AI and the Carrot Approach to Zero-Trust Network Access

When you tackle the job of security with artificial intelligence, the result is a liberated user base and a re-energized IT crew.

Chris Russo
Director of Sales, BlackBerry

HIGHER EDUCATION IT HAS ALWAYS understood the risks of a remote workforce. Any time a faculty member or student headed out to do work in the field, it was up to IT to help that individual get a secure connection back to the institution's network for uploading data and accessing resources, typically through the virtual private network. But it was the all-encompassing shift to remote learning, teaching and working that underscored the inadequacies of VPN security. After all, VPNs take a static approach to authentication and authorization. Once a threat actor passes an initial verification, they're often assumed safe for the duration of their connection.

Traditionally, heavy reliance on personal devices has created a conundrum for institutions: Either students and faculty would have limited access to the resources they needed, or unmanaged access was going to create a huge attack vector for malicious actors. When taking into account all of the personal, financial and healthcare-related data maintained by colleges and universities, it's little wonder higher ed quickly became one of the top targets for cyber criminals.

The answer has become Zero Trust, defined by NIST as "an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources." To enable Zero Trust without impacting end user experience requires constant autonomous verification and authentication for users and devices.

This is the kind of job that cries out for the use of artificial intelligence.

AI and Security

BlackBerry Gateway is a Zero Trust Network Access (ZTNA) solution. Using an AI-powered Zero Trust framework that continuously assesses risk ensures only secure and trusted devices access institutional resources. AI uses mathematical models to continuously examine numerous factors when determining trust and access levels of remote participants. Trust levels may be adjusted, for example, based on the following criteria:

- Is the user operating from a high-risk location?
- Is the user who they say they are?
- Is the user behaving normally?
- Is the user accessing expected resources?
- Does the user's behavior align with other users performing similar roles?

When a user's trust score changes, the AI can be configured to take various actions. For positive changes in trust, a user could be rewarded with continued or upgraded access. Negative trust changes may result in less access or a request to re-authenticate, or it might trigger security alerts and remediation procedures.

When we see AI in science fiction movies, we think of something that dims the lights when it's running. This isn't like that at all; this is a simple calculation that executes seamlessly – within nanoseconds – on the user's device.

Ensuring the technology is always on and working is a constant challenge for an IT team, especially with remote user devices. In this case, the carrot concept works extremely well. In order for a user to get to the carrot (files, folders, applications, intranets, etc.), they need to take the secure path to get there.

BlackBerry Gateway, when integrated with the BlackBerry Protect advanced AI-powered endpoint security product, provides a comprehensive defense against threats targeting devices, networks and user identity. BlackBerry Protect leverages AI to prevent known, unknown and zero-day threats, while BlackBerry Gateway ensures business networks are only accessed by trusted and healthy devices.

The Mission Hasn't Waivered

My first experience with mobility started with BlackBerry.

Some 20 years ago, I was outfitted with a BlackBerry device, and it was the first time I could get e-mail from the road. But it wasn't the built-in keyboard that made that device so special. It was really the fact that my organization's IT department trusted the BlackBerry security model so deeply, I could use my device to access sensitive corporate information.

BlackBerry's mission hasn't changed. But now, that security emphasis is used to secure some 500 million endpoints — including cars — produced by various companies.

That's why higher education has rediscovered BlackBerry. The university IT organization trusts the company to keep devices secure, whether they're owned by the institution or individual people — students, staff or faculty.

And now, without having to use a college-owned device that navigates through the college-owned firewall, users can once again be liberated, just like we were two decades ago, when we first got a taste of the freedom allowed by mobility.

***Chris Russo** is the director of sales for education and state and local government at BlackBerry. Previously, he served as enterprise sales manager for AI cybersecurity company Cylance, which was acquired by BlackBerry in 2019.*