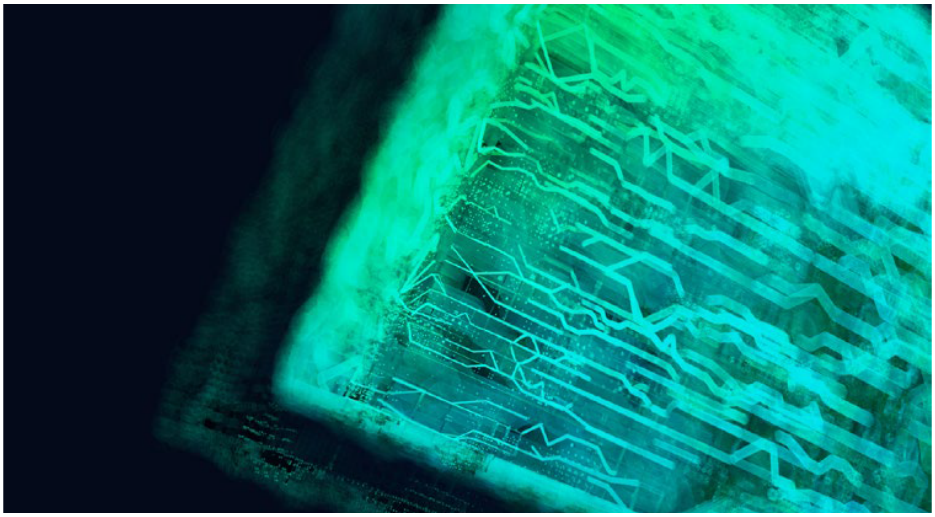
# BlackBerry Protect

## Przyszłościowe rozwiązanie do ochrony stacji końcowych



Przez wiele lat podstawowa ochrona antywirusowa opierała się na sygnaturach tworzonych po tym, jak stacja robocza została już zainfekowana, a szkody wyrządzone. Używanie sygnatur miało sens zakładając, że przyszłe ataki będą identyczne, jak te już dokonane. Obecnie złośliwe oprogramowanie zmienia się codziennie, a nawet co godzinę - narzędzia oparte na sygnaturach stają się więc niewydajne i stwarzają potrzebę bardziej zdecydowanego, opartego na prewencji podejścia do bezpieczeństwa punktów końcowych.

Wykorzystując zautomatyzowane podejście oparte na zapobieganiu, BlackBerry określiło na nowo, co rozwiązanie do ochrony endpointów może i powinno robić dla organizacji. BlackBerry Protect jest wydajnym i skutecznym rozwiązaniem do zapobiegania zaawansowanym zagrożeniom i złośliwym oprogramowaniom na punktach końcowych organizacji. Agent Protect zapobiega naruszeniom i zapewnia dodatkową kontrolę bezpieczeństwa w celu ochrony przed atakami opartymi na skryptach, pamięci, urządzeniach zewnętrznych i przed atakami bezplikowymi. BlackBerry Protect chroni endpointy bez udziału użytkownika czy administratora, bez konieczności korzystania z chmury, sygnatur, heurystyki czy sandboxa.

## WŁAŚCIWOŚCI

### Egzekwowanie polityk korzystania z urządzeń

- Kontrola urządzeń zewnętrznych.
- Zapobieganie kradzieży danych za pośrednictwem nośników wymiennych.

### Kontrola dostępu oparta na rolach (RBAC)

- Minimalizacja ryzyka dzięki szczegółowemu zarządzaniu rolami za pomocą RBAC.
- Zwiększenie ograniczeń dostępu do sieci w oparciu o role poszczególnych użytkowników.
- Ograniczenie praw dostępu pracowników tylko do informacji, które są im potrzebne do wykonywania pracy.

### Kontrola aplikacji

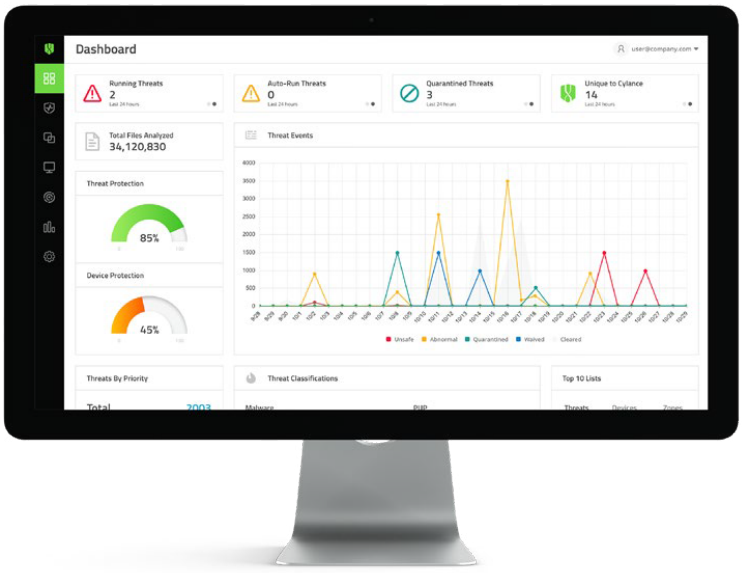
- Blokowanie urządzeń o stałych funkcjach.
- Zapobieganie złym plikom binarnym lub modyfikacjom takich plików.
- Blokowanie określonych systemów i ograniczanie zmian.

