5 ways identity accelerates Zero Trust adoption

IT and security leaders are increasingly prioritising a Zero Trust security posture centered around identity and access management. Discover how it helps secure the hybrid workforce, futureproof against rising cyberthreats, and embrace cloud technology at scale.

99% of organisations globally say identity is important or critical to their Zero Trust security strategy
Source: The State of Zero Trust Security 2022, Okta

1 Streamlines digital transformation

As organisations accelerate their journeys into the cloud, providing secure access can be a long and arduous process. By leveraging a modern identity platform that provides out-the-box integrations with business-critical apps, IT leaders can quickly secure and deploy the tools and platforms employees need with minimal fuss.

97% of enterprise decision makers believe the pandemic sped up their company's digital transformation
Source: COVID-19 Digital Engagement Report, Twilio
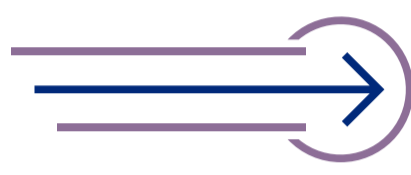
2 Secures the hybrid workforce

Employees today expect the freedom to work wherever they feel most comfortable and productive. By unifying access controls across all cloud and on-premises apps for every user, a modern identity solution ensures all users have instant, secure access to all the resources they need, when and where they need them.

89% of employees would prefer to work remotely at least some of the time
Source: PwC, Global Workforce Hopes and Fears Survey 2022

3 Mitigates the most common cyberthreats

In their haste to keep up with the demands of the remote and hybrid workforce, organisations often sacrificed security to maintain business continuity. By adopting modern identity tools like MFA and SSO, organisations can quickly eliminate password friction while strengthening resilience at the identity layer.

61% of cyberattacks in 2021 involved stolen or weak credentials
Source: 2022 Data Breach Investigations Report, Verizon

4 Hyper automates manual provisioning processes

While cloud technology can improve cyber resilience, deploying apps manually increases the risk of data breaches through human error. By hyper automating provisioning with identity, many of these risks disappear and IT teams can focus their attention on strengthening security elsewhere.

88% of data breaches in 2021 exploited credential data
Source: 'Why Do People Make Mistakes?', Tessian

5 Protects APIs as well as apps

As well as protecting apps, the right identity provider will also provide rich access controls to all technologies used by the workforce, including secure access to the APIs that are the building blocks of modern applications but can expose sensitive data to the web.

API attacks rose **681%** in the past 12 months
Source: State of API Security Report 2022, Salt

Where to begin on your Zero Trust Journey

If you want to know more about how identity can help accelerate your Zero Trust security ambitions, or if you're uncertain of what stage you're currently at on your Zero Trust journey and want to know where to go next, watch the video podcast with Brian Glick, Computer Weekly Editor in Chief, and Okta's Ian Lowe.