IBM Newsroom

IBM AI Innovations Sharpen Risk Detection in Identity Management

More Individualized Approach Helps Optimize Both Security & User Experience

CAMBRIDGE, Mass., Dec. 10, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced it is extending its artificial intelligence (AI) technology originally developed to protect users in the financial services industry, to clients in all industries via the company's identity-as-a-service (IDaaS) offering. IBM Cloud Identity now features AI-based adaptive access capabilities that help continually assess employee or consumer user risk levels when accessing applications and services. The solution escalates suspicious user interactions for further authentication, while those identified as lower risk are "fast tracked" so they can access applications and services they need.

With data breaches on the rise, traditional means of securing access, like passwords, are often not enough to prevent unauthorized access. The rise of credential-stuffing attacks, where a malicious actor obtains a list of credentials and tests them at various other sites using a bot, demonstrates that many password combinations have been leaked. According to a 2019 report, compromised and weak credentials are cited as the cause for more than 80% of data breaches.[1] Meanwhile, 2017 research found that large companies are managing hundreds of applications – up to 788 custom applications on average for companies with more than 50,000 employees.[2] Considering the amount of programs and passwords that employees are managing between their professional and personal lives, it is increasingly important that new security measures do not hinder user experience.

"Companies are constantly trying to optimize both security and user experience, but the trick is ensuring security is not disrupting the everyday user journey," said Jason Keenaghan, Director, IBM Security. "IBM Cloud Identity with adaptive access is using AI to give organizations a holistic view of context for user access, based on indicators like malware and risk indicators, device insights, and user behavior, to help them focus security on high risk logins and give the majority of users seamless access to their accounts and applications."

Adaptive Access: Smart Context

Many organizations continue to rely on older username and password methods to provide employee and consumer users access to services. Due to the patchwork of applications and solutions organizations are working with, they may not be able to deploy more modern security layers. This can create a blind spot that prevents security teams from easily implementing rules that flag suspicious indicators like malicious logins, unknown locations, unrecognized devices, and whether a user is on a company's network VPN.

IBM Cloud Identity is an identity-as-a-service solution that helps organizations connect every user to every application using adaptive access. Through the use of AI, the service helps simplify access management and security for users by assigning user risk levels based on a defined set of factors. With these risk levels, administrators can create rules that level up or level down authentication - implementing strong authentication but only when needed. The service leverages the following features to determine risk and enable adaptive access decisions:

- **Artificial Intelligence -** a user behavior score is assigned based on the level of trust or risk assessed for each user. A number of factors are assessed including web intelligence, location data, malware and risk indicators, and device insights. For example, using AI, the system can detect irregular mouse movements or flag a user trying to login from a browser infected with keylogging malware. IBM Cloud Identity with adaptive access leverages IBM Trusteer AI technology to assess users based on a fraud evidence database, fraudulent pattern analysis, and cross-organizational patterning.
- **Smart Access and Seamless Login:** Since AI capabilities are able to assign risk levels, only users considered to pose a higher threat are prompted to go through multifactor authentication or denied access. By only prompting specific users to further verify their identification, rather than all users, organizations may be able to reduce operational expenses related to items such as two-factor authentication and help desk password resets for both current and new users. This can potentially lead to cost cuts considering organizations spanning different sectors have allocated more than $1 million per year to password-related support alone.[3]
- **Low-code Deployment:** Adaptive access policies can be created and applied to applications and APIs with little to no development effort, and without application changes.

"According to our primary research results, the establishment of low-friction end user experiences has the potential to help boost security effectiveness while reducing management efforts and related costs," said Steve Brasen, Research Director, Enterprise Management Associates. "By injecting intelligence into access processes, IBM is helping its customers implement the appropriate level of authentication enforcement for users while minimizing impacts to their productivity."

To learn more about IBM Cloud Identity with adaptive access, visit: www.ibm.com/us-en/marketplace/cloud-identity

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

CONTACT:
Kimberly Samra
ksamra@ibm.com
510-468-6406

[1] *2019 Data Breach Investigations Report* (Verizon, 2019)

[2] *Custom Applications and IaaS Trends 2017* (Cloud Security Alliance, 2017)

[3] *Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers* (Forrester, 2018)

SOURCE IBM

https://newsroom.ibm.com/2019-12-10-IBM-AI-Innovations-Sharpen-Risk-Detection-in-Identity-Management