Identity is more than just passwords and tokens — identity is defined by authentic behavior. Security leaders are waking up to this reality and more are re-evaluating MFA and CIAM approaches. Simple passwords and tokens are no longer sufficient to prevent account takeovers. Pulse and Acceptto surveyed 100 security leaders to understand the authentication and identity & access management challenges they face, and the rising popularity of continuous, passwordless authentication.

The vast majority (92%) of security decision makers admit that identity and access management has become more challenging—and requires more IT resources to address—in the remote work era. As security leaders look to better address account takeovers, almost three-quarters (74%) agree that relying on passwords and traditional two-factor authentication (2FA) isn't enough. Due to the inadequacy of one-time authorization methods—like passwords and 2FA—90% of security executives agree that intelligent MFA would help them better protect company resources.

has securing access become a bigger challenge and/or require more resources since the mass work-from-home migration?

Are traditional passwords and two-factor authentication approaches no longer sufficient for securing user access?

Do you agree that a more advanced MFA tool that provides continuous, behavioral authentication would improve your company’s security posture?

Would your company be better protected from account takeovers if you had more visibility into user behavior post-authorization?

Data collected from August 14-September 4, 2020 Respondents: 100 Security executives Managing identity and access is harder than ever—and current tools aren’t cutting it. Most execs are increasing their investment in more advanced tools. Current tools aren’t providing enough visibility.

In addition to admitting traditional authentication is insufficient, most security executives (89%) do not feel they have sufficient visibility into a user’s behavior post-authorization. To better protect user accounts against compromise, 88% of respondents want more visibility post-authorization. To achieve a higher level of visibility into user behavior post-auth, 46% of security leaders are planning to implement intelligent MFA.

Of the security leaders who currently rely on intelligent MFA or plan to implement it, 85% are planning to increase their investment this year. The vast majority (81%) also plan to increase their spending on customer identity and access management in the next year.