okta Braxton-Grant TECHNOLOGIES

INNER CIRCLE CONVERSATIONS

Ten Steps along the journey to Zero Trust Security

As discussed in our recent Inner Circle Conversations, Zero Trust Security isn't a switch you can turn on; it's a journey. With *'never trust, always verify'* at the core of the strategy, it makes sense that the journey starts with identity. Organisations are creating detailed roadmaps to deliver a holistic approach to network security, that incorporate several different principles and technologies. Below we've highlighted ten steps along that journey, from the basecamp of fragmented identity to a peak of frictionless, secure access for employees, customers and partners. Where is your organisation on the journey to Zero Trust Security?

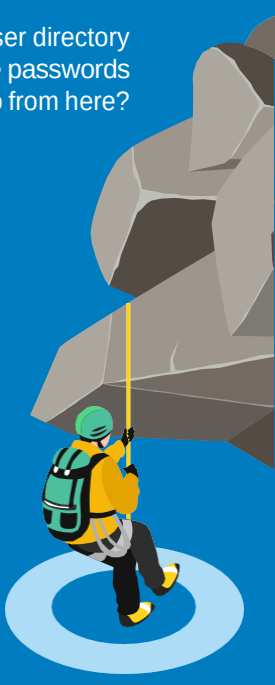
B Basecamp is packed with organisations without a unified user directory across all apps, little to no cloud integration and multiple passwords as the cornerstone to security. So, where do you go from here?

UNIFIED IAM

1 **Single sign-on across employees, contractors and partners.**

2 **Modern multi-factor authentication.** 44% of organisations have implemented MFA.[1]

3 **Unified policies across apps and servers.**



CONTEXTUAL ACCESS

The biggest barrier to getting here is provisioning.

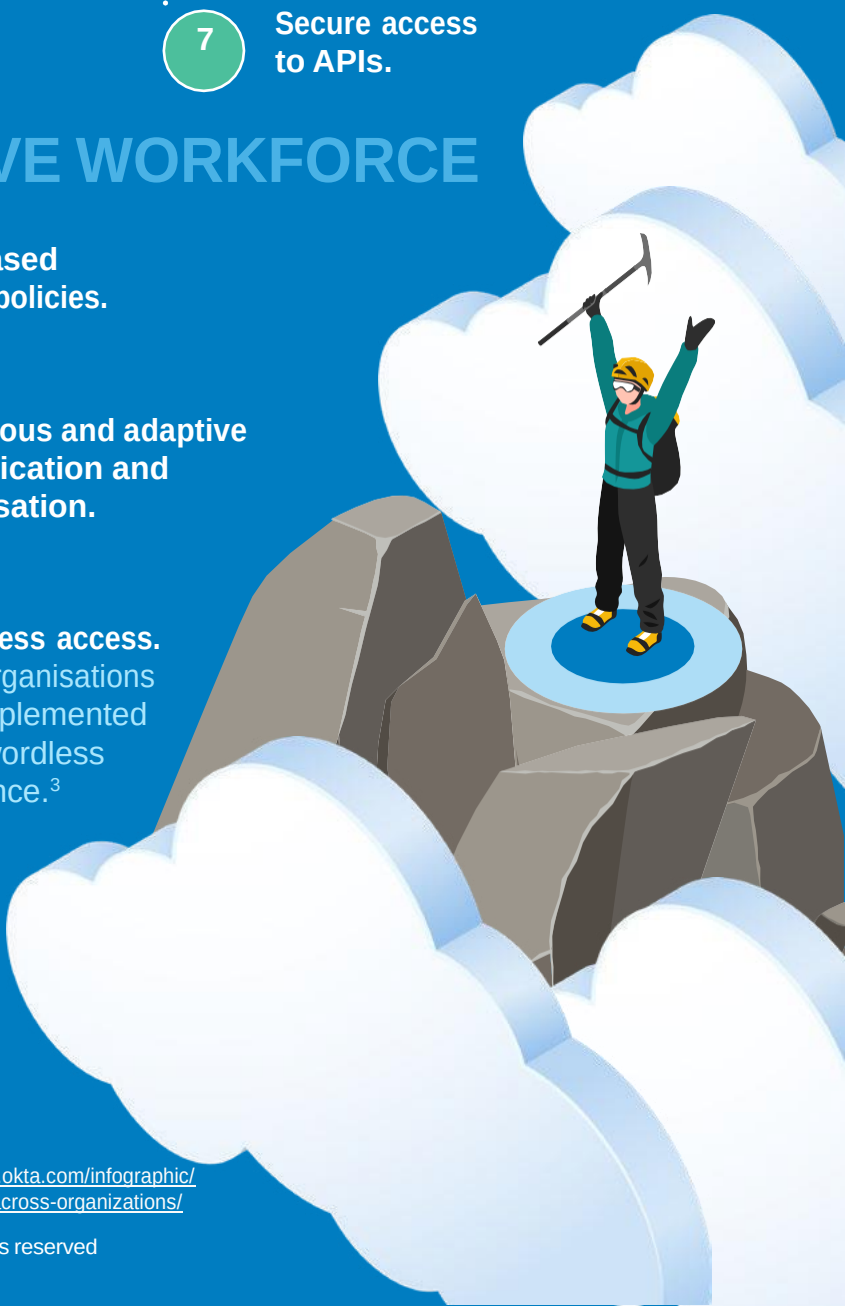
4 **Context-based access policies.**

5 **Multiple factors deployed across user groups.**

6 **Automated deprovisioning for leavers.** 18% of workforces have a fully automated provisioning/deprovisioning mechanism.[2]

7 **Secure access to APIs.**

ADAPTIVE WORKFORCE



8 **Risk-based access policies.**

9 **Continuous and adaptive authentication and authorisation.**

10 **Frictionless access.** 8% of organisations have implemented a passwordless experience.[3]

Looking for a more in depth view? Read the Okta Whitepaper on Zero Trust.

Source: 1,2,3: https://www.okta.com/infographic/the-maturity-of-zero-trust-across-organizations/