje problemy związane z bezpieczeństwem w przedsiębiorstwie:

- **Skradzione Dane Uwierzytelniające —** BlackBerry Persona chroni organizację przed szkodami wyrządzonymi w przypadku naruszenia danych uwierzytelniających pracowników. BlackBerry Persona weryfikuje interakcje użytkownika z jego urządzeniem w czasie rzeczywistym za pomocą analizy zachowań i modeli postępowania, po czym określa ryzyko dla użytkownika. Jeśli przekroczony zostanie próg ryzyka, do chmury wysyłane są alerty i podejmowane są automatyczne działania łagodzące, takie jak monit o zastosowanie metody uwierzytelniania drugiego czynnika.
- **Zagrożenia Wewnętrzne —** BlackBerry Persona chroni organizację przed szkodami wyrządzonymi przez nieuczciwych pracowników poprzez ciągłą analizę ich postępowania. Jeśli zachowanie pracownika odbiega od jego standardowych zachowań, BlackBerry Persona zidentyfikuje to zachowanie jako anomalne. W oparciu o zdefiniowaną przez administratora politykę zostaną podjęte ostrzeżenia i działania proaktywne.
- **Naruszenia Fizyczne —** BlackBerry Persona chroni pracowników i organizacje przed atakami, w których urządzenie zostało fizycznie naruszone i/lub skradzione. Jeśli nieuprawnieni użytkownicy uzyskają dostęp do punktu końcowego, modele analizy zachowania mogą wykryć nowego użytkownika i wysłać alerty lub zablokować urządzenie. Działania te są wykonywane automatycznie i nie wymagają połączenia z siecią ani interakcji z chmurą.

"...BlackBerry Persona dla komputerów stacjonarnych wykorzystuje analizę zachowań i modele ML oparte na zachowaniach, aby stworzyć wynik zaufania użytkownika do urządzenia w czasie rzeczywistym."



Jak to działa?

Możliwości BlackBerry Persona w zakresie uczenia maszynowego umożliwiają identyfikację wzorców zachowań i lokalizacji wielu użytkowników w celu określenia ryzyka. Jeśli system zidentyfikuje powtarzające się wzorce dużych skupisk pracowników w tej samej lokalizacji, może automatycznie określić ją jako miejsce pracy lub, jeśli firma tak postanowi, może wstępnie załadować znane lokalizacje.

BlackBerry Persona wykorzystuje analizę zachowań do rozpoznawania typowych wzorców użytkowania oprogramowania. Obejmują one porę dnia i sposób, w jaki użytkownik korzysta z oprogramowania, przekierowania wewnętrzne i zewnętrzne itp. BlackBerry Persona wykorzystuje szereg innych czynników, aby zdecydować, jaki poziom dostępu powinien zostać przyznany profilowi pracownika lub wykonawcy w danym momencie, takich jak:

- **Analiza Behawioralna:** BlackBerry Persona ocenia charakterystykę danych wejściowych użytkownika w celu określenia standardu analizy behawioralnej, na podstawie którego ustalana jest autentyczność danych uwierzytelniających.
- **Lokalizacja Behawioralna:** BlackBerry Persona analizuje częstotliwość i wzorce użytkowników na podstawie analizy predykcyjnej anonimowych danych o lokalizacji w celu określenia poziomu ryzyka.
- **Zaufanie Do Sieci:** BlackBerry Persona określa częstotliwość korzystania z sieci i dynamicznie dostosowuje zabezpieczenia w oparciu o ten profil. Uzyskanie dostępu do publicznej sieci Wi-Fi po raz pierwszy odpowiednio dostosowuje wynik ryzyka.
- **Anomalie w Użytkowaniu*:** BlackBerry Persona ocenia użycie aplikacji i odróżnia użycie dopuszczalne od anomalnego w celu określenia zaufania do danych uwierzytelniających użytkownika.

Analiza wyników ryzyka: Dynamiczne dostosowywanie wymagań bezpieczeństwa

BlackBerry Persona posiada unikalną możliwość przyznawania dostępu i wydawania wyzwań uwierzytelniających w oparciu o analizę ryzyka w czasie rzeczywistym, zwiększając tym samym komfort i produktywność użytkowników końcowych bez uszczerbku dla zasad bezpieczeństwa. W oparciu o analizę ryzyka w czasie rzeczywistym, BlackBerry Persona może:

- udzielać dostępu
- przyjmować polityki bezpieczeństwa
- wydawać polecenia uwierzytelniania
- ostrzegać i usuwać nieprawidłowości

BlackBerry Persona dynamicznie dostosowuje postawę bezpieczeństwa i polityk i w razie potrzeby stosuje środki zaradcze. Pozwala to na wzajemną i dynamiczną optymalizację doświadczeń użytkownika i bezpieczeństwa/polityki.

*Funkcje oczekujące

Dzięki ciągłemu uwierzytelnianiu, BlackBerry Persona wykorzystuje analizę zachowań w celu rozpoznania typowych wzorców użytkowania oprogramowania desktopowego, aby w czasie rzeczywistym określić, które zachowania stanowią wysokie lub niskie ryzyko."

Zalety BlackBerryPersona

W przeciwieństwie do tradycyjnych rozwiązań, które muszą najpierw przesłać wszystkie dane z punktu końcowego do chmury w celu ich przetworzenia, BlackBerry Persona wykorzystuje i przetwarza niezaszyfrowane, czyste dane z urządzenia końcowego. Dodatkowo, dane i logika BlackBerry Persona znajdują się w punkcie końcowym, co pozwala na szybsze wykrywanie i kompleksowy zestaw proaktywnych działań zaradczych.

Szybkie Wykrywanie

Znacząca ilość informacji może zostać przejęta w ciągu kilku dni od ataku. BlackBerry Persona zapewnia ochronę szybko reagując na naruszenie poprzez ograniczenie niewłaściwego wykorzystania danych uwierzytelniających.

Większa Dokładność

BlackBerry Persona to unikalne rozwiązanie, ponieważ zawiera scoring oparty na zachowaniu użytkownika lokalnie w punkcie końcowym, bez przesyłania danych do chmury.

Redukcja Kosztów

Ze względu na obecność BlackBerry Persona na punkcie końcowym, wszystkie analizy i oceny użytkowników mogą odbywać się w czasie rzeczywistym, co zmniejsza ilość danych, które muszą być przesyłane i przechowywane w chmurze.

Większa Kontrola

Oprócz alertów generowanych w konsoli administracyjnej, BlackBerry Persona proaktywnie podejmuje działania w punkcie końcowym, takie jak prezentowanie wyzwań 2FA, ograniczanie dostępu do sieci, zawieszanie kont użytkowników i inne.

SKONTAKTUJ SIĘ Z NAMI:

www.bakotech.pl

blackberry@bakotech.pl

+48 12 340 90 30

bako tech®