7 Reasons Hybrid Work is Driving IT to Ditch VPN

For Remote Desktops and Zero Trust Access

hp teradici.

Teradici surveyed more than 8,000 respondents across a range of industries about the security challenges related to remote work. Teradici published the results in a report, **"Corporate Cybersecurity Report – Securing the Hybrid Workplace in 2022 and Beyond."** The following seven factors will influence IT teams as they look to increase security for hybrid work models.

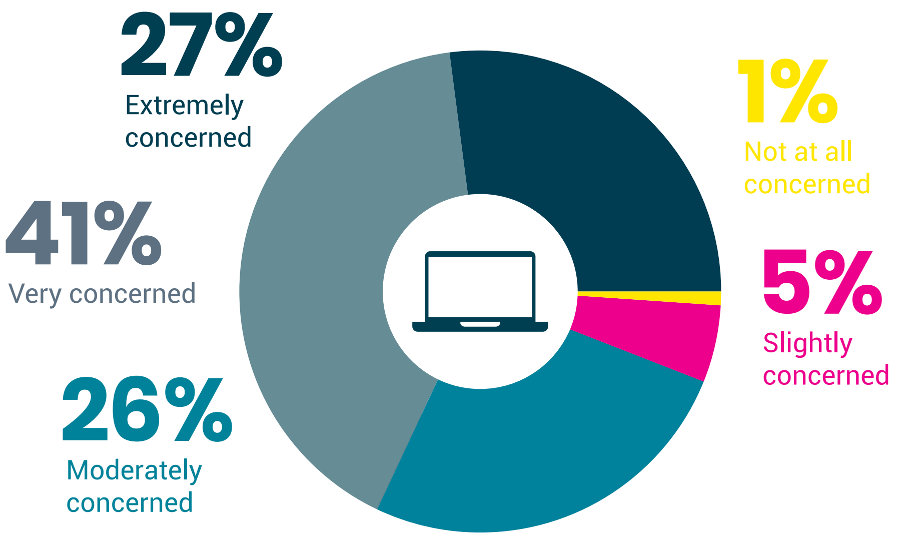
1 Hybrid work is here to stay

99% of respondents reported their companies will have a hybrid workforce

Nearly 40% of respondents expect more than half of their workforce to operate remotely at least twice a week post-pandemic

2 Endpoint security is keeping IT leaders up at night

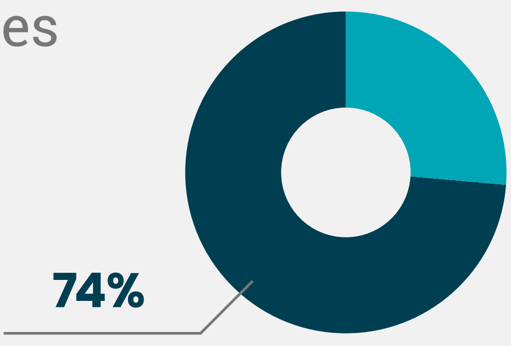
94% of respondents indicated their companies are concerned about the security of corporate data exposed via home-based devices



3 BYOD use continues to rise significantly, increasing the risk of data breaches

Only 10% of employees are predominantly using corporate-owned devices at home; the rest are using a mix of BYOD and corporate devices (42%); or predominantly BYOD (48%)

74% of respondents report they expect more use of BYOD



4 VPNs have been a challenge

For respondents whose companies use VPN technology to home-based endpoints, 75% reported user complaints about slow performance or disconnects that can impact productivity

33% High level of user complaints about slow performance or disconnects

42% Moderate user complaints about slow performance or disconnects

22% Few user complaints about slow performance or disconnects

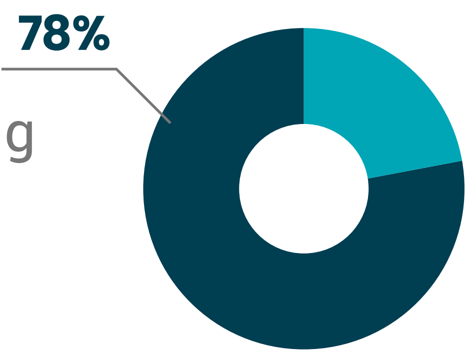
3% We don't deploy VPN client technology on employee devices

5 The majority of respondents are currently using remote desktop technology or DaaS (55%) as their primary method of mitigating corporate data exposure, compared with VPN (41%)

DaaS **55%**

VPN **41%**

6 78% of respondents are currently implementing Zero Trust or planning to in the next two years



7 Trusted endpoints are a priority for 97% of respondents. Continuous verification of endpoints is important to 95% of them.

53% Important for all users

42% Important for a few users

User and device authentication and continuous authorization of devices are critical for end-to-end Zero Trust posture. For more info and to read the full report, visit: www.teradici.com/security-report