Choosing remote access software: key pointers to consider

hexnode

Work doesn't solely mean working from within your office premises anymore. Although remote work has been there for quite a while, it wasn't until the pandemic that remote work gained the traction it has at present. It gives employees the flexibility to work from anywhere they choose. Remote access software makes it easier for admins to remotely access any device managed by their organization and push necessary configurations to keep both devices and data secure.

The stats regarding the popularity of remote access software pretty much speak for themselves. In 2020, the global market size of remote access software was valued to be at 1095.01 million USD and in 2027, it is expected to reach 2329.32 million USD.

Most modern enterprises already have a substantial number of their staff working from outside company premises. Depending on the industry in which your business operates, you may even have frontline staff and other critical teams working remotely full time. The absence of the right remote access software can make it incredibly challenging for your admin to ensure all important files and applications are available to users when they need them.

In addition to gaining access to the remote devices, the software also provides admins with the convenience of controlling the end device, making the process of resolving any technical hiccups and other troubleshooting issues for remote users a whole lot easier.

What are the different kinds of remote access software?

Remote access software can be of two types – OS based and third-party solutions. You could choose from either one of these two depending on your operational workflow and current business requirements. Major OS vendors such as Microsoft and Apple already have remote access capabilities built into their platforms making it a convenient option for businesses with a limited budget. Third-party tools on the other hand comes with additional features when enabling remote access on the user end devices.

Apple

Mac screen sharing

It enables you to view and control the screen of another Mac connected to your network.

Remote login with secure shell (SS) connection

Users can login to any other Apple device using SSH and SFTP.

Apple remote desktop

Apple's own remote management app that lets you control the screen of other Mac users.

It also comes with a messaging feature for easier interaction. Some of the other features of this tool includes sending files and configuring the settings of the device.

Microsoft

Remote desktop

It provides users with the flexibility to fetch files, open applications and troubleshoot in remote Windows devices.

Why do you need remote access software?

A remote access software can help resolve issues quickly without dampening the productivity of your employees. It also helps businesses to minimize unwanted travel costs and ensure the continuity of various business operations defined within the Service Level Agreements (SLA). Since these tools offer a wide range of functionalities, it can be quite confusing to find the right tool that works well with your company's daily operations. Asking a few critical questions usually helps to narrow down the functionalities you really want to implement to ensure the protection of devices and users. These could include:

Understanding the different software and hardware assets:

It never hurts to have a complete and updated list of all the hardware and software assets managed by your organization. This can give your IT team a clear-cut idea of the different device types and the OS platforms they need to manage. It would also help your team make proper decisions regarding the purchasing of the right remote access software.

Understanding different users and their job roles:

You need to set restrictions on remotely accessing the devices of users with access to highly sensitive data. This includes users with admin privileges and other senior members of your organization. When choosing a remote access software, you have to make sure it comes with the capability to set restrictions to prevent unauthorized members from your IT team from viewing critical information.

Understanding the privacy laws of the place where users are located:

You may have employees flung across different regions of the globe. Meeting the requirements of various privacy laws and other regulatory compliances is steadily being a top priority amongst many organizations. Prior to remotely accessing the intended device of your end users, you need to understand the privacy laws and other local regulations of

the place in which the user is located. It helps to choose software that would aid in streamlining all the controls you need in implementing the various requirements of compliance regulations.

Key considerations when choosing a remote access software

It's important to choose a remote access software that is unique to your organization. In addition to providing the convenience to access the screen of remote users, you need to make sure the tool makes it easier to protect both corporate networks and end user devices. Some of the key considerations you need to keep in mind when choosing a remote access software include:

- Establishing an efficient communication channel where end users can communicate with technicians remotely accessing their system.
- Ability for technicians to see what remote users can see on their screen.
- Ability for users to quickly access the files and resources they need for work.
- Provides the convenience to deploy custom scripts to automate a number of repetitive tasks while troubleshooting.
- Offering strong network security.
- Improving employee collaboration.
- Ensuring user privacy and security.

