Modernizing security for a **mobile workforce**

Agencies need to redirect their security efforts to keep pace with the changes and movements of the workforce

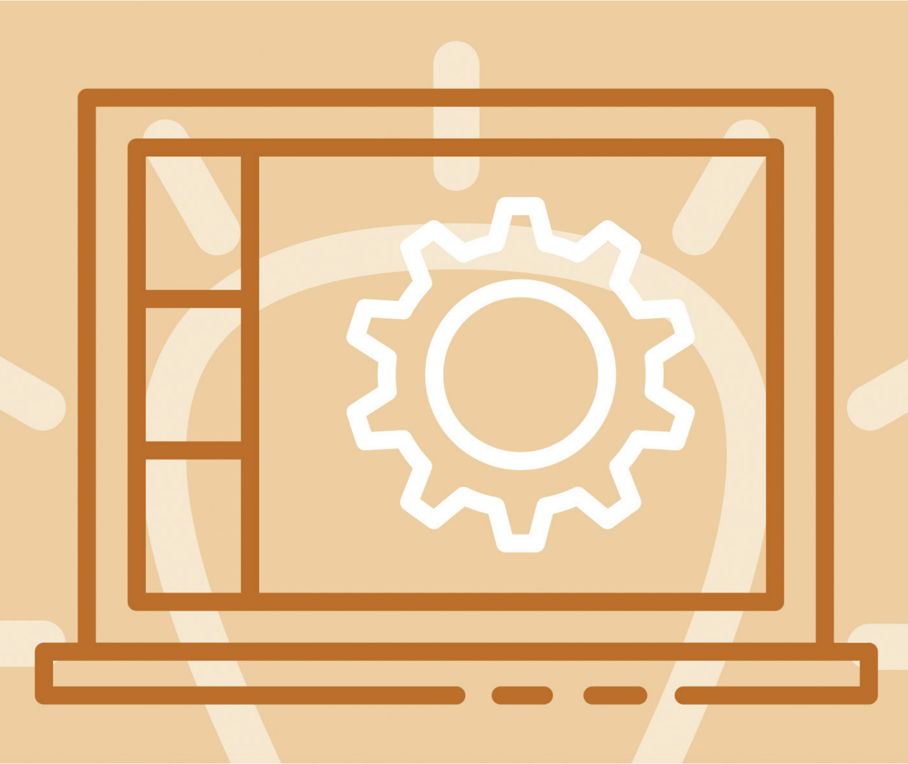
Brian Robison
Vice President, Solutions Strategy, and
Chief Evangelist, BlackBerry Inc.

THE TREND TOWARD REMOTE WORK accelerated during the pandemic, as did cybersecurity challenges. Many employees used their personal devices from home, which meant an influx of unknown machines flowing through VPNs and into government networks. In addition, some employees might have skipped normal security precautions in an effort to complete their work under chaotic and new conditions.

BlackBerry was a pioneer of remote work in the late 1990s. From the beginning, BlackBerry recognized securing access to data and communications was key for protecting the work being done. Agencies can apply these same principles by directing their security efforts to three areas: people, data and apps.

The move to continuous authentication

Securing data and apps begins with positively identifying the user. In government, agencies have used multifactor authentication and all kinds of certificates, but those are simple pass/fail security checks. Once users are allowed to cross the security barrier, they often have wide-ranging access to government resources. This means adversaries and malicious (or careless) insiders passing the security checks receive free rein as well.



Government needs to move to a continuous authentication model, which leads to better security and a better user experience. It involves seamlessly authenticating users every step of the way — when they touch the keyboard or scroll through an app on a screen. That activity, down to the microscopic vibrations in a person's fingertip, can be sensed and understood so that IT administrators can answer the question: Is this really the authenticated user, or is it somebody else?

Furthermore, data and even apps are no longer sitting inside castle-and-moat technology where agencies can control access through specific gates, such as VPNs. Today, data and apps could be anywhere, so agencies need to be able to secure their communications as well. For example, BlackBerry invented a technology that provides an additional layer of security for communications whether they are traveling over a hotel network, a coffee shop's Wi-Fi or a cell signal.

Finally, data should be encrypted when it is in motion and at rest. It should only be decrypted when an authorized user needs to see and interact with it. It's essential to continually ask: Does this person have permission and authorization to access

Shutterstock/FCW Staff

> **Data and even apps are no longer sitting inside castle-and-moat technology** where agencies can control access through specific gates, such as VPNs.

this data? Even though the credentials are correct, does the person's current behavior match known behavior, or could his or her account have been compromised?

Putting AI to work

Fortunately, advances in artificial intelligence (AI) can make it much easier for agencies to understand a user's normal behavior. AI can identify when someone does something out of the ordinary and immediately take action. For example, it can require a user to re-authenticate and block access until additional information is provided proving his or her identity.

AI can also tell the difference between good and bad software before it's allowed to execute. BlackBerry technology can detect and block ransomware because there are only certain ways to write encryption-capable malware. Using an AI engine trained on billions of files, good and bad, BlackBerry solutions can predict the behavior of software before it executes. If a recognized file, or even an unknown one, proves to be malicious, AI can stop it from running.

Agencies using all the tools available to secure people, data and apps are the key to building a modern and secure workplace. ■

Brian Robison is vice president of solutions strategy and chief evangelist at BlackBerry Inc.