LoginRadius Announces Release of Risk-Based Authentication

LoginRadius unveils authentication layer in its Cloud-based Identity Platform that offers a frictionless customer experience while maintaining data privacy.

VANCOUVER, BC, CANADA, September 25, 2017 /EINPresswire.com/ -- LoginRadius, a leader in Customer Identity Management, announced today the release of Risk-Based Authentication as an additional layer of security within the LoginRadius Platform.

As passwords are becoming less effective forms of authentication, organizations are moving to newer technologies such as Multi-factor Authentication, One-time Passwords, or even voice-call backs to better manage security risk. However, consumers don't want to deal with taking a call or entering a pin to get access. According to KuppingerCole, 75% of consumers are sick of passwords*.

However, they are still very concerned with maintaining the security of their personal data. Consider the following statistics:
- 90% have data privacy concerns*
- 74% have limited their online activity in the last year due to privacy concerns**
- 28% have stopped an online transaction due to privacy concerns**

Risk-Based Authentication (RBA), also known as "Adaptive Authentication", intelligently determines whether a user is who they claim to be or are being misrepresented. RBA allows you easily set up rules and actions to identify a user based on specific criteria:
- Current location - City and/or Country,
- Past logins,
- Browser or device IDs,
- Login failure attempts.

Using these criteria, you can create a Risk Profile to spot behavior out of character for that user and trigger actions to lessen any potential malicious activity. For example, User A's risk profile says that she accesses her online account once a day around 10 am Pacific from Washington State. Any login attempt matching that profile will be granted access.

If one day, that login request came instead from a computer located in the Shanxi province in central China at 1 am, those variables would suggest an unauthorized login attempt, and the platform then triggers an additional action, which serves as an second layer of authentication.

Actions can be anything from a notification email being sent to the user or administrator, to more drastic measures such as forcing the user to go through two-factor authentication, asking security questions, or blocking their access completely.

"Eliminating the need for a password to authenticate the user serves two purposes. First, it creates a much smoother experience for the user. And second, it actually makes the user's personal data more secure by not including it in the authentication process", said Deepak Gupta, CTO and Co-Founder of LoginRadius. "Devaluing personal identity attributes is recognized as a way to increase data security,

which is why we continue our efforts to innovate in passwordless identity authentication.”

In addition to Risk-Based authentication, the LoginRadius Identity Platform also offers additional authentication methods such as, Phone Login, Passwordless Login, Two/Multi-Factor Authentication and Anonymous Login.

To learn more about these features please visit https://www.loginradius.com/customer-identity/

* KuppingerCole - “Balancing User Experience, Privacy and Security for the Connected Customer 2017

** NCSA & TRUSTe US Consumer Privacy Index 2016

- End -

Media Team
LoginRadius Inc
1-844-625-8889
email us here
