BlackBerry | Cyberbezpieczeństwo

CylancePROTECT

Przyszłościowe zabezpieczenia punktów końcowych

ARKUSZ DANYCH

Przez lata podstawowa ochrona przed zagrożeniami w produktach zabezpieczających punkty końcowe opierała się na sygnaturach, tworzonych po tym, jak pacjenci zero odczuli wpływ zagrożeń i doszło do nieodwracalnych szkód. Zakładając, że wszystkie ataki były już znane, używanie sygnatur miało sens. Obecnie złośliwe oprogramowanie mutuje codziennie, a nawet co godzinę, co sprawia, że narzędzia zapobiegawcze oparte na sygnaturach stają się przestarzałe i stwarzają potrzebę solidniejszego podejścia do bezpieczeństwa punktów końcowych opartego na zapobieganiu.

W BlackBerry na nowo zdefiniowano to, co rozwiązanie do ochrony punktów końcowych może i powinno robić dla organizacji, wykorzystując zautomatyzowane podejście oparte na zapobieganiu. Jest to dokładne, wydajne i skuteczne rozwiązanie do zapobiegania wystąpieniu zaawansowanych trwałych zagrożeń i wykonaniu złośliwego oprogramowania na punktach końcowych organizacji. CylancePROTECT® zapobiega naruszeniom i zapewnia dodatkową kontrolę bezpieczeństwa w celu ochrony przed atakami opartymi na skryptach, bezplikowymi, na pamięć i opartymi na urządzeniach zewnętrznych. CylancePROTECT działa bez interwencji użytkownika lub administratora, połączenia z chmurą, sygnatur, heurystyki czy sandboxów.

Możliwości

Egzekwowanie zasad korzystania z urządzeń

- Kontrola korzystania z urządzeń pamięci masowej USB
- Zapobieganie kradzieży danych z nośników wymiennych

Kontrola dostępu oparta na rolach (RBAC)

- Minimalizacja ryzyka dzięki bardziej szczegółowemu zarządzaniu rolami z niestandardową kontrolą RBAC
- Lepsze ograniczenia dostępu do sieci w oparciu o role poszczególnych użytkowników
- Ograniczenie praw dostępu pracowników tylko do tych informacji, których potrzebują do wykonywania swojej pracy
- Brak wpływu na istniejących użytkowników

Kontrola aplikacji

- Blokowanie urządzeń o stałej funkcji
- Zapobieganie złym plikom binarnym lub modyfikacjom plików binarnych
- Blokowanie określonych systemów i ograniczenie wszelkich zmian

CylancePROTECT DLA URZĄDZEŃ STACJONARNYCH

Model algorytmiczny wykorzystywany w CylancePROTECT oznacza, że nie ma sygnatur, łatania, skanowania systemu ani powolnych punktów końcowych z powodu działającego na nich rozwiązania w zakresie bezpieczeństwa. Klienci, którzy przeszli z reaktywnych, starszych produktów antywirusowych opartych na sygnaturach, odnotowali nawet 99% zwrot z inwestycji, 97% redukcję ponownego obrazowania maszyn, zwiększoną wydajność sprzętu i baterii oraz 90% redukcję godzin pracy personelu wymaganych do zarządzania rozwiązaniem.[1]

Architektura CylancePROTECT składa się z lekkiego jednego agenta, który jest zarządzany za pośrednictwem konsoli w chmurze opartej na usłudze BlackBerry® SaaS. Konsola w chmurze łatwo integruje się z istniejącymi systemami zarządzania oprogramowaniem i narzędziami bezpieczeństwa. Opcje zarządzania hybrydowego i lokalnego są dostępne dla środowisk z mechanizmami Air-Gap. Agent punktu końcowego wykrywa złośliwe oprogramowanie i zapobiega mu na hoście, niezależnie

od połączenia z chmurą i bez potrzeby ciągłych aktualizacji. CylancePROTECT jest w stanie wykrywać i poddawać kwarantannie złośliwe oprogramowanie w otwartych, izolowanych i wirtualnych sieciach. Podejście oparte na uczeniu maszynowym BlackBerry zatrzymuje wykonywanie szkodliwego kodu niezależnie od posiadania wcześniejszej wiedzy lub stosowania nieznanej techniki maskowania. Żaden inny produkt antywirusowy nie może się równać z dokładnością, łatwością zarządzania i skutecznością CylancePROTECT.

Architektura CylancePROTECT składa się z lekkiego jednego agenta, który jest zarządzany za pośrednictwem konsoli w chmurze opartej na usłudze BlackBerry SaaS.

