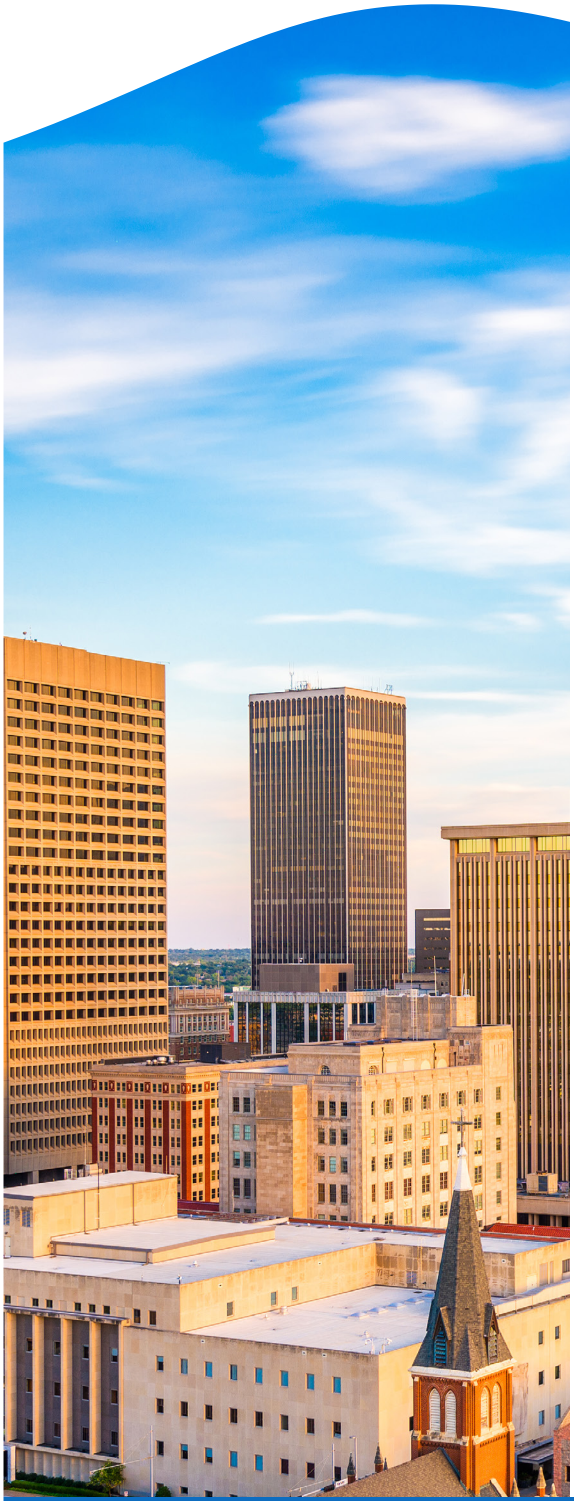

Top 5 Considerations When Choosing a Remote Access Solution for Your Hybrid Workforce

splashtop®

When COVID-19 hit, IT scrambled to support employees who quickly moved from an office environment to remote working. Post-pandemic, that trend is here to stay. The rise of the hybrid workforce—a new blend of both remote and on-site employees, is top of mind for most organizations.

Remote work has become a must, not a choice. With 68% preferring a hybrid workplace model even after the pandemic ends, employees expect their employers to offer remote work options, even if it's just a few days per week.

Hybrid Work Creates New Issues for IT

Not offering hybrid work options can present a real risk, as companies could lose top talent to companies who offer hybrid environments. Up to 42% of employees would look for a different job if their employer refused to offer remote work options long term. At the same time, hybrid work models create massive pressure on IT to have the right technology in place to ensure performance, availability, and security.

Hybrid workforces amplify BYOD (bring your own device) issues when employees use their own laptops and mobile devices to access corporate information. And this isn't an uncommon practice: two out of three employees use their personal devices at work, regardless of their employer's BYOD policies, which increases security exposure especially with VPNs.

Remote Access Solutions are Key to Productive Remote Work

In a hybrid workplace, employees must have the right tools to work from any location, but technology solutions often fall short. A recent O2 Business survey reports that 42% of respondents don't have access to all the work systems needed to do their jobs which impacts productivity and job satisfaction.

Organizations need a reliable, fast, and secure solution that lets hybrid workers securely access key computing resources. For companies with these requirements, remote access solutions are setting a new trend.

Remote access solutions support hybrid work by:

- Connecting employees to their work computers when they're not at the office.
- Enabling IT to support computers and mobile devices remotely to troubleshoot, diagnose, and fix issues.
- Leveraging existing computing resources and giving users more flexibility in accessing them.
- Ensuring business continuity.
- Improving security, performance, and scalability vs. traditional VPN solutions which fall short in those areas.

42%

of respondents don't have access to all the work systems needed to do their jobs.

68%

prefer a hybrid workplace model even after the pandemic ends.

splashtop®

TOP 5 Considerations When Choosing a Remote Access Solution

When you're evaluating remote access solutions, be sure to look for these five key characteristics.

#1: Fast performance and dependable reliability

A remote access solution must work from anywhere regardless of whether the user is at home, the airport, Starbucks®, or another location. It needs to support fast connections for common business tasks such as video calls, file downloads, and corporate applications to eliminate user frustration and ensure high productivity.

Additionally, some users need access to specialized solutions like 3D modeling and video editing software. Fast remote connections are critical for those users who need to run these applications on their remote computers.

