Datasheet

BlackBerry Intelligent Security

Most unified endpoint management products on the market, including BlackBerry® UEM, 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 traveling in a higher-risk location?

The BlackBerry® Intelligent Security service, built on the BlackBerry Spark™ platform, solves this problem with what we call "analytics-driven" security. BlackBerry Intelligent Security models the unique BlackBerry analytics data that is derived from its secure containers and 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 BlackBerry Intelligent Security 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.

BlackBerry Intelligent Security 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:** BlackBerry Intelligent Security 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 Intelligent Security 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 & Usage Anomalies:** BlackBerry Intelligent Security can determine and build a contextual risk score based on learning how and when you normally access data.

- **Device and App DNA:** BlackBerry Intelligent Security has the ability to determine whether the device and apps are compliant and up to date, and can adjust the security policy based on the device and app DNA profile.

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

Risk Score Analysis: Dynamically Adapt the Security Requirements

BlackBerry Intelligent Security integrates seamlessly with other identity providers and systems as BlackBerry's proven security infrastructure to enable all data to be securely and easily shared. Therefore, BlackBerry Intelligent Security 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 Intelligent Security can:

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

BlackBerry Intelligent Security 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.

BlackBerry Intelligent Security Benefits

Increased Endpoint Security

- Decreases the risk that comes with lost devices
- Protects against device/app cloning and/or user impersonation
- Detects and remediates behavior that can lead to data loss - whether intentional or not

Enhanced End User Experience

- 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

Improved Productivity and Reduced Cost

- Streamlined access to apps and services for users
- Builds on existing investments in BlackBerry® UEM, BlackBerry® Dynamics™, and BlackBerry(R) Enterprise Identity

BlackBerry Intelligent Security Consultancy Service

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.

The BlackBerry® Intelligent Security Consulting Service provides you with the expertise and experience of our team of cybersecurity consultants who will enable policy development in line with the BlackBerry Intelligent Security capabilities. The consultancy service will guide you in understanding your threat surface and attack vectors in the current threat landscape, enabling maximum benefit from BlackBerry Intelligent Security.

About BlackBerry

BlackBerry is an enterprise software and services company focused on securing and managing IoT endpoints. The company does this with BlackBerry Spark™, an end-to-end Enterprise of Things platform, comprised of its enterprise communication and collaboration software and safety-certified embedded solutions. Based in Waterloo, Ontario, the company was founded in 1984 and operates in North America, Europe, Asia, Australia, Middle East, Latin America and Africa. The Company trades under the ticker symbol "BB" on the Toronto Stock Exchange and New York Stock Exchange.

For more information, visit www.BlackBerry.com.