CORPORATE CYBERSECURITY REPORT:

Securing the Hybrid Workplace in 2022 and Beyond

New survey finds companies are turning away from VPN in favor of remote desktops and Zero Trust Architectures as hybrid workplaces become the new norm

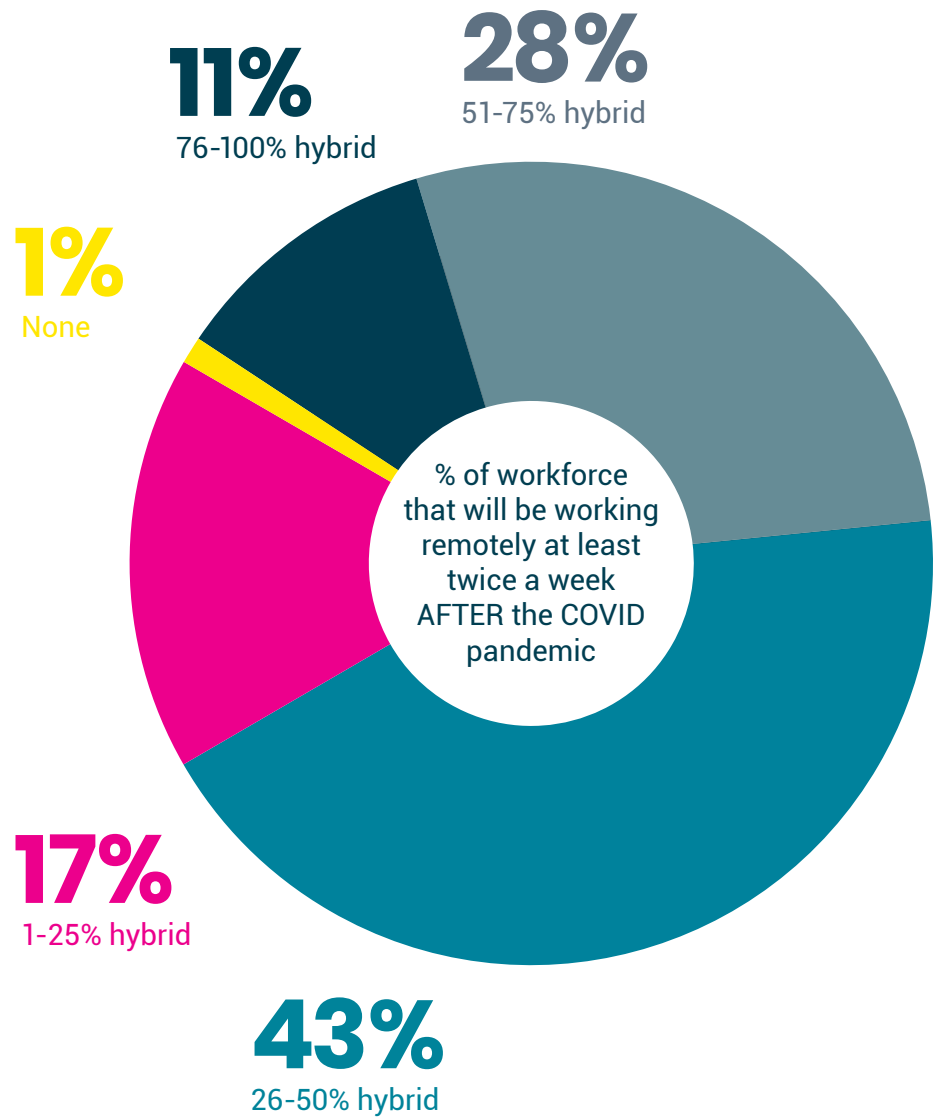
hp teradici

When organizations abruptly shifted to remote work at the start of the global COVID-19 pandemic, they had to scale their network and security capabilities quickly. That meant snap decisions for many companies, deploying more of what they were already using, likely taking some shortcuts that left optimizing security and user experience for another day.

A new survey from Teradici polled more than 8,000 people across a range of industries, including Education (16%), Finance (24%), Healthcare (15%), Military & Government (19%), Media & Entertainment (14%) and Technology & IT (11%) and found that hybrid workplaces are the new norm—that message was loud and clear in the survey results, with 99% of respondents reporting their companies will have hybrid workforces post-pandemic. Nearly 40% expect more than half of their workforce will work remotely at least twice a week. And this is consistent across all sectors, even the more traditional in-office industries see a hybrid future.

Unsurprisingly, this abrupt shift to working from home left significant technology gaps and, as companies look ahead 2-3 years at the hybrid work future, they are turning away from VPN in favor of remote desktops and Zero Trust Architectures to secure their hybrid infrastructure.

This report highlights some of the key security challenges that were uncovered as companies moved to remote work, as well as how they plan to increase security as hybrid work models mature and become the norm.



