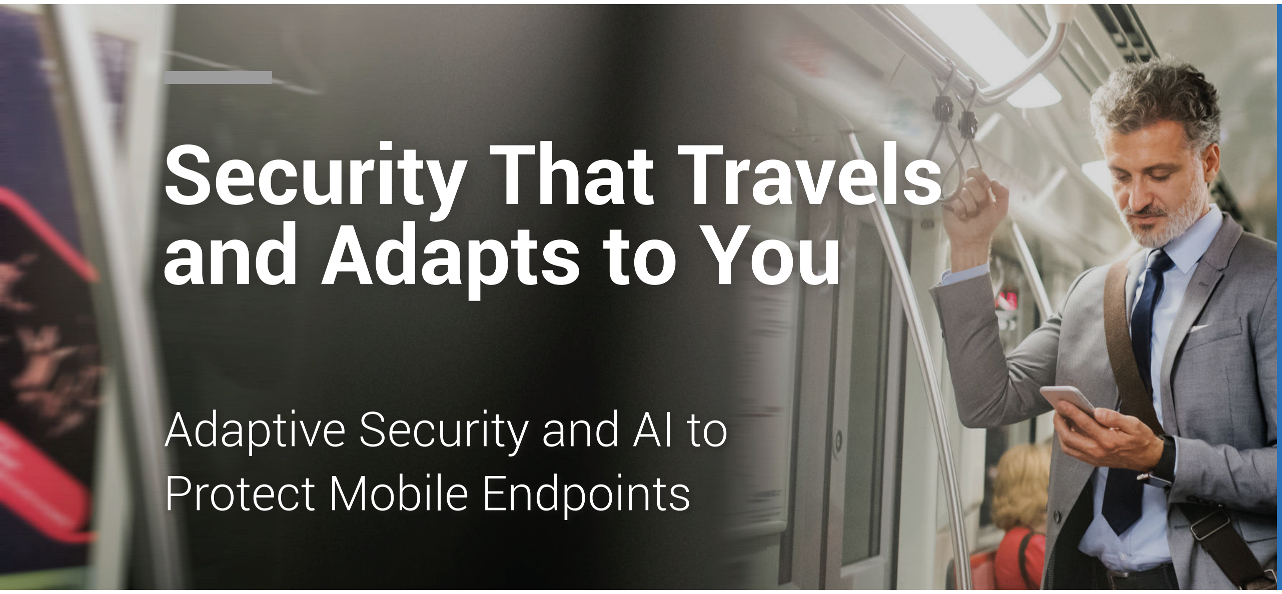
BlackBerry

Brochure



Security That Travels and Adapts to You

Adaptive Security and AI to Protect Mobile Endpoints

iOS

macOS

The Challenge of Staying Secure — and Productive — in a Mobile World

The explosion in mobile has provided unprecedented value and convenience for consumers, but there's also a downside. The shift from landlines to mobile devices significantly broadens the attack surface, which means that businesses are more vulnerable than ever before to cyberattacks, user impersonation, and data theft. The cost of cybercrime is steep and getting steeper.

Until recently, the options for businesses trying to secure employee devices and apps were limited. For the most part, mobile device management (MDM) solutions depended on pushing out security policies to each individual endpoint. But this was a difficult and costly responsibility for companies with thousands or more employees, many of whom were now bringing their own devices to work.

Introducing CylancePERSONA

Now there's a way to adjust your security policies on the fly to match changing risk profiles of users as they move from place to place. CylancePERSONA® is an advanced solution that intelligently administers and enforces security policies across all of your endpoints using artificial intelligence (AI) and predictive analytics to adjust and update policies automatically based on changing situational risk.

Instead of applying inflexible, static policies, now you can continuously adapt your security and policy posture to keep pace with the fast-changing risks experienced by users. CylancePERSONA is an effective way to keep all your people secure without impacting their productivity, and safeguard your data and assets by leveraging the power of adaptive security and AI to enhance mobile endpoint security in zero trust environments.

CylancePERSONA

Adapting As You Move: Wherever you go around the world, CylancePERSONA travels with you, adapting policies automatically to your changing location and work habits.

Boosting Productivity: CylancePERSONA streamlines access to apps and services when people are working in a safe, trusted environment, then tightens access in riskier locations.

Locking Out Attackers: CylancePERSONA helps companies keep cybercriminals at bay and neutralize attacks proactively.

Real-time Risk Scoring

CylancePERSONA dynamically adapts the security requirements of protected devices and apps to every user's real-world experience. It generates a continually evolving risk score in real time based on:

- **Geographic location:** Learns the trusted locations, frequency and patterns of users based on analysis of anonymized location and other behavioral inputs to determine behavior and location-based risk score. Locations can be predefined with a set of policy actions to be executed when a user is within the location boundaries.
- **Network trust:** Learns the frequency of network use and adjusts security dynamically based on that profile. For example, the solution would adjust the risk score accordingly for a user who is accessing any new Wi-Fi for the first time.
- **Time and usage anomalies:** Learns how and when employees normally access data to protect against instances of anomalous behavior.
- **Device and application DNA*:** Builds a uniquely identifying signature for trusted, compliant devices and apps, and uses that signature to detect and block access attempts by rogue, non-compliant devices.

