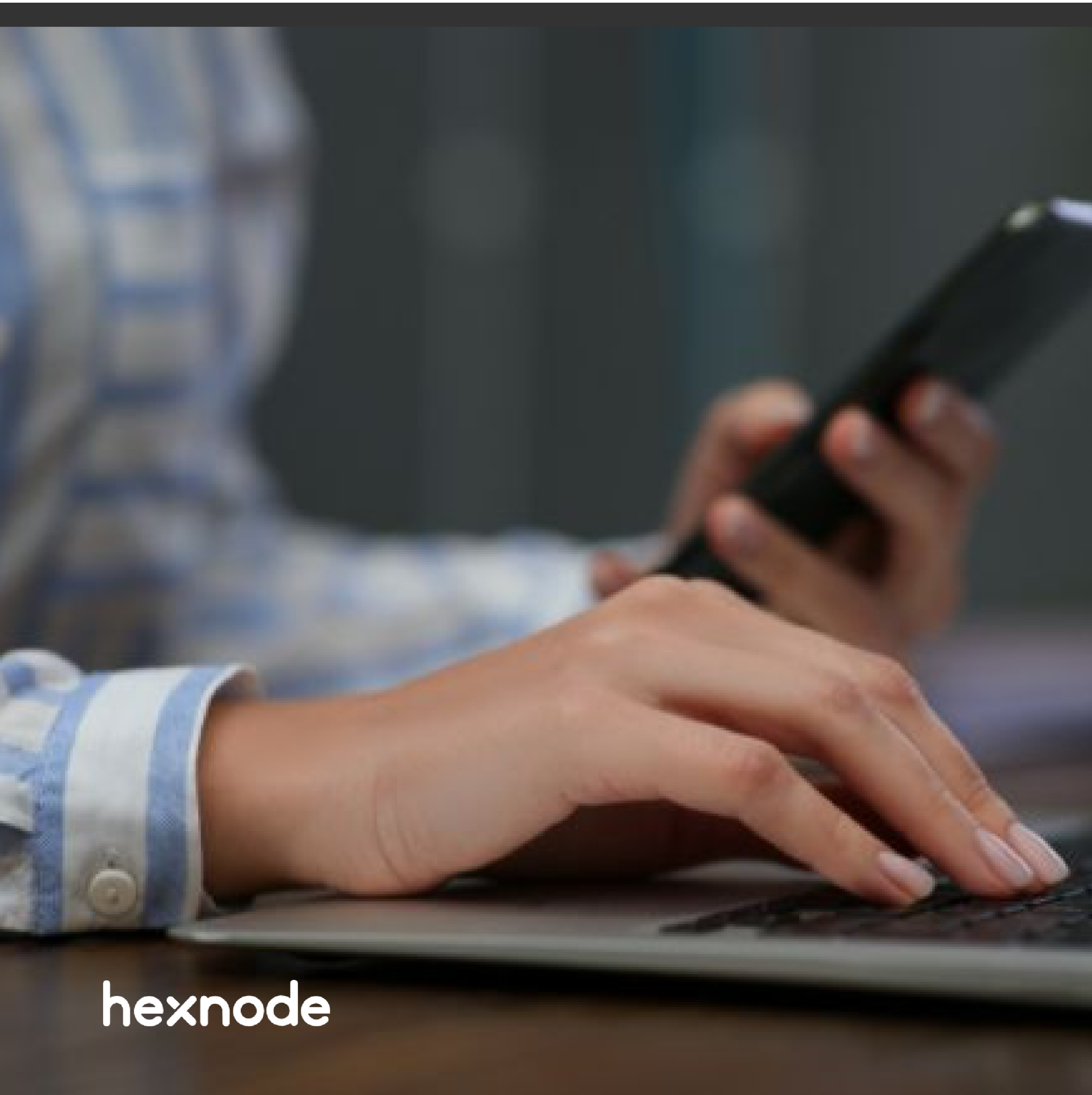
Top 5 Android remote access tools to use in 2023