Definitions

Zero Trust

Zero Trust is a strategy (and bundle of technologies) that replaces traditional perimeter-based security with a model focused on users, devices, applications, and assets. Extending trust principles beyond mere network access goes a long way to improving enterprise security. By forcing users and devices to authenticate themselves continuously and limiting resource access to only the files and data they need for the given task, users and devices are less vulnerable to hackers.

Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) have been in use for decades. They provide an encrypted "tunnel" between the corporate network and the user's device. Data is encrypted and downloaded to a user's device where it is processed by a local application. The user typically has the same access to services and files as if they were working from the office but uses local hardware to run the applications.

Desktop as a Service (DaaS)

Desktop as a Service (DaaS), also known as cloud-hosted virtual desktops, is a desktop virtualization technology enabled by cloud computing. These virtual environments can be accessed from anywhere. All the user requires is an internet connection to log in.

Zero Trust vs. VPN vs. DaaS

VPN: VPNs use a "castle and moat" security model. All the protection is on the perimeter; once users are authenticated, they have broad access. Companies have to set up a VPN server to run on the local network, as well as a VPN client software, which needs to be installed on endpoint devices for users to access the VPN.

Zero Trust: Aptly named, the network trusts no device, user or transaction. Users are not provided blanket access to applications, services, and files, they can only access the resources needed for a given task or function. Even within the company network, devices undergo verification and authentication checks at several points before accessing company data.

DaaS: DaaS is a desktop service that is hosted in the cloud by a company like Amazon or Microsoft. With DaaS, all of the hardware and security is managed by the provider, so companies don't have to do it themselves.

Endpoint security

Endpoint security is an approach to the protection of user- and corporate-supplied devices that are remotely bridged onto a corporate network. The connection of endpoint devices, such as laptops, tablets, mobile phones, IoT devices, and other wireless devices to corporate networks creates attack surfaces for security threats.

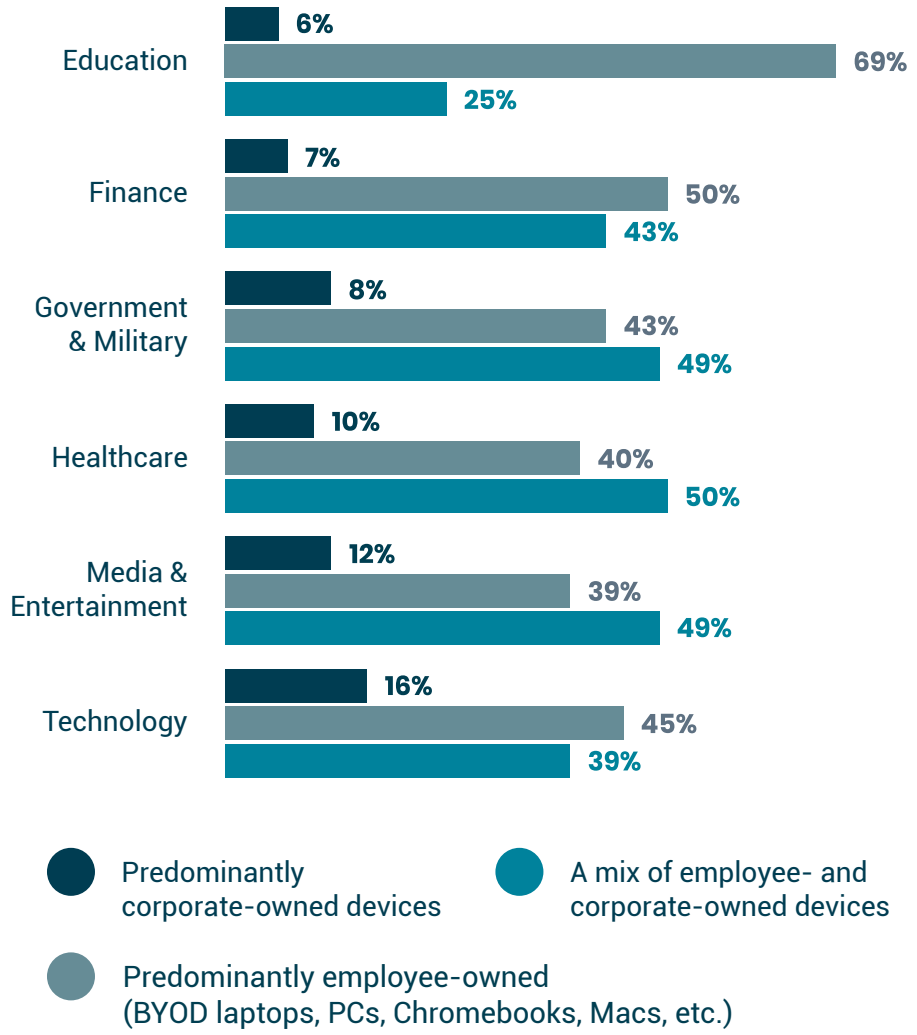
Looking Beyond Pandemic Response to a Hybrid Reality

