BlackBerry

ADAPTIVE SECURITY AND AI TO PROTECT MOBILE ENDPOINTS

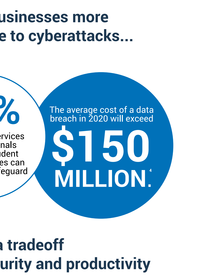
CylancePERSONA® Dynamically Adapts Security Policies Based on Situational Risk

In a Mobile World, It's Tough to Be Both Secure and Productive

More employees are going mobile…

87% of companies expect their employees to use their personal devices for work purposes.[1]

By 2025 there will be roughly **75 BILLION** connected devices.[2]



…making businesses more vulnerable to cyberattacks…

94% of financial services IT professionals are not confident their employees can adequately safeguard data.[3]

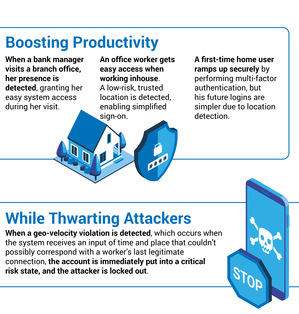
The average cost of a data breach in 2020 will exceed **$150 MILLION.**[4]

…and forcing a tradeoff between security and productivity

Apps are the #1 driver of productivity, but **80%** of financial services firms are limiting their deployment of apps due to security concerns.[5]

But Now You Can With

CylancePERSONA



Leverage real-time risk scoring

Enhance end user experience and productivity **without sacrificing security policies.**

Grant access and issue authentication challenges **based on real-time risk analysis.**

Automatically adjust security policies based on situational risk.

Build trusted user-behavior models with BlackBerry artificial intelligence and machine learning technology.

So the more you use it, the smarter your security gets

Security levels are **instantly adjusted** based on changes to **user location**, **past behavior**, and the **device or app being used.**

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.

Protecting Your People on the Move

When an international banker travels outside his country, device policies are dynamically adapted. Upon his return, in-country policies are automatically applied.

When a military officer enters a restricted zone, his camera and Bluetooth® connectivity are automatically disabled, while access to restricted information is enabled via secure browser.

Upon leaving the restricted zone, his camera and Bluetooth connectivity are automatically enabled, while access to restricted information is disabled.

Boosting Productivity

When a bank manager visits a branch office, her presence is detected, granting her easy system access during her visit.

An office worker gets easy access when working inhouse. A low-risk, trusted location is detected, enabling simplified sign-on.

A first-time home user ramps up securely by performing multi-factor authentication, but his future logins are simpler due to location detection.

While Thwarting Attackers

When a geo-velocity violation is detected, which occurs when the system receives an input of time and place that couldn't possibly correspond with a worker's last legitimate connection, **the account is immediately put into a critical risk state, and the attacker is locked out.**

Intelligent Security That Enforces Security Policies with AI

Learn More

blackberry.com/cylancepersona

*Pending feature

Sources
1. Symtonic: symtonic.com/wp-content/uploads/2016/09/Symtonic-2016-BYOD-Usage-in-the-Enterprise.pdf
2. Statista: www.statista.com/statistics/477/364/iot-number-of-connected-devices-worldwide/
3. Ponemon Institute: www.ponemon.org/local/upload/file/Ponemon%20Study%20Report.pdf?ep=financial-services-study-its-time-to-recognize-user-needs-and-secure-them.pdf
4. Juniper Research: www.calnetsolutions.com/cyber-security-facts-stats/
5. QuinStreet: www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-financial-services-study-its-time-to-recognize-user-needs-and-secure-them.pdf