According to the research carried out by Gartner on the future of remote work, 50% of respondents preferred to continue to work from home long after the pandemic. This is good news when looking from the perspective of your employees, they can after all get things done from the confines of their own homes, avoid cumbersome travel expenses and manage their time more effectively. It can be a nightmarish experience as an IT admin. Suddenly, you are thrust with the responsibility to ensure that users are connected to a secure network and have adequate measures to protect sensitive data. The list is endless. Fortunately, there are plenty of tools out there to make this process easier.
One of the challenges you would have to face is to resolve any issues your remote employees might be facing at the time. A quick peek at the troubled device would usually do the trick. But this is no easy task when the employee is working remotely. This is where a remote access tool would be of help. Most of the remote access tools don't just limit themselves to making it easier for admins to start a remote session. They take into consideration the various security challenges organizations face in making sensitive resources and other services available for remote employees. Android is one of the most widely used OS within the enterprise. In this blog, we've compiled a list of remote access tools admins can use to remotely view and control Android devices in real-time with other devices.

1) GoTo

Formerly known as LogMeIn, GoTo is one of the most widely used remote access tools. It helps businesses neatly resolve a wide range of technical hiccups while ensuring complete privacy of the remote sessions at the same time. Their remote support and access features are quite extensive and are dispersed across multiple products such as GoToResolve (remote IT support), Pro (remote device access), Central (remote monitoring and management), GoToMyPC (remote desktop access) and GoToAssist (remote support software).

Pros

- Enable in-session system diagnostics
- Secure transfer of files
- Initiate remote sessions on unattended devices
- Enhance productivity with multi-session handling, handle 10 sessions at the same time
- Multi-platform support – macOS, Linux, ChromeOS, iOS and Android
- Remotely view and control devices running on Android 6+
- Remotely view iPads and iPhones with the iOS broadcast feature
- Transfer remote sessions to other technicians

- Record live remote sessions
- Enhanced security features such as AES 256 end-to-end encryption, TLS, zero trust based access control, MFA and SSO
- Improve collaboration by sharing computer and file access to authorized users
- Multi-monitor display
- Guard against cyber threats with malware protection and detection of online threats
- Segregate users into groups, enable role-based access controls
- Group devices based on location, function and access levels

Cons

- Remote connection to PCs is not very smooth
- Sometimes requires reconnection for mass transfer of files from target system

2) ConnectWise Control

When it comes to remote access and control, the features of ConnectWise Control are pretty well stacked. What makes this tool stand out from most of its competitors are its resources on scam prevention which educates businesses on the various ways they can fall prey to tech support scams. This can be helpful considering the multiple means hackers make use of to gain access to confidential data.

Pros

- Easily compatible with various platforms such as Android, iOS, Windows, macOS, ChromeOS and Linux
- Works with multiple browsers such as Firefox, Safari, Chrome and Microsoft Edge
- Enhanced security with secure end-to-end connections, role-based security, 2FA, SSL, logging and auditing
- Builds client trust with user consent, AES 256 encryption and in-session chats
- Personalize customer logins
- Integrations with top vendors to automate various workflows
- Initiate remote sessions on unattended devices
- Set role-based access and permission levels
- Access the toolbox folder to store scripts, documents and share them with relevant teams
- Record ongoing remote meetings and take downloadable screenshots
- Create custom themes for meetings
- Implement role-based security to manage the number of attendees during the meeting
- Integration with top vendors to ensure data backup and password protection

- Access ConnectWise View to enable the end user to see and resolve the issues in real time
- Keep visual records of live stream sessions
- Make use of the backstage mode to allow hosts to access a remote system without any user intervention. Helps admins to have access to multiple troubleshooting tools such as Windows command prompt, powershell and Windows defender firewall
- Log session activity to review timestamps and session activities
- Log out users after a pre-determined number of login attempts
- Define IP restrictions to define the IP addresses the tool can be accessed from
- Provide resources to educate users on tech support scams

Cons

- The sessions tend to go offline. Forcing users to restart the session remotely from another system or domain
- The triggers used to alert should be more defined

3) Splashtop

Splashtop started out in 2006 by being the very first browser operating system to allow PC users to securely get online in under 5 seconds. They didn't become a full-fledged remote access software until 2010 when the tool was first used for iPads and iPhones. Their remote access capabilities now extend to a wide range of endpoints running on Windows, Linux, macOS, iOS, Android and ChromeOS. It also includes rugged and IoT devices. They offer remote access and support to a wide range of businesses and classrooms. Some of the key highlights of Splashtop include screen sharing and mirroring, group view and auto lock screens to ensure the privacy of the remote sessions.

