BlackBerry
Intelligent Security. Everywhere.

Datenblatt

BlackBerry Persona

KI-gesteuerte kontinuierliche Authentifizierung und Verhaltensanalysen

BlackBerry Persona ist ideal für alle Unternehmen, die einen Zero-Trust-Ansatz für ihre Cyber-Sicherheitsstrategie implementieren wollen.

Persona for Desktops – Übersicht

BlackBerry® Persona ist eine KI-gesteuerte Lösung für kontinuierliche Authentifizierung und Verhaltensanalyse, mit der verdächtige Benutzer in Echtzeit identifiziert werden können. Hauptmerkmale:

- Schutz vor Missbrauch gestohlener Zugangsdaten durch Verhaltensanalyse und Verlaufsanalyse.
- Schutz vor Insider-Bedrohungen durch Verlaufsanalyse.
- Echtzeit-Risikominderungsmaßnahmen am Endpunkt, etwa 2FA-Abfragen, Netzwerkentfernung und Sperrung von Benutzerkonten.
- Anzeige von Endpunkt-Ereignissen und Integrität eines Anwenders beinahe in Echtzeit, auf einer einzigen, vertrauten, intuitiven Cloud-Konsole.
- Integration von Drittanbietern wie Ping und OKTA zur Bereitstellung einer kontinuierlichen Authentifizierung für Webanwendungen.

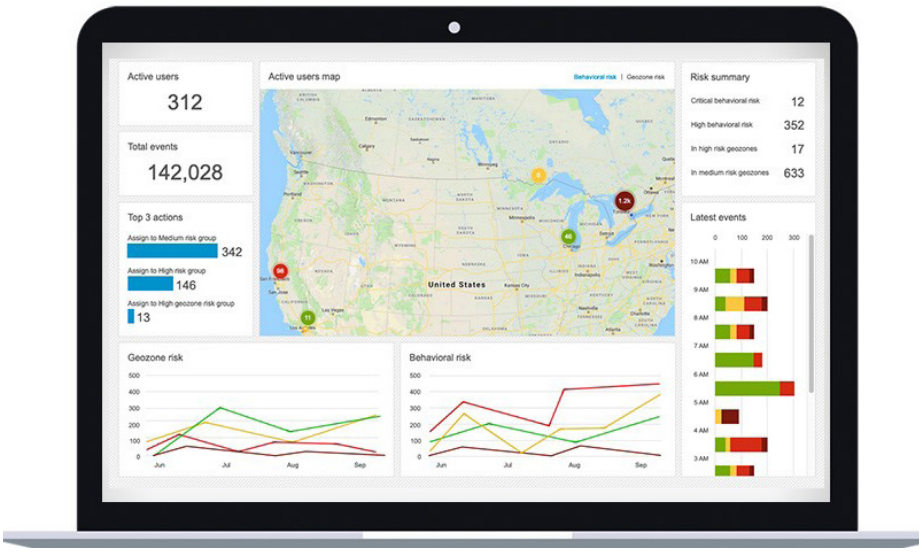
BlackBerry Persona

Anwendungsfälle

BlackBerry Persona ist ideal für alle Unternehmen, die einen Zero-Trust-Ansatz für ihre Cyber-Sicherheitsstrategie implementieren wollen. BlackBerry Persona für Desktops nutzt die bereits in BlackBerry Persona for Mobile (eine Komponente der BlackBerry Spark® Unified Endpoint Management Suite) bewährte Verhaltensanalyse sowie verhaltensbasierte Machine-Learning-Modelle und ermittelt so die Vertrauenswürdigkeit des Gerätenutzers. Diese Information wird verwendet, um eine automatisierte Risikominderungn auszulösen, durch die Angriffe mittels Zugangsdaten in Minuten gestoppt werden können. Folgende Sicherheitsprobleme des Unternehmens werden durch BlackBerry Persona sofort nach der Bereitstellung gelöst:

- **Gestohlene Zugangsdaten –** BlackBerry Persona schützt ein Unternehmen vor Schäden infolge kompromittierter Zugangsdaten von Mitarbeitern. BlackBerry Persona analysiert anhand von Verhaltensanalyse und Verhaltensmodellen die Benutzerinteraktion mit dem Gerät in Echtzeit und ermittelt das Risiko. Überschreitet der Anwender den Risikogrenzwert, werden Warnmeldungen an die Cloud gesendet und automatische Maßnahmen ergriffen, etwa Zwei-Faktor-Authentisierung.
- **Insider-Bedrohungen –** BlackBerry Persona schützt Unternehmen auch vor Schaden durch Mitarbeiter. Das Mitarbeiterverhalten wird laufend auf bedrohende Aktionen analysiert. Wenn das normale Verhalten eines Mitarbeiters vom Standardverhalten abweicht – er etwa riskante Anwendungen herunterlädt oder Daten exfiltriert –, so wird dieses Verhalten von BlackBerry Persona als anormal identifiziert. Auf der Grundlage der vom Administrator definierten Richtlinien werden Warnmeldungen ausgegeben und proaktive Maßnahmen ergriffen.
- **Physische Kompromittierung –** BlackBerry Persona schützt Mitarbeiter und Organisationen vor Angriffen, bei denen das Gerät physisch kompromittiert und/oder gestohlen wurde. Haben unbefugte Benutzer Zugriff auf den Endpunkt, so können die Verhaltensanalysemodelle (Tastenanschlag, Maus) einen neuen Benutzer erkennen und Warnmeldungen senden oder das Gerät sperren. Diese Aktionen erfolgen automatisch am Endpunkt und erfordern keine Netzwerkverbindung oder Interaktion mit der Cloud.