With the shift to hybrid working models, we asked respondents how concerned their companies are about unmanaged endpoints and how they plan to increase remote work security. The following trends and challenges emerged:

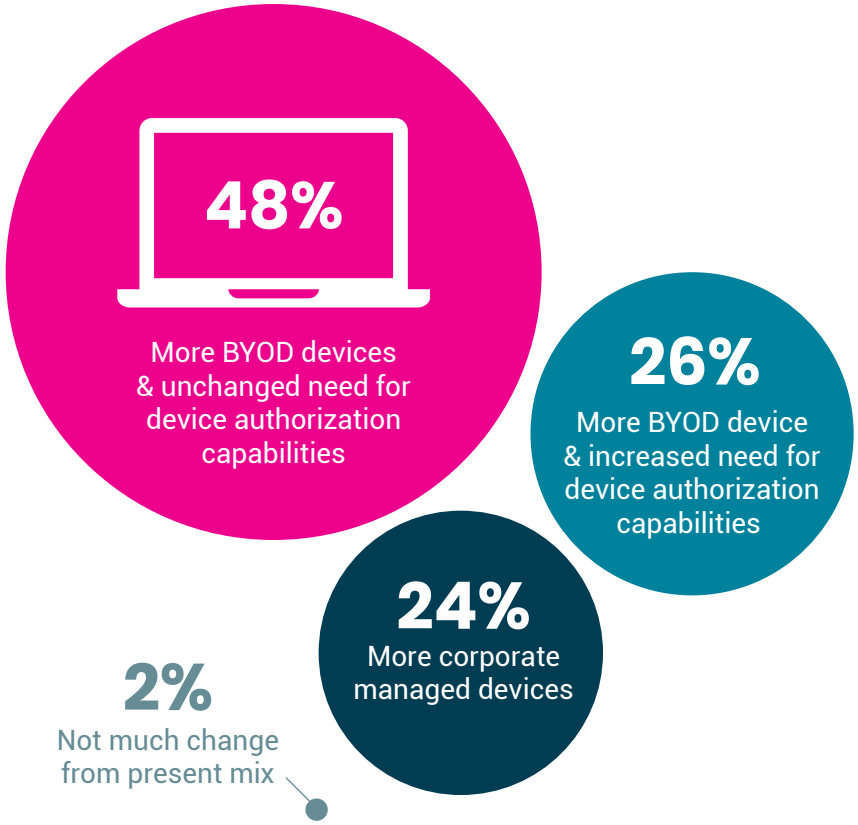
BYOD—Securing Consumer Devices

BYOD, or bring your own device, has its advantages—it's popular with employees, helps with productivity and reduces operating costs, among other benefits—but companies have little control over any corporate data stored on employee devices or accessed via employee devices, nor with non-corporate applications or other applications stored on employee devices. Employees' personal devices are not only connected to the corporate network, but some may also have corporate data stored on them. If an employee forgets to install a security update, or the device is lost or stolen, they could inadvertently put company data at risk.

Asked what type of devices at-home employees are currently using, respondents reported 90% are using a mix of employee- and corporate-owned devices (42%) or predominantly employee-owned devices (BYOD laptops, Chromebooks, Macs, etc.) (48%). Only 10% are predominantly using corporate-owned devices. Use of corporate-owned devices was highest in Media & Entertainment (12%) and Technology & IT (16%) sectors and lowest in Education, with only 6% on corporate-owned devices and the highest proportion among all sectors predominantly using BYOD (69%).