A remote access solution also needs to be reliable and work consistently (many remote access solutions struggle in this area), which helps eliminate support tickets and ensure enthusiastic end user adoption.

VPN is often a traditional fallback for remote access, but it has many weaknesses. It's often expensive, tedious to set up and maintain, and difficult to scale. VPN usually has numerous security holes, offers poor performance, and is cumbersome for employees to use—especially if they're utilizing their own devices.

A modern remote access solution should:

- **Maintain high-performance** speed on any device even for resource-intensive tasks like video editing, 3D drawings, and more.
- **Be consistently reliable**— downtime isn't an option.
- **Eliminate lag** when supporting remote users, wherever they're located.

How IT Teams Use Remote Access Solutions

- Access end users' computers and mobile devices to troubleshoot and resolve issues.
- Manage and monitor corporate computers to ensure they're up-to-date.
- Ensure company data is protected while keeping remote employees productive.
- Give remote employees access to their work computers.
- Remotely control computers over fast connections with HD quality and sound.
- Eliminate manual steps of logging into multiple systems to manage issues through seamless integrations with helpdesk ticketing, ITSM and PSA solutions.

splashtop®

#2: Simple for IT to set up, manage, and scale

Your IT team is likely busy solving issues and supporting remote users; they don't need to babysit a remote access solution. Solutions should be straightforward, quick to deploy and require minimal maintenance.

A remote access solution should have functionality that makes IT's job easier, including:

- **Easy-to-use administration console** that makes managing users, devices, and settings simple.
- **Scales quickly** to support thousands of users and work consistently so productivity isn't impacted and business continuity is maintained.
- **Integrate with other popular IT tools** such as help desk ticketing, ITSM (IT Service Management), and PSA (Professional Services Automation) solutions to minimize the amount of manual work IT needs to perform and increase their productivity.

#3: Easy and intuitive for end users

End users have a few requirements for new software: it needs to work—every single time—while being easy and intuitive to use. A reliable solution ensures that it is used consistently; otherwise, employees may look for alternate solutions (which can increase issues and result in security holes).

The ideal solution is also so simple that it doesn't require training which eliminates the need for IT to set up and run training sessions while boosting end-user adoption.

Be sure to ask the vendor if their solution supports:

- File transfer, chat, multi-monitor support, remote reboots, and sharing desktops.
- Multiple operating systems and devices, including Windows, Mac, iOS, Android, and Chromebooks. This type of broad support is critical so employees can use their own computers, tablets, or phones.

How Hybrid Workforces Use Remote Access Solutions

- To remotely access work PCs, Macs and connected hardware, such as extended storage, from a laptop or mobile device.
- Access corporate applications that can't be installed locally such as those for reporting, video editing, billing and invoicing, ERP, and CAD software.
- Access confidential client and/or patient data.

"I just wanted to send my appreciation to you and your wonderful support team for getting us sorted out with Splashtop… everyone at Splashtop has been excellent in guiding me through the setup of the system! I have to say that the customer support for this product is the best I have ever experienced."

Rick Campion
Technical Operations Manager
Music Department at Goldsmiths
University of London

"Splashtop utilizes stringent security procedures that keeps our remote sessions and data secure."

Jake Harrelson
Patient Navigator
Home Farm Family Medicine
Read the case study.

24/5
customer support

300+
million customers

2000+
five star reviews

splashtop®

#4: Top-notch security

Many security policies are built around the assumption that users will access data from an organization's physical location, which isn't compatible with the new world of hybrid work. To safeguard against breaches, you'll need a remote access solution with strong security for corporate data, devices, and your network.

Look for these security features:

- **Authorization and authentication** should take place each time users and devices log in and connections need to be encrypted.
- **Access permissions need to be manageable at the granular level** to ensure secure and streamlined IT practices and reduce manual work.
- **Comprehensive logs** for auditing and compliance.
- **SSO (single sign-on) integration** eliminates the need for your IT team to manage multiple user accounts. SSO makes it easier to know who is connecting and to manage those connections.

#5: World-class customer support

As an IT pro, you understand how important it is to provide timely and effective support, and be easily accessible to end users. A remote access vendor needs to give you the same level of service with quick, real-time support.

Be sure to ask these questions to evaluate a vendor's customer service:

- Do you offer 24/5 live support?
- Do you offer different channels of support via email, ticket, chat, and phone?
- How much attention can you give my business?
- Do you have references I can speak with?
- Are your customer reviews, such as G2, consistently positive?

Take the next step!

When you're narrowing down your options for a remote access solution, consider Splashtop Enterprise. Splashtop offers an all-in-one solution, so hybrid workforces can remotely access corporate resources and IT teams can support them. It also provides the performance, security, flexibility, and control that organizations need to support their growing businesses.

Splashtop is trusted by Toyota, AT&T, State Farm, UPS, Harvard University, Target, OSF Healthcare, S&P Global, and over 200,000 businesses and government agencies.

G2 reviews rate Splashtop as having the Best Relationship, Best Usability, Easiest to Use, and Easiest to Admin.

Learn more about how Splashtop Enterprise can help you easily support your hybrid workforce.

[1] Pulse of the American Worker Survey, Prudential.
[2] The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits, DataInsider, November 24, 2020.
[3] Creating a Dynamic Workforce: Empowering Employees for Productivity and Growth, O2 Business, March 2021.
[4] Remote Access is Just One of Many COVID-19 IT Challenges, TechTarget, April 27, 2020.