## BlackBerry Protect dla urządzeń stacjonarnych

Model matematyczny zastosowany w BlackBerry Protect oznacza brak sygnatur, brak poprawek, brak skanowania systemu lub spowolnienia endpointa z powodu działającego na nim rozwiązania antywirusowego. Klienci, którzy zmienili rozwiązanie antywirusowe z rozwiązania opartego na sygnaturach na BlackBerry Protect, odnotowali 99% zwrot z inwestycji, przy redukcji kosztów sięgającej aż 97% oraz 90% redukcję liczby godzin pracy personelu IT do zarządzania systemami bezpieczeństwa na stacji końcowej[1].

Architektura BlackBerry Protect składa się z lekkiego pojedynczego agenta, który jest zarządzany za pomocą chmurowej konsoli BlackBerry opartej na modelu SaaS. Konsola w chmurze łatwo integruje się z istniejącymi systemami zarządzania oprogramowaniem i narzędziami bezpieczeństwa. Hybrydowe opcje zarządzania oraz on-premise są również dostępne.

Agent instalowany na stacji końcowej będzie wykrywał i przeciwdziałał złośliwemu oprogramowaniu bezpośrednio na urządzeniu, niezależnie od połączenia z chmurą i bez potrzeby ciągłych aktualizacji, jak ma to miejsce w systemach sygnaturowych. BlackBerry Protect jest w stanie wykryć i poddać kwarantannie złośliwe oprogramowanie w sieci otwartej, izolowanej czy wirtualnej. Podejście BlackBerry oparte na uczeniu maszynowym zatrzymuje uruchamianie szkodliwego kodu. Żaden inny produkt antywirusowy nie może równać się dokładności, łatwości zarządzania i skuteczności BlackBerry Protect.




**Architektura BlackBerry Protect składa się z lekkiego pojedynczego agenta, który jest zarządzany przez własną, chmurową, opartą na SaaS konsolę BlackBerry.**

## WŁAŚCIWOŚCI

### Ochrona pamięci

• Proaktywne wykrywanie i powstrzymywanie szkodliwego wykorzystania pamięci.

• Zapobieganie atakom opartym wyłącznie na pamięci, takim jak eskalacja uprawnień.

### Kontrola skryptów

• Powstrzymywanie uruchomienia nieautoryzowanych skryptów.

• Możliwość korzystania z szczegółowych funkcji białej i bezpiecznej listy.

• Obsługa systemów MacOS®, Microsoft® i Linux®.

• Zapobieganie wykorzystania skryptów PowerShell.

### Wykrywanie zainstalowanych aplikacji IOS®

• Zainstalowane aplikacje spoza App Store są natychmiast skanowane i wykrywane.

## Cechy BlackBerry Protect

| Ochrona przed atakami zero-day | Ochrona oparta na AI | Zarządzanie skryptami |
|---|---|---|
| Model matematyczny zastosowany w BlackBerry zapobiega wykonaniu szkodliwego kodu. | Sprawdzony model AI analizuje każdą aplikację próbującą uruchomić się na stacji końcowej i decyduje czy jest ona bezpieczna. | Zapewnia pełną kontrolę tego, gdzie i kiedy skrypty są uruchamiane w środowisku. |
| **Egzekwowanie zasad korzystania z urządzeń** | **Ochrona pamięci operacyjnej** | **Kontrola aplikacji na urządzeniach o stałych funkcjonalnościach** |
| Kontroluje, które urządzenia mogą być używane w określonym środowisku, eliminując urządzenia zewnętrzne jako potencjalny wektor ataku. | Proaktywnie identyfikuje próby złośliwego wykorzystania pamięci (ataki bezplikowe) z natychmiastową, automatyczną reakcją na potencjalny incydent. | Zapewnia, że urządzenia o stałych funkcjach (POS, infokioski, itp.) są zawsze w oryginalnym stanie i wykorzystywane zgodnie z przeznaczeniem. |

# WŁAŚCIWOŚCI

- **Skanowanie złośliwego oprogramowania na Android™**
- **UEM dla App Store Android i skanowanie APK**

• Skanowanie wszystkich aplikacji w BlackBerry UEM, w tym aplikacji klientów i aplikacji partnerskie w celu ochrony przed złośliwym oprogramowaniem.