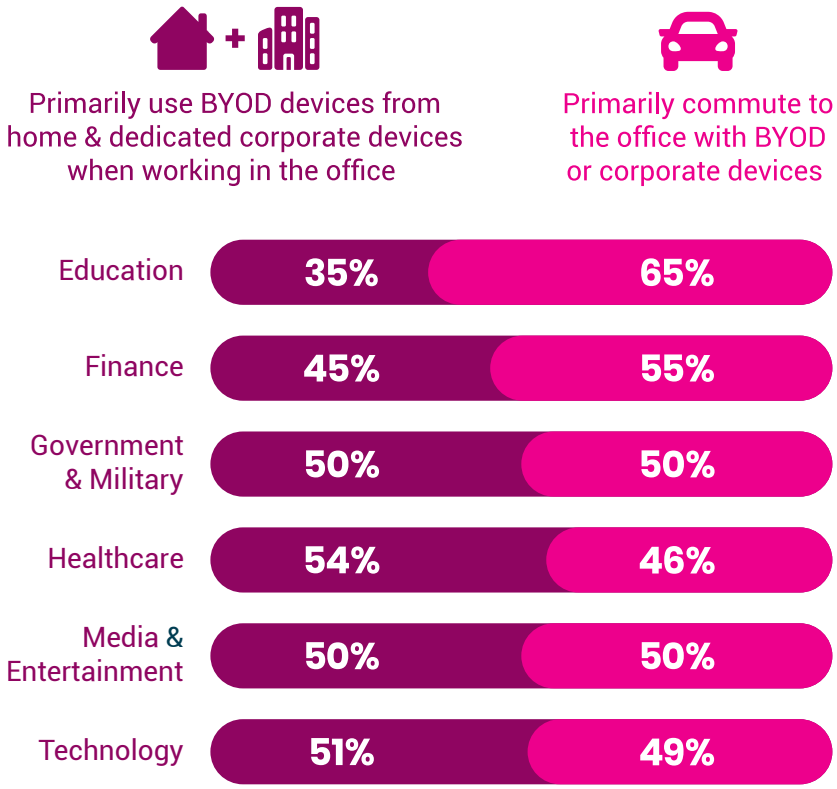


Survey responses indicate that this shift to BYOD devices will continue post-pandemic, with 74% of respondents reporting they expect more use of BYOD, and nearly 25% seeing increased need for device authorization.



Taking a closer look at industries, Military & Government, as well as Healthcare are expecting a more significant shift, with 82% foreseeing increased BYOD use vs. corporate-managed devices. The Education sector was somewhat different, with 45% expecting more corporate managed devices, vs. 54% BYOD.

In terms of how employees will use their devices once they are back in the office, there was nearly an even split between employees primarily using BYOD devices from home and dedicated corporate devices when working in the office (47%), and employees primarily commuting to the office with BYOD or corporate devices (53%).



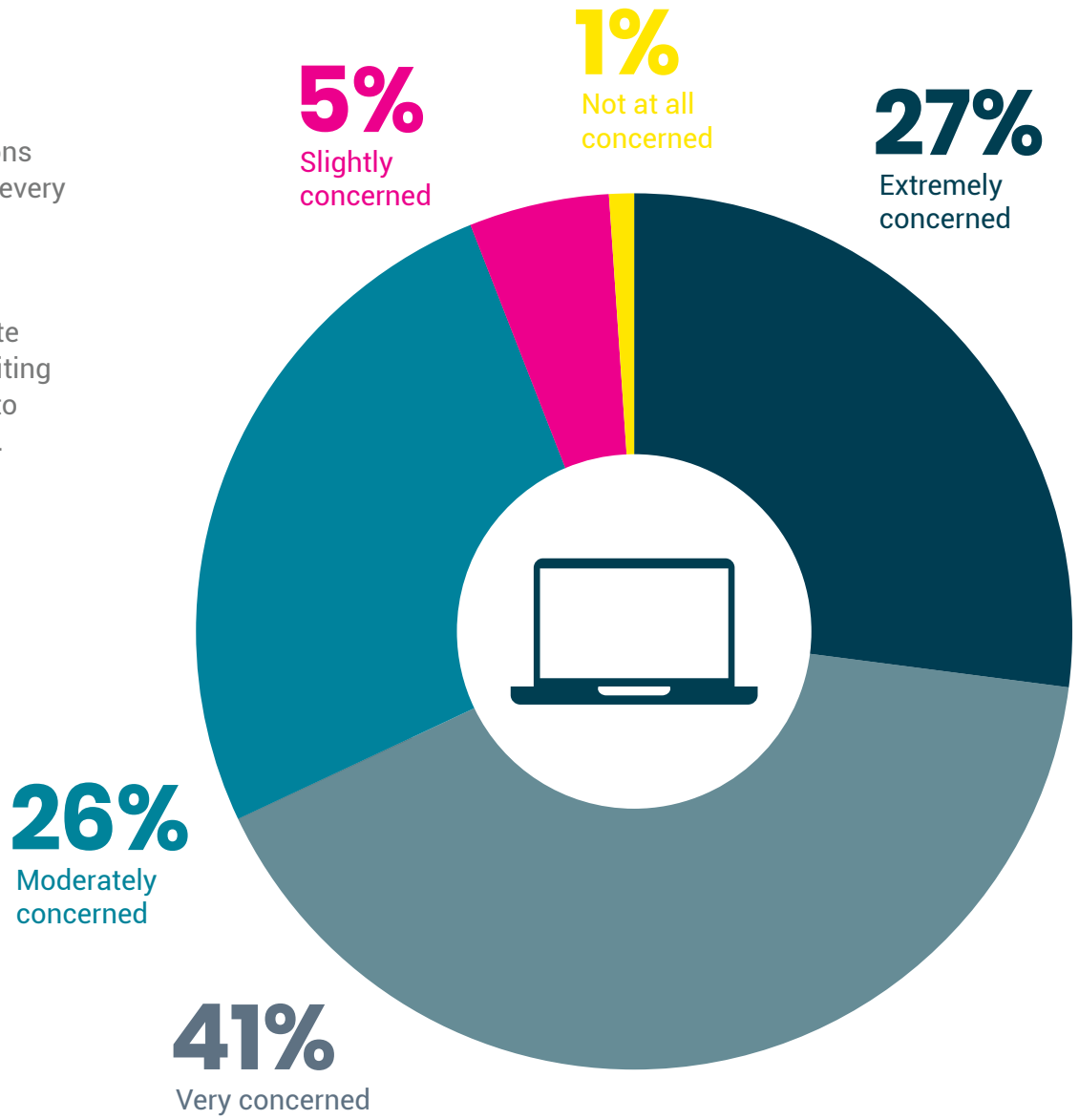
This relatively even split was consistent across all industries, except for Education, where respondents expected a higher proportion will commute with devices (65%) rather than using separate devices when working at home and in the office (35%).

