BlackBerry®
Intelligent Security. Everywhere.

Data Sheet

BlackBerry Persona

AI-Driven Continuous Authentication and Behavior Analytics

Organizations seeking to employ a Zero Trust approach to their cybersecurity policy are finding BlackBerry Persona for desktop devices to be a foundational element.

Persona for Desktops Overview

BlackBerry® Persona is an AI-driven continuous authentication and behavior analytic solution designed to identify suspicious users in real time to prevent security breaches. Key features include:

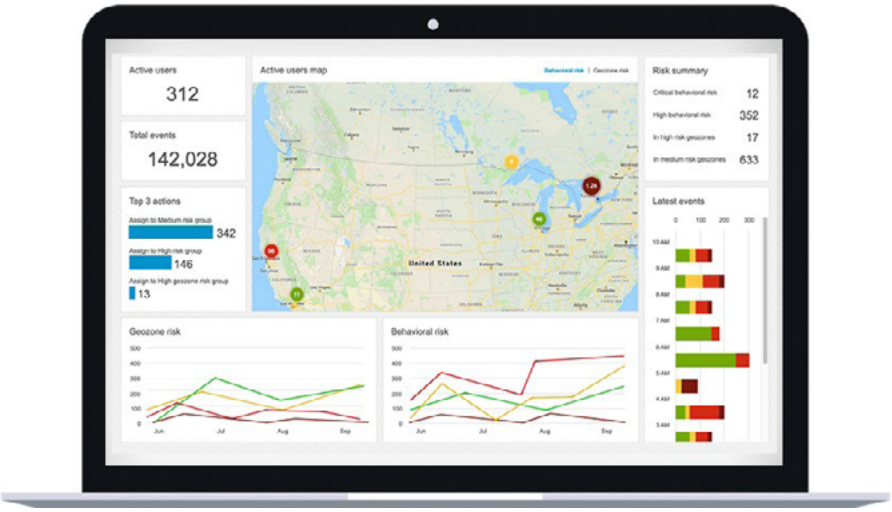
- Protection from misuse of stolen credentials using both behavior analysis and conduct analysis engines.
- Protection from insider threats through malicious conduct analysis engines.
- Real-time mitigation actions at the endpoint such as 2FA challenges, network removal, and user account suspension.
- A near real-time view of endpoint events and user trust scores, all from a single, familiar, intuitive cloud console.
- Integrations with third-party providers such as Ping and OKTA to provide continuous authentication for web apps.

BlackBerry. Persona

Key Use Cases

Organizations seeking to employ a Zero Trust approach to their cybersecurity policy are finding BlackBerry Persona for desktop devices to be a foundational element. As proven with BlackBerry Persona for mobile devices (a component of the BlackBerry Spark® Unified Endpoint Management Suite), BlackBerry Persona for desktops leverages behavior analysis and conduct-based ML models to create a real-time user trust score on the device. This information will be used to trigger automated mitigation actions, enabling attacks involving user credentials to be stopped within minutes. When deployed, BlackBerry Persona immediately solves these enterprise security issues:

- **Stolen Credentials —** BlackBerry Persona protects an organization from damage done when employee credentials have been compromised. BlackBerry Persona analyzes the user's interaction with their device in real time via behavior analysis and conduct models — and makes a determination of user risk. If the user exceeds the risk threshold, alerts are sent to the cloud and automated mitigation actions such as prompting for a second-factor authentication method are taken.
- **Insider Threats —** BlackBerry Persona protects an organization from damage done from rogue employees by continuously analyzing their conduct and determining if their actions are malicious. If an employee's normal conduct deviates from their standard behavior, such as downloading risky applications and data exfiltration, BlackBerry Persona will identify this conduct as anomalous. Alerts and proactive actions will be taken, based on administrator-defined policy.
- **Physical Compromises —** BlackBerry Persona protects employees and organizations against attacks where the device has been physically compromised and/or stolen. If unauthorized users gain access to the endpoint, the behavior analysis models (keystroke, mouse) can sense a new user and send alerts or lock the device. These actions happen automatically at the endpoint and don't require a network connection or interaction with the cloud.


Active users
312

Total events
142,028

Top 3 actions

Assign to Medium risk group	342
Assign to High risk group	146
Assign to High geozone risk group	13

Risk summary

Critical behavioral risk	12
High behavioral risk	352
In high risk geozones	17
In medium risk geozones	633

> "...BlackBerry Persona for desktops leverages behavior analysis and conduct-based ML models to create a real-time user trust score on the device."

How it Works

The machine learning capability of BlackBerry Persona enables the system to identify behavioral and location patterns of multiple users to determine location risk. For example, if the system identifies repeated patterns of large clusters of employees in the same location, it can automatically determine that as a work location, or if the business chooses to, it can preload known locations.

With continuous authentication, BlackBerry Persona uses behavior analysis to recognize typical desktop software usage patterns to determine what behavior is high or low risk in real time. The usage-based patterns include time of day and how the user is using the software, forwarding internally vs. externally, etc. BlackBerry Persona uses a range of other factors to decide what level of access should be granted to an employee or contractor profile at any given moment, including:

- **Behavioral Analytics:** BlackBerry Persona evaluates a user's input characteristics to determine a behavioral analytic standard from which a determination on user credential authenticity is made.
- **Behavioral Location:** BlackBerry Persona looks at the frequency and patterns of users, based on predictive analysis of anonymized location data to determine a location-based risk score.
- **Network Trust:** BlackBerry Persona determines the frequency of network use and adjusts security dynamically based on that profile. Accessing a public Wi-Fi for the first time would adjust the risk score accordingly.
- **Usage Anomalies*:** BlackBerry Persona assesses the application usage and gauges acceptable usage from anomalous usage to determine trust of the user's credentials.

> "With continuous authentication, BlackBerry Persona uses behavior analysis to recognize typical desktop software usage patterns to determine what behavior is high or low risk in real time."

Risk Score Analysis: Dynamically Adopt the Security Requirements

BlackBerry Persona has the unique capability to grant access and issue authentication challenges based on real-time risk analysis, enhancing end-user experience and productivity without sacrificing security policies. Based on real-time risk score analysis, BlackBerry Persona can:

- Grant Access
- Adopt a Policy
- Issue an Authentication Challenge
- Alert and Remediate

BlackBerry Persona dynamically adapts security and policy posture and will apply remediation when needed. This allows the user experience and security/policy posture to be mutually and dynamically optimized, versus in conflict.

*Pending Features

BlackBerry Persona Benefits

In contrast to traditional solutions that must first send all data from the endpoint to the cloud for processing, BlackBerry Persona leverages and processes unencrypted, clean data, from the point of truth – the endpoint. Additionally, BlackBerry Persona's data and logic reside at the endpoint, allowing for faster time to detection and a comprehensive set of proactive mitigation actions.

Fast Time to Detection

A significant amount of data can be exfiltrated within days of a compromise. BlackBerry Persona offers protection rapidly in response to a compromise by limiting the misuse of credentials.

Increased Accuracy

BlackBerry Persona is unique in that it includes scoring based on user behavior locally at the endpoint without streaming data to the cloud.

Reduced Costs

Because of the presence of BlackBerry Persona on the endpoint, all user analysis and scoring can occur continuously in real time at the endpoint, vastly reducing the amount of data that needs to be transmitted and stored in the cloud.

Greater Control

In addition to alerts that will be generated in the administration console, BlackBerry Persona will proactively take action at the endpoint such as presenting 2FA challenges, restricting network access, suspending user accounts, and more.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry®

Intelligent Security. Everywhere.