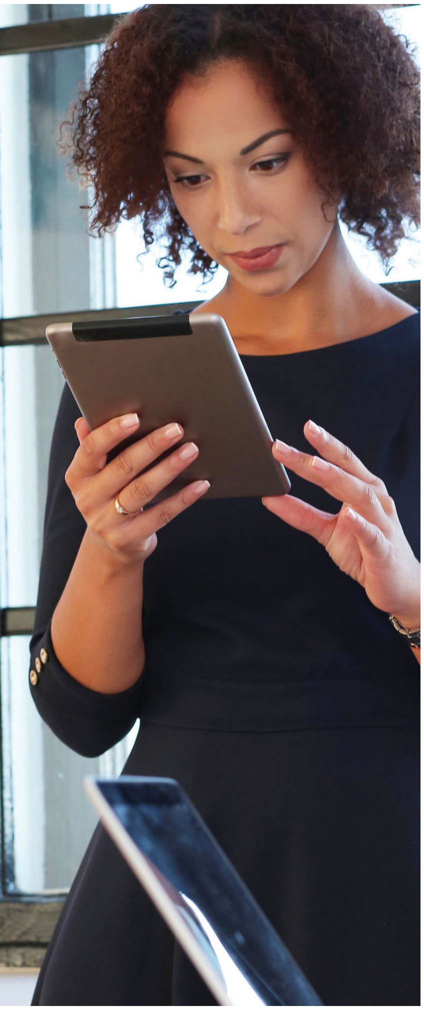
Adjust Security Requirement to Match Risk Exposure

As the risk score is continuously updated, users may be required to change how they login and access different enterprise systems and applications. For example, if users are signing in from an office location that is frequently used — and running apps that are typical for those users — they may only need a simple password to gain entry. But for users traveling to a new, potentially high-risk place, or launching apps for the first time, tighter controls may be put in place.

You're in Control

With CylancePERSONA, you can build trusted user-behavior models designed for your specific business and industry. For example, you can create customized risk score ranges and specify the management actions to be taken at each risk level. You can also define custom geo-zones and assign unique risk levels and management actions for each one. An example of a geo-zone might be a secure, trusted office location, to which you would assign a low risk level.

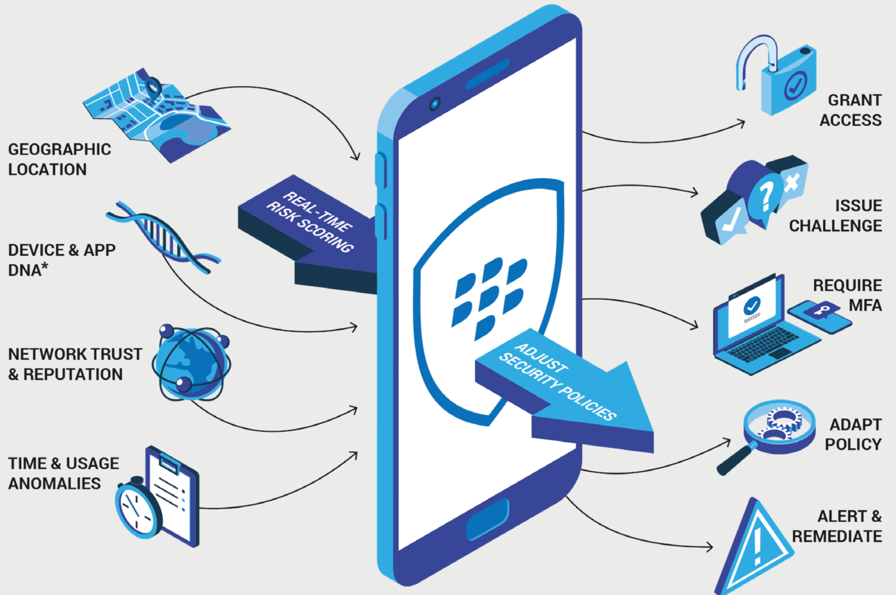
* Pending feature



Cost-effective and Extensible

In most cases, you can implement CylancePERSONA with minimal new investments in IT infrastructure, and it may help you save money by eliminating the need for a separate multi-factor authorization solution. And because the solution is built on BlackBerry's extensible Platform-as-a-Service (PaaS) architecture, you can integrate third-party data and threat-detection services. The solution works with most SAML-based business applications such as Salesforce and Microsoft® Office® 365 through integrations with BlackBerry Enterprise Identity.

Inside CylancePERSONA



* Pending feature

Continuous Authentication

Continuous Authentication assesses a user's ongoing behavior to authenticate and grant access to corporate data. With Continuous Authentication, CylancePERSONA uses in-app behavior analysis to recognize typical app usage patterns within BlackBerry® Dynamics™ applications and determine if any specific in-app actions are high or low risk in real time. Malicious users are automatically blocked from accessing apps when they exhibit anomalous behavior that doesn't fit with legitimate users' learned, trusted behaviors. This enhances the security posture, and at the same time, improves end user experience.

Enhanced User Experience

With CylancePERSONA, employees and other users experience less frustration because the solution adapts the security and policy posture to their current work circumstances instead of applying a one-size-fits-all static policy.

CylancePERSONA Changes the Game

Learn more about CylancePERSONA at blackberry.com/cylancepersona.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.