Możliwości

Ochrona pamięci

- Proaktywna identyfikacja i zatrzymywanie złośliwego wykorzystania pamięci
- Zapobieganie atakom tylko na pamięć, takim jak eskalacja uprawnień
- Korzystanie ze szczegółowego wykluczenia oraz ulepszonego rozwiązywania problemów i raportowania

Kontrola skryptów

- Zatrzymanie uruchamiania nieautoryzowanych skryptów
- Korzystanie ze szczegółowych funkcji białej listy i listy bezpiecznych adresów IP
- Obsługa systemów MacOS®, Microsoft® i Linux®
- Zapobieganie wykonywaniu jednowyrazowych poleceń programu PowerShell

Wykrywanie aplikacji spoza App Store w systemie iOS®

- Aplikacje spoza App Store są natychmiast skanowane i wykrywane

CECHY CylancePROTECT

Prawdziwa prewencja ataków zero-day

Odporny model sztucznej inteligencji zapobiega wykonywaniu ataków zero-day.

Egzekwowanie zasad korzystania z urządzeń

Kontrolowanie, które urządzenia mogą być używane w środowisku, eliminując urządzenia zewnętrzne jako potencjalny wektor ataku.

Zapobieganie złośliwemu oprogramowaniu oparte na sztucznej inteligencji

Sprawdzona w praktyce sztuczna inteligencja sprawdza każdą aplikację, która próbuje uruchomić się na punkcie końcowym przed jej wykonaniem

Wykrywanie i zapobieganie wykorzystywaniu pamięci

Proaktywne identyfikowanie złośliwego wykorzystania pamięci (ataki bezplikowe) z natychmiastowym automatycznym reagowaniem prewencyjnym.

Zarządzanie skryptami

Zachowanie pełnej kontroli nad tym, kiedy i gdzie skrypty są uruchamiane w środowisku.

Kontrola aplikacji dla urządzeń o stałej funkcji

Zapewnianie, że urządzenia o stałej funkcji są stale w nieskazitelnym stanie, eliminując dryf, który występuje w przypadku urządzeń niezarządzanych.

Możliwości

- Skanowanie złośliwego oprogramowania w systemie Android™

Skanowanie złośliwego oprogramowania w systemie Android i plikach APK w sklepie z aplikacjami UEM.

- Skanowanie wszystkich aplikacji w sklepie z aplikacjami BlackBerry® UEM, w tym aplikacji klientów i niestandardowych aplikacji partnerów, chroniąc przed złośliwym oprogramowaniem

Wykrywanie phishingu i złośliwych adresów URL

- Wykorzystywanie sztucznej inteligencji do automatycznego wykrywania i zatrzymywania złośliwych adresów URL, w tym tych z osadzonymi elementami phishingowymi

Bezpieczne tworzenie aplikacji

- Umożliwia partnerom i firmom tworzenie niestandardowych, bezpiecznych aplikacji na urządzenia dostępne dla przedsiębiorstw

Sprawdzanie integralności aplikacji IOS® dla aplikacji BlackBerry Dynamics SDK

- Zapewnianie integralności aplikacji zbudowanych na platformie BlackBerry® Dynamics™ SDK
- Umożliwianie zapisywania na urządzeniach tylko bezpiecznych aplikacji i zapobieganie wszelkim manipulacjom przy aplikacjach BlackBerry

CylancePROTECT MOBILE

Obecnie, bardziej niż kiedykolwiek, organizacje korzystają z urządzeń mobilnych, aby konkurować na elastycznym, ewoluującym rynku i mieć stały kontakt ze swoimi pracownikami. Po raz pierwszy ponad połowa wszystkich urządzeń podłączonych do Internetu to urządzenia mobilne2. Jednocześnie złośliwe oprogramowanie mobilne jest bardziej rozpowszechnione niż kiedykolwiek wcześniej, a liczba ataków wzrosła o 50% tylko w ciągu ostatniego roku[3]. Podczas gdy rozwiązania związane z bezpieczeństwem dla przedsiębiorstw historycznie koncentrowały się na urządzeniach stacjonarnych, coraz więcej firm odkrywa rosnące zagrożenie atakami phishingowymi złośliwego oprogramowania skierowanymi na urządzenia mobilne, zwłaszcza w aplikacjach.

Szkody spowodowane tymi atakami mogą być znaczące, a informacje umożliwiające identyfikację osób (PII) i inne krytyczne dane wyciekają z większą częstotliwością niż kiedykolwiek wcześniej.