„... BlackBerry Persona für Desktops nutzt die Verhaltensanalyse und verhaltens-basierte ML-Modelle und ermittelt so die Vertrauens-würdigkeit des Gerätenutzers.“



Funktionsweise

Die Fähigkeit von BlackBerry Persona zu maschinellem Lernen ermöglicht es dem System, durch Identifikation der Verhaltens- und Standortmuster mehrerer Benutzer, das Standortrisiko zu bestimmen. Identifiziert das System etwa wiederholte Muster großer Mitarbeitercluster am selben Standort, so kann es diesen automatisch als Arbeitsort festlegen. Auf Wunsch können auch im Voraus bekannte Standorte geladen werden.

Bei kontinuierlicher Authentifizierung verwendet BlackBerry Persona Verhaltensanalyse zur Erkennung typischer Nutzungsmuster von Desktop-Software und bestimmt in Echtzeit, welches Verhalten ein hohes bzw. geringes Risiko darstellt. Zu den nutzungsbasierten Mustern gehören die Tageszeit und die Software-Nutzungsart des Anwender, etwa interne oder externe Weiterleitung. BlackBerry Persona verwendet eine Reihe weiterer Faktoren, um zu entscheiden, welche Zugriffsebene zu einem Mitarbeiter- oder Auftragnehmerprofil zu einem Zeitpunkt gewährt wird. Dazu gehören:

- **Verhalten:** BlackBerry Persona wertet die Eingabemerkmale eines Benutzers aus und bestimmt so einen analytischen Verhaltensstandard, aus dem es die Authentizität der Zugangsdaten ableitet.
- **Standort:** BlackBerry Persona betrachtet die Häufigkeit und die Muster vonAnwendern, basierend auf der prädiktiven Analyse anonymisierter Standortdaten zur Bestimmung eines standortbasierten Risikowertes.
- **Netzwerk:** BlackBerry Persona bestimmt die Häufigkeit der Netzwerknutzung und passt auf Grundlage dieses Profils die Sicherheit dynamisch an. Der erstmalige Zugriff auf ein öffentliches Wi-Fi würde eine entsprechende Anpassung der Risikobewertung nach sich ziehen.
- **Anomalien*:** BlackBerry Persona bewertet die Anwendungsnutzung und arbeitet mit einer Abschätzung von akzeptabler und anomaler Nutzung, um die Vertrauenswürdigkeit der Zugangsdaten zu bestimmen.

Risikoanalyse: Dynamische Anpassung der Sicherheitsanforderungen

BlackBerry Persona verfügt über die einzigartige Fähigkeit, basierend auf Echtzeit-Risikoanalysen Zugriff zu gewähren und Authentifizierungsabfragen auszugeben. Das erleichtert die Arbeit des Anwenders, ohne die Sicherheitsrichtlinien zu beeinträchtigen. BlackBerry Persona kann auf Basis einer Echtzeit-Risikowertanalyse Folgendes:

- Zugang gewähren
- Eine Richtlinie anpassen
- Zur Authentifizierung auffordern
- Warnen und Gegenmaßnahmen einleiten

BlackBerry Persona passt die Sicherheits- Richtlinien dynamisch an und ergreift gegebenenfalls Gegenmaßnahmen. So können die Sicherheits-Richtlinien und die Anwendererfahrung ohne Konflikte dynamisch optimiert werden.

*Patent angemeldet

„Bei kontinuierlicher Authentifizierung verwendet BlackBerry Persona Verhaltensanalyse zur Erkennung typischer Nutzungsmuster von Desktop-Software, um in Echtzeit zu bestimmen, welches Verhalten ein hohes bzw. geringes Risiko darstellt.“

Die Vorteile von BlackBerry Persona

Im Gegensatz zu herkömmlichen Lösungen, die zunächst alle Daten vom Endpunkt zur Verarbeitung in die Cloud senden müssen, nutzt und verarbeitet BlackBerry Persona unverschlüsselte, unverfälschte Daten am Ort des Geschehens – am Endpunkt. Außerdem befinden sich die Daten und die Logik von BlackBerry Persona am Endpunkt, was schnellere Erkennung und umfassende proaktive Risikominderungsmaßnahmen ermöglicht.

Schnelle Erkennung

Nach einer Kompromittierung kann innerhalb weniger Tage eine beträchtliche Datenmenge exfiltriert werden. BlackBerry Persona bietet bei Kompromittierung raschen Schutz und begrenzt den Missbrauch von Zugangsdaten.

Erhöhte Sicherheitseffizienz

BlackBerry Persona ist einzigartig, da es auch auf der Grundlage des Benutzerverhaltens am Endpunkt bewertet, ohne Daten in die Cloud zu streamen.

Geringere Kosten

Da BlackBerry Persona sich am Endpunkt befindet, können alle Benutzeranalysen und -bewertungen kontinuierlich dort und in Echtzeit erfolgen. Das reduziert die in die Cloud übertragene und gespeicherte Datenmenge erheblich.

Bessere Kontrolle

BlackBerry Persona ergreift, zusätzlich zu den in der Verwaltungskonsole generierten Warnmeldungen, proaktiv Maßnahmen am Endpunkt, fordert etwa 2FA an, schränkt den Netzwerkzugriff ein oder sperrt Benutzerkonten.

Über BlackBerry

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 175 Millionen Autos, die heute auf unseren Straßen unterwegs sind. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpunkt-Sicherheitsmanagement, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist eine sichere vernetzte Zukunft, der man vertrauen kann.

Für weitere Informationen besuchen Sie BlackBerry.com und folgen Sie @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-0687 | 201120