Pros

- Cross-platform support – Windows, Mac, Linux, iOS, Android and ChromeOS
- Access virtual machines
- Transfer files without starting a remote session
- View multiple screens at the same time via the multi to multi-monitor feature
- Remotely wake up the target computer
- Enhances the security of the remote sessions through TLS and 256-bit encryption, device authentication and 2FA
- Logs all connections, file transfers and events
- Implements 24/7 intrusion detection
- Initiates blank screen, screen auto lock, session idle timeout and remote connection notification to preserve the privacy of the remote sessions

- Enable two members of the same team to access a system at the same time via the group view feature
- Enable role-based access and permissions

Cons

- Not very friendly for beginners, gets a little laggy when more devices are connected
- Transfer of files can be a slow process

4) BeyondTrust Remote Support

Previously known as Bomgar, one of the highlights of BeyondTrust is its neat integration of security within its remote access features to limit access users have to sensitive data via privileged remote access. The tool can be easily used across a wide range of endpoints such as mobile devices, desktops, laptops and servers. In addition to managing and monitoring privileged accounts, and remote access to endpoints, third-party vendors can be managed as well. It’s not an easy task to keep track of all the users and systems connected to your network. The cloud security management feature of BeyondTrust makes it easier to manage and keep track of all users and systems in place.

Pros

- Multi-platform support, these include Windows, Mac, Linux, Android, iOS and ChromeOS
- Control screens remotely
- Enable screen sharing
- Remotely wake up systems and initiate a remote session
- Easily share files during the session
- Use the camera of iOS and Android devices to get a better understanding of what happens at the end-user screen
- Has integrations with external directories like AD and LDAP to easily manage users, groups and permissions
- Record all session activities and monitor them in real-time
- Maintain logs
- Generate reports to keep track of users, systems and actions initiated on those systems
- Ask for user consent before the session begins
- Control access of employees and third-party vendors to systems when accessing them remotely from the network
- Define permission and access levels of users
- Create audit trails

- Set authorization and notification preferences

Cons

- The connection can be buggy after the system is rebooted
- The initial setup is not very intuitive

5) Hexnode

Hexnode UEM supports the management of multiple endpoints such as mobile devices, tablets, desktops, PCs, and rugged and IoT devices. In addition to making it easier for admins to remotely access and control user end devices, Hexnode's remote monitoring and management capabilities help to ensure the devices only function according to the policies set by your organization and are compliant with the requirements mandated by different regulatory frameworks and cybersecurity experts.

Pros

- Quickly resolve issues with the built-in messenger
- Easily transfer critical files to the exact location within the device
- Multi-platform support – Android, iOS, Windows, macOS, tvOS, iPadOS and Fire OS
- Remotely control screens on iOS and Android devices
- Make use of a wide range of remote management features to resolve issues in real-time
- Notify users of consent before starting a remote session
- Permits users to start and stop a session
- Broadcast messages and share troubleshooting instructions to users via the in-built messenger
- Deploy essential content while keeping the best data security measures in mind
- Adjust the remote view video quality
- Define the required screen orientation
- Improve collaboration by sharing files with authorized users
- Integration with various directory services and other vendors to group devices, and users and automate workflows
- Generate real-time reports of devices and users

Cons

- Remote control does not extend to Windows, macOS, tvOS, FireOS and iPadOS
- Does not support ChromeOS

Bottomline

Before deciding on the remote access tool that works well for your business, there are some key factors you need to consider. These include usability, compatibility with any device or browser, ability to provide adequate monitoring and reporting and high levels of data security. While testing the tool out, be sure to check whether it works well for both your IT team and employees in terms of scalability, productivity and security.