Endpoint Security is Keeping IT Leaders up at Night

Cyberattacks are a major threat to an organization's operations and reputation. With millions of people affected by breaches every year, it's no surprise that endpoint security is a top concern for IT leaders.

The importance of endpoint security, which protects corporate data stored on endpoints and prevents endpoints from exploiting vulnerabilities or introducing malicious code while attached to corporate networks, has only increased during the pandemic.

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

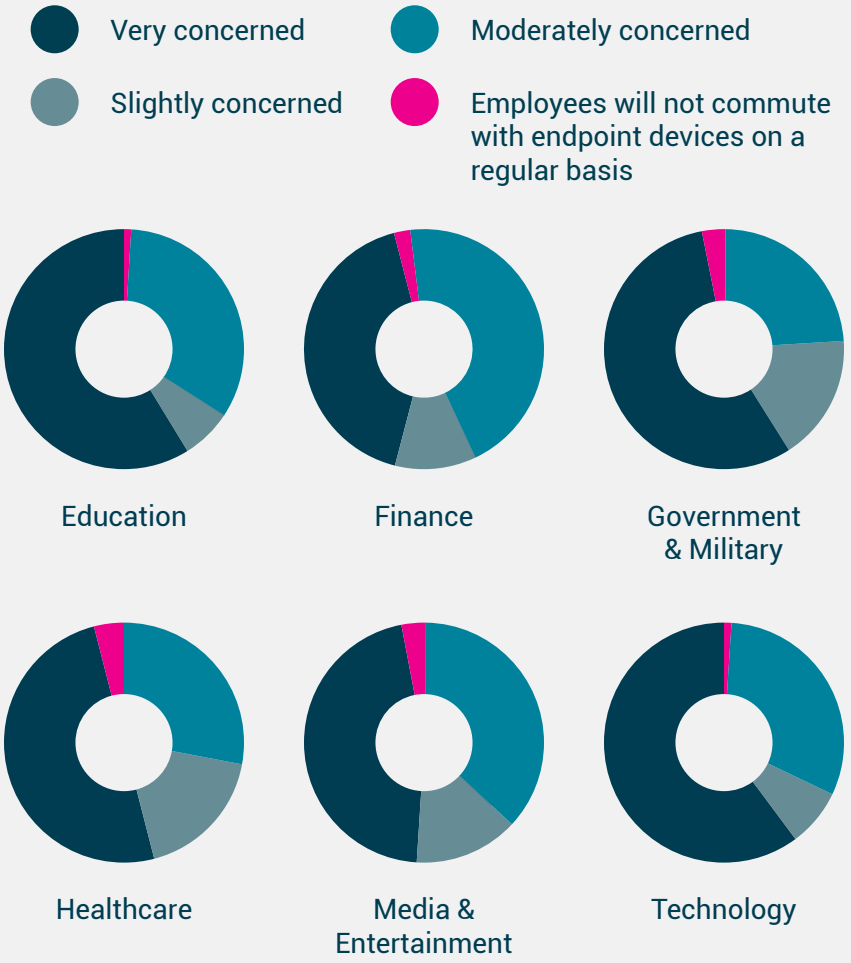


Concern is highest among respondents in the Education sector, with 81% reporting they are either 'extremely concerned' (47%) or 'very concerned' (34%), which may correlate to the higher number of employees using BYOD and commuting with their devices.

As noted in the previous section, 53% of respondents plan to enable employees to commute with endpoint devices, and this is a hot button of concern for IT. 98% of respondents are concerned about security and/or data integrity as a result of employees commuting with endpoint devices. Concern is highest in the Technology & IT sector, with 60% reporting they are 'very concerned', as well as in the Education sector (59%).

When employee devices are unmanaged, concern rises to red-alert levels—94% of respondents reported they are more concerned. Respondents in the Education sector where more likely to be 'much more concerned' (60%), and those in Military & Government (59%) and Healthcare (60%) were more likely to be 'slightly more concerned' about unmanaged devices.

Concern with security and data integrity as a result of employees commuting with endpoint devices



Acceleration of Zero Trust Adoption

At the end of 2019, Gartner® made the bold prediction that:

"By 2023 60% of enterprises will phase out VPNs in favor of Zero Trust access."