Why choose Hexnode?

A Unified Endpoint Management (UEM) solution relies on various components such as Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Security Management (MSM) and Identity and Access Management (IAM) to securely manage every aspect of devices and users right from the onboarding stage to disenrollment. Ensuring the security of your corporate resources when making them available to remote users can be difficult. You need to make sure the devices are connected to a secure corporate-approved network and have all the required security settings enabled to ensure the safety of both devices and data. Doing all of this manually can be a tedious process. UEM simplifies this process where all security policies specific to your organization can be remotely pushed to users across different device types with varying platforms.

Using a UEM solution like Hexnode with remote access and control management capabilities can be a time saver for your team. Here are some of the ways in which a third-party tool like Hexnode helps organizations stay connected with their remote users:

Remote view and control

Admins can view the screen of iOS, Windows 10 PCs and macOS devices in real-time from the portal. This saves them the need to be physically present when resolving any technical issues users may be encountering at the time. Sometimes, guiding end users through the issue may not be much of a feasible option. The remote control feature offers the convenience of taking over the user's screen and operate on it just like you would when sitting in front of an actual device. This feature is supported on Samsung Knox devices.

File management

The speed with which you make essential files and other resources available to users can define how successful your remote work implementations are. File management is an important component of any remote access software where files can be easily deployed. The file path of the document can be defined from the portal before it is pushed to user end devices.

Built-in messenger

Maintaining proper communication with your remote staff is important. Hexnode comes with a built-in messenger that helps admins broadcast important messages and send in personalized messages to users. This makes it easier for technicians to reach out to end users when resolving an issue.

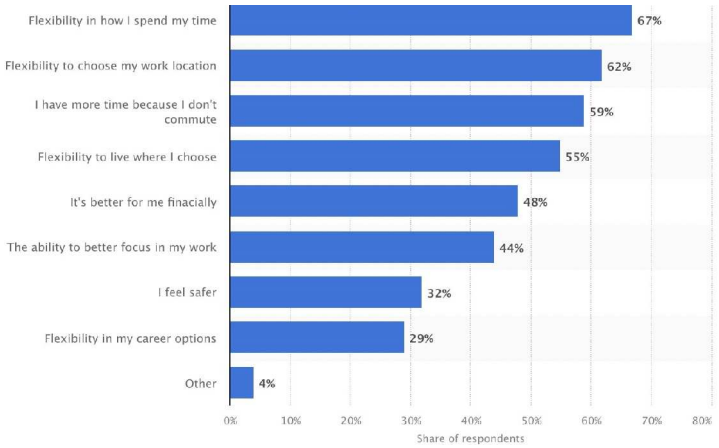
Remotely manage device to ensure device security

Deploying custom scripts can help automate multiple manual tasks your IT team may encounter when fixing a particular problem. It also helps take care of a wide variety of admin tasks that are tedious and time-consuming. Implementing the right remote management strategy that aligns with your organization is important as it helps in keeping both devices and users safe from data breaches and information security incidents. Remote users always carry the risk of increasing the chances for third-party threats to occur. You can minimize this to a large extent by remotely pushing all the security configurations and restrictions needed to keep the endpoints secure. Lost devices can be secured by immediately initiating remote lock and data wipe on the device.

Conclusion

Majority of the people who prefer to continue working remotely do so because it offers them the comfort of making their work schedule more flexible. Remote work has been a success for many organizations with 83% of workers reported being satisfied with the shift. This makes it a much harder job for admins to ensure devices stay protected from

various cybersecurity threats.



A remote access software is an efficient tool that comes with the convenience of improving collaboration among different employees, securely accessing corporate resources and resolving any issues users may be facing without the need to be physically present.

Prior to the selection of any software, it is important for organizations to document a remote access policy that properly details the kinds of data your organization would have access to. This would help address a number of privacy issues your users may have. Once the policy has been documented, it should be made available to all employees via a management portal accessible to everyone within your organization.