Prowadzi to do tego, że coraz więcej organizacji stosuje technikę głębokiej inspekcji pakietów (DPI) i inne funkcje ochrony przed złośliwymi atakami.

Nic więc dziwnego, że rynek obrony przed zagrożeniami mobilnymi (MTD) szybko rośnie. MTD oferuje dodatkową warstwę bezpieczeństwa, zapobiegając, wykrywając, naprawiając i poprawiając ogólną higienę bezpieczeństwa na wszystkich poziomach floty mobilnej i aplikacji organizacji.

Rozwiązanie BlackBerry MTD, CylancePROTECT® MOBILE, rozszerza bazę zabezpieczeń zapewnianych przez BlackBerry UEM poprzez przeciwdziałanie zaawansowanym złośliwym zagrożeniom na urządzeniach mobilnych. CylancePROTECT MOBILE monitoruje ataki na poziomie urządzeń i aplikacji i wykracza poza bezpieczeństwo podstawowych kontenerów aplikacji.

- Na poziomie urządzeń CylancePROTECT MOBILE identyfikuje luki w zabezpieczeniach i potencjalne złośliwe działania poprzez monitorowanie aktualizacji systemu operacyjnego, parametrów systemu, konfiguracji urządzeń i bibliotek systemowych.
- Na poziomie aplikacji urządzenia CylancePROTECT MOBILE wykorzystują sandboxing aplikacji i analizę kodu, a także testy bezpieczeństwa aplikacji w celu identyfikacji złośliwego oprogramowania i potencjalnie niechcianego oprogramowania.

Ponadto urządzenia CylancePROTECT MOBILE identyfikują wszelkie złośliwe oprogramowanie, które może zostać wprowadzone za pośrednictwem aplikacji spoza App Store, unikalnego złośliwego oprogramowania opartego na sygnaturach lub symulacji, dodając dodatkową warstwę zabezpieczeń do platformy BlackBerry Dynamics SDK. Umożliwia to partnerom i firmom tworzenie niestandardowych, bezpiecznych aplikacji, które można załadować na urządzenia, do których dostęp mają przedsiębiorstwa.

TYPOWE PRZYPADKI UŻYCIA CylancePROTECT

CylancePROTECT zapewnia zapobieganie zagrożeniom w pełnym spektrum, które powstrzymuje naruszenia punktów końcowych, rozwiązując następujące przypadki użycia:

- Identyfikacja i blokowanie złośliwych plików wykonywalnych bez konieczności ciągłych aktualizacji lub połączenia z chmurą
- Identyfikacja luk w zabezpieczeniach i potencjalnych złośliwych działań poprzez monitorowanie aktualizacji systemu operacyjnego, parametrów systemowych, konfiguracji urządzeń i bibliotek systemowych
- Kontrola nad tym, gdzie, jak i kto może wykonywać skrypty
- Zarządzanie wykorzystaniem urządzeń USB i zapobieganie używaniu nieautoryzowanych urządzeń
- Powstrzymywanie ataków złośliwego oprogramowania bez plików
- Blokowanie urządzeń o stałej funkcjonalności, takich jak kioski, terminale POS itp.
- Zapobieganie atakom zero-day i ransomware
- Powstrzymywanie ataków na pamięci i przypadków wykorzystania pamięci
- Korzystanie z sandboxingu aplikacji i analizy kodu, a także testów bezpieczeństwa aplikacji w celu identyfikacji złośliwego oprogramowania i potencjalnie niechcianego oprogramowania
- Identyfikowanie wszelkiego złośliwego oprogramowania, które może przedostać się przez aplikacje spoza App store, unikalne złośliwe oprogramowanie oparte na sygnaturach lub symulacje
- Ochrona punktów końcowych, gdy użytkownicy są online lub offline

DOWIEDZ SIĘ WIĘCEJ

CylancePROTECT to tylko jedno z szerokiej gamy światowej klasy rozwiązań związanych z bezpieczeństwem oferowanych przez BlackBerry. Dowiedz się więcej o naszej pełnej ofercie pakietów zabezpieczeń, które mogą zapewnić Twojej organizacji inteligentną ochronę w każdym miejscu.

Odkryj nasze produkty:

BlackBerry Spark® Suite

BlackBerry Spark®
Unified Endpoint Security Suite

BlackBerry Spark®
Unified Endpoint Management Suite

1 https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html#form-anchor
2 https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet
3 https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

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.

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

BB23 | 220412