Survey respondents not only agreed (37%), a further 38% anticipate that new workplace flexibility requirements spurred by hybrid work will accelerate Zero Trust adoption even faster. 18% believe Zero Trust adoption will take longer than Gartner predicts, and only six percent think that VPNs will not be phased out to such an extent.

37% I agree with the Gartner prediction

38% The unanticipated recent need for workplace flexibility will accelerate the adoption of Zero Trust access even faster than Gartner predicts

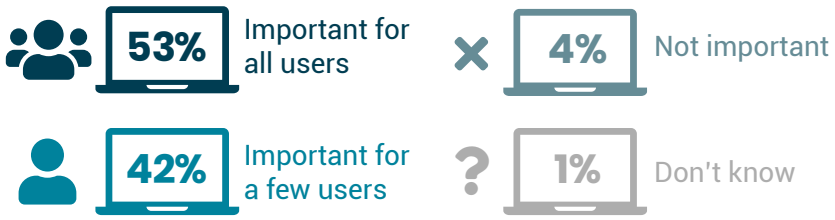
18% Zero Trust access adoption will take longer than Gartner predicts

6% Enterprises will not phase out VPNs to such an extent

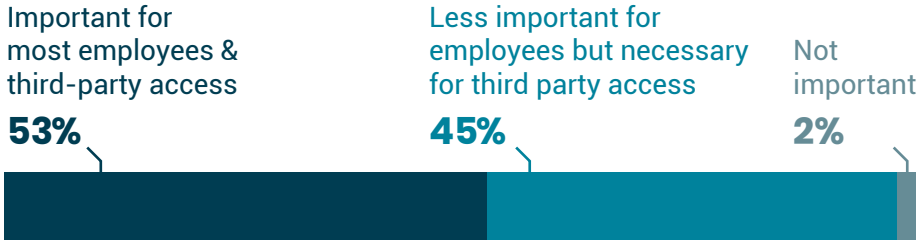
1% Don't know

The survey also indicates the shift to Zero Trust Architecture models is well underway, with 78% of respondents currently implementing or planning to in next two years. A further 19% are planning to implement but are unsure when. Only two percent have no plans to implement a Zero Trust model. Zero Trust adoption is highest in the Finance (85%) and Education (84%) sectors, and lower in Media & Entertainment and Healthcare (both 73%).

The bottom line is that Zero Trust-based endpoint management is a priority for 97% of respondents. Further, 95% of respondents contend that continuous verification of BOTH endpoint devices AND users is important.



Granular control over endpoint device authorization, such as location, time-limited access, or network properties (Wi-Fi/wired), is a necessary measure. 53% reported this is important for most employees and third parties, such as temporary workers and contractors, and 45% reported it's less important for employees but necessary for third party access. Only 2% believe granular control is not important.

