Techstrong Research

PulseMeter

Sponsored by

MENLO SECURITY

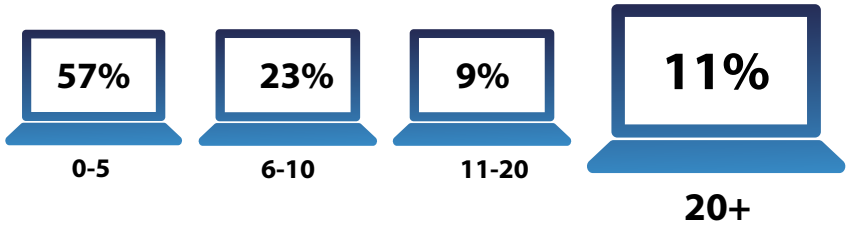
Security can't be a roadblock—employees need access to corporate apps and data without friction. How can you safely give employees and contractors access to core enterprise applications while staying secure? The challenge of securely providing access to enterprise applications has only become more complex with the increasing reality of "work from anywhere." While you need to make it easy for employees to quickly access critical applications, businesses also must make sure that only authorized individuals can access applications and data.

During the first two weeks of February 2022, our team conducted several flash polls among the Techstrong Group member community. Techstrong Group members include readers, influencers and contributors to our various communities focused on DevOps, cloud-native, security and our digital CxO community. The goal of these polls was to understand our members' evolving priorities around secure application access, especially in light of the changing workplace landscape and shifts in distributed workforces. Across all of the polls we received more than 725 responses.

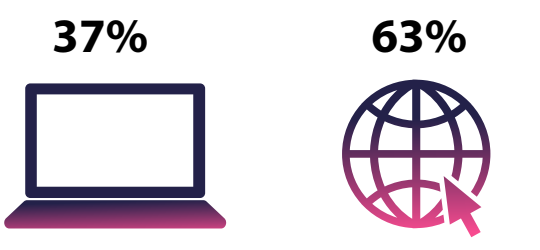
Accessing Corporate Applications

It's clear that employees must access web applications to get their job done effectively and efficiently. Nearly two out of five respondents reported needing access to six or more applications. The majority access these applications through a browser.

How many corporate applications (not productivity apps like Microsoft 365 or Google Workspace) do you need access to for your job?



How do you get access to your corporate applications?

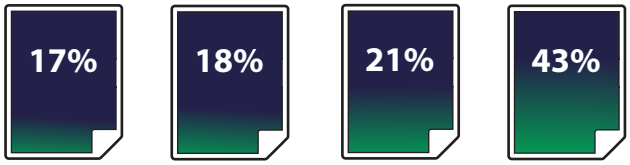


The Impact of Distributed Employees and Contractors

Although about one-third of participants reported that their applications are more secure since work-from-home policies became ubiquitous; more than one in five say it's less secure.

Are your remotely accessed applications more or less secure than before ubiquitous work from home?

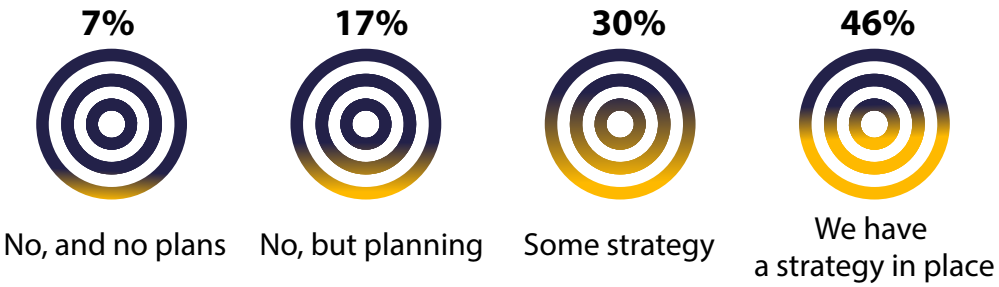
What percentage of your organization's corporate application access is by third parties or contractors?



Planning for secure access

Remote working isn't new, but many businesses still don't have a plan in place to provide easy, reliable access to corporate applications while preventing unauthorized access.

Do you have a security strategy for providing access to applications?



Techstrong Research Analyst View

Security teams need to walk a fine line between removing all friction in favor of easy access and locking everything down in the name of security and making it difficult for employees to get their job done. Remote access to corporate web applications isn't a new challenge. For decades, VPNs have been used to give distributed workers access to corporate applications.

However, VPNs were never designed for today's world in which it's not uncommon for businesses to have 90% or more of their workforce remote. In addition, VPNs tend to be overly permissive and don't allow an organization to tailor access to specific individuals.

For this reason, organizations are looking at new approaches to give employees remote access to applications, data and services based on clearly defined access control policies—either for a specific role or for an individual employee.