Almost all respondents (94%) are concerned that their organization will be breached or hacked as a result of credential theft or compromise. This is exacerbated by the rise in mobile endpoints within organizations, as most organizations reported to have, on average, two mobile endpoints per user and managing three sets of credentials per user.

On average, one out of every five (20%) IT support tickets are resulting from lost or forgotten usernames and passwords.

Over 50% already use two-factor authentication to secure external users’ access to resources, indicating the varied use of the technology.

As IT continues to look to two-factor authentication to deal with the credentials crunch, the vast majority (91%) of respondents are seeking to do this by managing their organization’s two-factor authentication centrally.

In an effort to overcome the security challenges around mobility, the majority of IT departments (90%) plan to implement two-factor authentication for access to cloud applications.

Currently, 38% of users use two-factor authentication, with over half (57%) expecting usage to rise in two years.

Almost all (92%) of respondents currently have at least one application protected by two-factor authentication, with cloud applications, web portals and VPNs among the top-three apps protected.

Two in five (41%) IT managers are already doing this by having the ability to implement uniform policies that address security threats in a consistent way. Two-factor authentication can at the same time streamline access to numerous applications.

The majority of organizations (90%) agree that managing two-factor authentication centrally can help monitor and reduce shadow IT in their organizations.