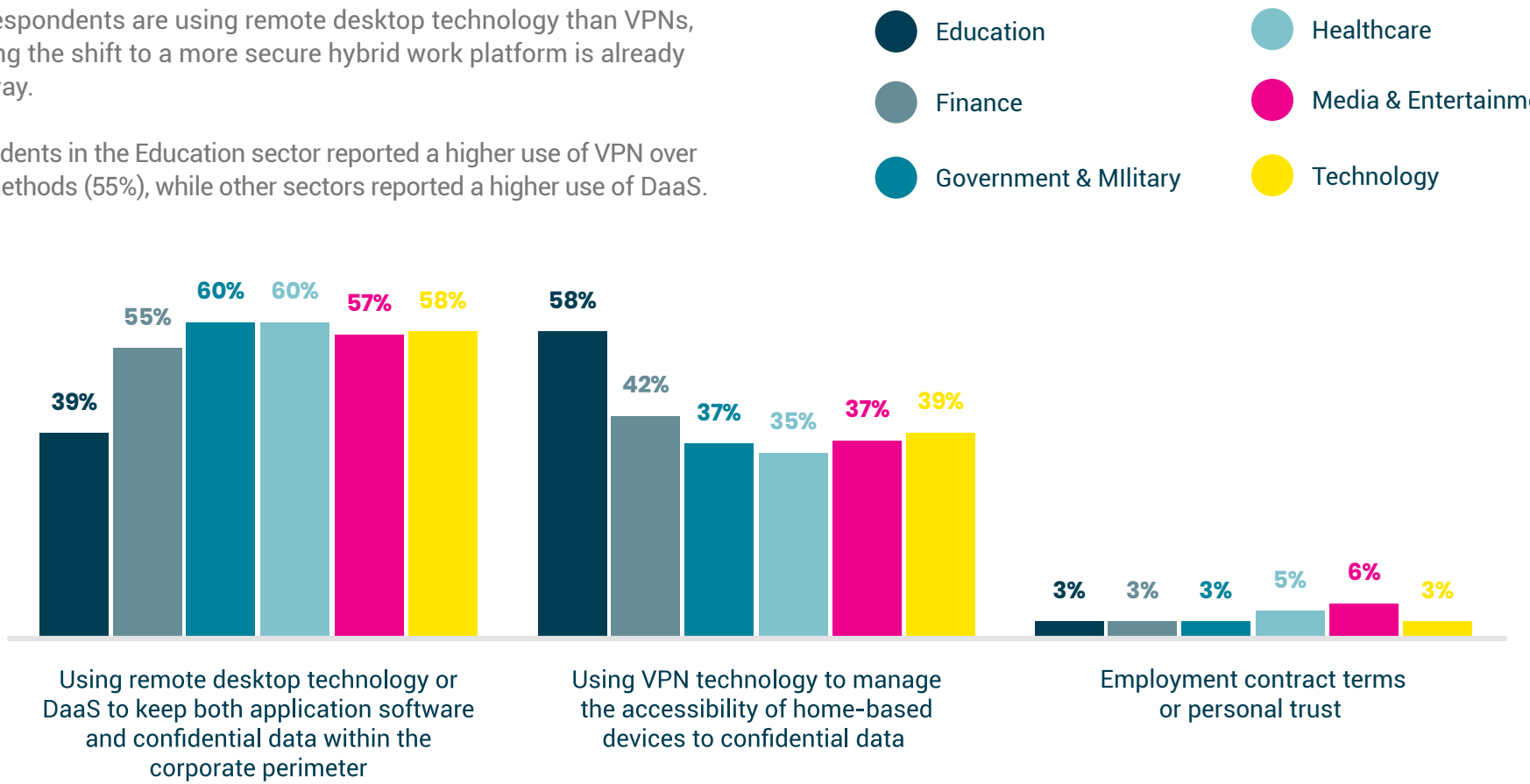


Goodnight Traditional VPN

When asked about their company's primary method of mitigating corporate data exposure via home-based devices, 41% said their companies currently rely on VPN technology, 55% are using remote desktop technology, or DaaS to keep both application software and confidential data within the corporate perimeter, and 4% are using employment contract terms or personal trust.

More respondents are using remote desktop technology than VPNs, signaling the shift to a more secure hybrid work platform is already underway.

Respondents in the Education sector reported a higher use of VPN over other methods (55%), while other sectors reported a higher use of DaaS.



In companies that are using remote desktop technology or DaaS, respondents report they are predominantly deploying managed thin clients or zero clients (using thin client vendor tools or Teradici Management Console) for their employee devices (58%), compared with managed PCs using corporate tools over a VPN (29%), or IoT device management tools, such as Intel AMT/EMA, Microsoft Intune, etc. (8%). Of this group, 5% report their devices are predominantly unmanaged.

Rated performance of VPN technology to home-based endpoints

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

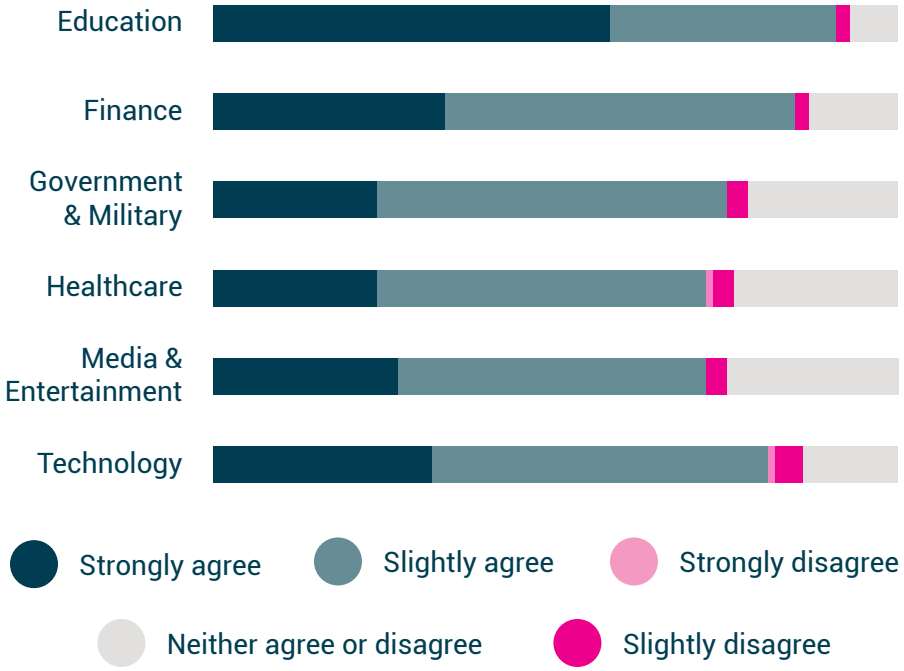
3%

We don't deploy VPN client technology on employee devices

For respondents whose companies use VPN technology to home-based endpoints, 75% reported user complaints about slow performance or disconnects that can impact productivity. Respondents in Government & Military (83%) and Education (80%) reported the highest levels of dissatisfaction.

