::: BlackBerry. | Cybersecurity

CylancePERSONA

Most unified endpoint management products on the market place a policy on the device or within the application that tells the device or app what the security policy should be. While this works, it is very rigid, such that you would have the same profile when working at the office as you would when traveling.

Wouldn't it be better if the security policy could relax when you are at the office, or change dynamically if you are travelling in a higher-risk location?

CylancePERSONA™, which is part of BlackBerry Spark® Suite, solves this problem with what we call "analyticsdriven" security. CylancePERSONA models the unique BlackBerry analytics data that is derived from our secure containers and our NOC combined with spatial data to determine a real-time risk score that adapts the security policy for the user to create the best experience.

RISK SCORE FACTORS: HOW IT WORKS

In addition to the adaptive policy, the machine learning capability of CylancePERSONA 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, 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. The usage-based patterns include time of day and how the user is using the app, for example forwarding internally vs. externally.

CylancePERSONA 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, such as:

- **Behavioral Location:** CylancePERSONA 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:** CylancePERSONA 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.

- **Time and Usage Anomalies*:** CylancePERSONA integrates seamlessly with other identity providers and systems, such as BlackBerry's proven security infrastructure, to enable all data to be securely and easily shared.

- **Device and App DNA*:** CylancePERSONA has the ability to determine whether devices and apps are compliant and up to date and can adjust the security policy based on the Device and App DNA profile.

Using CylancePERSONA, IT can dynamically adapt the security requirements and behavior of enterprise devices and apps to each user's real-world experience.

*Pending Features

RISK SCORE ANALYSIS: DYNAMICALLY ADAPT THE SECURITY REQUIREMENTS

CylancePERSONA 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, CylancePERSONA can:

• Grant access

• Adopt a policy

• Issue an authentication challenge

• Alert and remediate

CylancePERSONA dynamically adapts the 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.

CylancePERSONA BENEFITS

INCREASED ENDPOINT SECURITY	ENHANCED END-USER EXPERIENCE	IMPROVED PRODUCTIVITY AND REDUCED COST
• Decreases the risk that comes with lost devices • Ensures that devices/app cloning is virtually impossible • Detects and remediates behavior that can lead to data loss— whether intentional or not	• Adapts security and policy posture to actual context, versus applying only static policies • For example, enabling zero sign-in and/or increasing timeouts if it is a low-risk pattern in high-trust location	• Streamlined access to apps and services for users • Builds on existing investments in BlackBerry® UEM. BlackBerry Dynamics, and BlackBerry EID

CylancePERSONA SECURITY SERVICES

BlackBerry will take the time to understand your unique business objectives and priorities, working to understand your business model and how you make money. BlackBerry will then help you build the right cybersecurity strategy from the ground up, mitigating your cybersecurity risk without disrupting employee productivity, product usability, customer convenience, or other business-critical outcomes.

CylancePERSONA Security Services provide you with the expertise and experience of our team of cybersecurity consultants who will enable policy development in line with CylancePERSONA capabilities. CylancePERSONA Security Services will guide you in understanding your threat surface and attack vectors in the current threat landscape, enabling maximum benefit from CylancePERSONA. is allows the user experience and security/policy posture to be mutually and dynamically optimized, versus in conflict.

::: BlackBerry. Intelligent Security. Everywhere.

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 over 195M vehicles. 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, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

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