- **Wykrywanie phishingu i złośliwych adresów URL**

• Wykorzystanie sztucznej inteligencji do automatycznego wykrywania i zatrzymywania złośliwych adresów URL, w tym z osadzonymi elementami phishingowymi.

- **Tworzenie bezpiecznych aplikacji**

• Umożliwia partnerom oraz organizacjom tworzyć własne, bezpieczne aplikacje dla urządzeń klasy enterprise.

- **Sprawdzanie integralności aplikacji IOS dla BlackBerry Dynamics SDK Apps**

• Zapewnia integralność aplikacji zbudowanych na platformie BlackBerry® Dynamics™ SDK.
• Umożliwia instalację tylko bezpiecznych aplikacji i zapobiega ingerencji w aplikacje BlackBerry®.

## BlackBerry Protect dla urządzeń mobilnych

Obecnie, bardziej niż kiedykolwiek, organizacje wykorzystują urządzenia mobilne, aby konkurować na dynamicznie rozwijającym się rynku i utrzymać swoich pracowników w kontakcie. Po raz pierwszy można zaobserwować sytuację, w której ponad połowa wszystkich podłączonych urządzeń do Internetu to urządzenia mobilne[2]! Wiąże się z tym również większe ryzyko ataków malware, których liczba zwiększa się z roku na rok. Jak dotąd rozwiązania zabezpieczające dla przedsiębiorstw koncentrowały się na urządzeniach stacjonarnych, jednak coraz więcej firm odkrywa rosnące zagrożenie ataków phishingowych wymierzonych w urządzenia mobilne, zwłaszcza w obrębie aplikacji.

Szkody wynikające z tych ataków mogą być istotne, a informacje umożliwiające identyfikację osób i inne krytyczne dane wyciekają z większą częstotliwością niż kiedykolwiek wcześniej. To sprawia, że coraz więcej organizacji decyduje się na zastosowanie głębokiej inspekcji pakietów (DPI) i innych rozwiązań bezpieczeństwa w celu ochrony przed złośliwymi atakami.

Nie jest zatem zaskoczeniem, że rynek mobilnych systemów ochrony przed zagrożeniami rozwija się w bardzo szybkim tempie. BlackBerry Mobile Threat Defense oferuje dodatkową warstwę ochrony dla samego urządzenia jak i dla aplikacji zainstalowanych na urządzeniach mobilnych.

**BlackBerry Protect monitoruje ataki na poziomie urządzenia i oprogramowania:**

• **Na poziomie urządzenia,** BlackBerry Protect identyfikuje luki w zabezpieczeniach oraz potencjalne złośliwe aktywności poprzez monitorowanie aktualizacji systemu operacyjnego, parametrów systemu, konfiguracji urządzenia oraz bibliotek systemowych.
• **Na poziomie aplikacji,** BlackBerry Protect dla urządzeń mobilnych wykorzystuje sandboxing aplikacji i analizę kodu, jak również testy bezpieczeństwa aplikacji, w celu identyfikacji złośliwego oprogramowania i grayware.

## Typowe przypadki użycia BlackBerry Protect

**BlackBerry Protect zapewnia pełne spektrum zapobiegania zagrożeniom, które powstrzymuje incydenty bezpieczeństwa na stacjach końcowych poprzez:**

- identyfikowanie i blokowanie złośliwych plików wykonywalnych bez konieczności ciągłych aktualizacji lub połączenia z chmurą;
- identyfikowanie luk w zabezpieczeniach i potencjalnych złośliwych działań poprzez monitorowanie aktualizacji systemu operacyjnego, parametrów systemowych, konfiguracji urządzeń i bibliotek systemowych;
- kontrolę gdzie, jak i kto może wykonywać skrypty;
- zarządzanie wykorzystywaniem urządzeń USB i zapobieganie używaniu nieautoryzowanych urządzeń;
- powstrzymywanie ataków bezplikowego złośliwego oprogramowania;
- blokowanie urządzeń o stałej funkcjonalności, takich jak infokioski, terminale POS itp.;
- zapobieganie atakom typu zero-day i ransomware;
- zapobieganie atakom opartym na wykorzystaniu pamięci i exploitom;
- wykorzystanie sandboxingu i analizy kodu aplikacji, a także testów bezpieczeństwa aplikacji w celu
- identyfikacji złośliwego oprogramowania i grayware;
- identyfikowanie złośliwego oprogramowania, którego źródłem może być sideloading, unikalne złośliwe oprogramowanie oparte na sygnaturach lub symulacje;
- ochronę punktów końcowych, gdy użytkownicy są w trybie online lub offline.


## SKONTAKTUJ SIĘ Z NAMI:

**www.bakotech.pl**

**blackberry@bakotech.pl**

**+48 12 340 90 30**

bako tech®

in @bakotechpl
@bakotechpl
Bakotech Poland&CEE