Throughout the shift to remote work, relying on VPNs has been a challenge for 81% of respondents. Those in Education (91%), Finance (85%) and Technology & IT (81%) reported the highest level of challenges.

Relying on VPNs has been a challenge...



Looking to the future, only 3% of respondents will be relying to VPN as the primary user authentication method for corporate services and remote desktops in 2 to 3 years. Cloud (e.g. Okta, Google and Microsoft Azure AD) and on-premises (e.g. Microsoft ADFS) identity services are taking over, according to 80% of respondents, with traditional VDI connection managers remaining primary for 17%.

Looking ahead 2 to 3 years, the primary user authentication method for corporate services and remote desktops will...

46%

Authenticate from the endpoint against a federated on-premises identity service (e.g. Microsoft ADFS)

17%

Continue to authenticate against traditional (non-federated) directory services (e.g. LDAP) via VDI connection managers

34%

Authenticate from the endpoint against a federated cloud identity service (e.g. Okta, Google, Azure AD)

3%

Continue to authenticate against traditional directory services (e.g. LDAP) over a VPN

hp teradici

What Does The Future Hold?

As companies embrace the opportunities that come with hybrid work, what should CSOs and IT teams prioritize in order to protect corporate assets and enable a productive, secure and reliable experience for workers? Survey results indicate:

- Hybrid work is here for the long term, and you need a security architecture that covers both in-office and remote access requirements. Don't just plan a security architecture for remote access; now is the time to consider in-office changes as well.
- Use of BYOD will continue to rise significantly, increasing the risk of data breaches. Security infrastructure and employee training need to function in tandem.
- VPN will be replaced by remote access and Zero Trust—it's not if, it's when, and it's happening already. The increased use of remote desktop technology and widespread implementation of Zero Trust Architecture models reported in the survey indicates the shift to a more secure hybrid work platform is already underway. Zero Trust incorporated into secure remote access is a clear next step.
- Besides the need for both user and device authentication, continuous authorization of devices will be critical to an end-to-end Zero Trust posture.

The vendor community has a major role to play, providing products with features that fit the Zero Trust Architecture (ZTA). If you're familiar with the data-plane requirements for ZTA and PCoIP® technology, you'll already know that features such as Multi-Factor Authentication (MFA) in Teradici CAS are prerequisites to enabling user access controls. However, under ZTA, PCoIP endpoints also require device access controls, and Teradici is working on these capabilities for PCoIP Zero Clients, Thin Clients and Teradici CAS Windows/macOS/Linux clients. Keep in touch to find out more.

Consider Teradici CAS

Teradici CAS remoting software helps keep content and data secure in your data center, no matter what kind of endpoints your employees are using and no matter where they are.

Based on our secure PCoIP remote display protocol that connects more than 15 million endpoints around the globe, no data or business information leaves the safety of the corporate network. With PCoIP technology, only display information in the form of fully encrypted pixels are transferred to the remote endpoint, and with Multi-Factor Authentication, only the right users can connect.

This is why IT administrators from government agencies, media conglomerates, production studios, financial firms and design houses trust Teradici to support their need for secure, high-performance virtual desktops and workstations delivered from private data centers, public clouds, or any combination of both.

You will love the experience too.

Problem	Consider Teradici CAS
Employees using consumer-grade devices at home	Even consumer devices remain secure with Teradici CAS, no corporate data ever goes to these endpoints
Unmanaged endpoints & commuting with unmanaged endpoints	Using the Teradici PCoIP remote display protocol to transfer only pixels, no corporate data needs to be on the device. Corporate assets remain securely located in industry-compliant, on-site or public cloud storage networks.
Bring your own device (BYOD)	IT administrators have complete control of their infrastructure to choose any cloud, data center, endpoint, OS, and application combination.

Survey Methodology

Teradici surveyed 8,392 respondents from Argentina, Australia, Brazil, Canada, China, Croatia, Egypt, England, Estonia, Germany, Greece, Hong Kong, Hungary, India, Italy, Japan, Malaysia, Malawi, Mexico, Myanmar, the Netherlands, New Zealand, Portugal, Scotland, Singapore, Spain, Sweden, Switzerland, Uruguay and the United States, across a range of industries from July 12 to August 15, 2021.

About Teradici

Teradici, an HP company, is the creator of the PCoIP remote display protocol, which delivers desktops and workstations from the data center or public cloud to end users with the highest levels of security, responsiveness, and fidelity. Teradici CAS, which won an Engineering Emmy® from the Television Academy in 2020, powers the most secure remote solutions with unparalleled performance for even the most graphics-intensive applications. Teradici technology is trusted by leading media companies, design houses, financial firms and government agencies and is deployed to more than 15 million users worldwide.

For more information, visit: www.teradici.com.

hp teradici