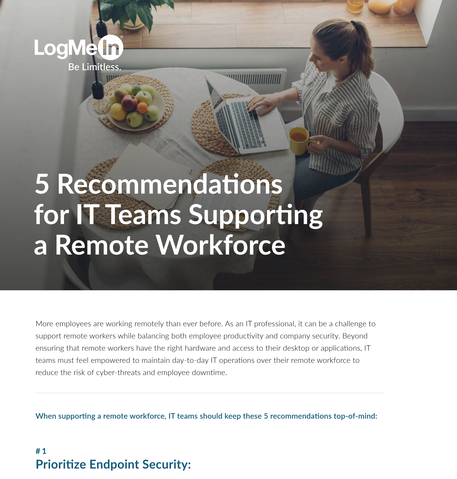


LogMeIn
Be Limitless.

5 Recommendations for IT Teams Supporting a Remote Workforce

More employees are working remotely than ever before. As an IT professional, it can be a challenge to support remote workers while balancing both employee productivity and company security. Beyond ensuring that remote workers have the right hardware and access to their desktop or applications, IT teams must feel empowered to maintain day-to-day IT operations over their remote workforce to reduce the risk of cyber-threats and employee downtime.

When supporting a remote workforce, IT teams should keep these 5 recommendations top-of-mind:

1
Prioritize Endpoint Security:

Regardless of whether your employees are in an office, coffee shop, or living room, they require robust endpoint security to mitigate the risk of a breach or cyber-attack.

For remote employees, it is particularly important for IT teams to provide strong security controls. In a recent study, over 70% of surveyed IT professionals thought remote staff posed a greater risk than onsite employees.

To reduce the risk of a successful attack on a remote employee, IT teams should ensure:

Systems are Patched:

Patch Management should never be deprioritized for remote workers and should be manageable from any location. 57% of cyber-attack victims report that they could have proactively prevented their attacks by installing an available patch.

Antivirus is Updated:

In a remote environment, it is not as easy for an employee to quickly sanity-check a potential phishing email with another employee prior to clicking a link or downloading an attachment. Therefore, IT teams must ensure that they have a strong antivirus in place that protects their computers. The antivirus should be able to prevent common malware and phishing attempts.

TIP: To maintain strong endpoint security while making it easy for IT teams, consider a solution that allows you to centrally manage both your patch management and antivirus from one platform.

2
Maintain a Remote IT Helpdesk:

No matter where your employees are submitting tickets from, IT teams need the ability to troubleshoot and fix potential issues in order to maintain employee productivity and reduce downtime.

For remote employees, this means that an IT team must be efficiently alerted of potential issues as well as aid employees without sitting directly in front of their computer.

IT teams should ensure that they can provide a remote IT helpdesk to support remote employees by:

Turning on Proactive Alerts:

For your remote employees, make sure that you have a system in place for notification of potential hardware or software issues they may be experiencing. The alerts should include performance (CPU), maintenance (folder size, file size), and general supports (if a user installed software, missing hardware).

Implementing Reliable Remote Access:

IT teams need to be able to provide troubleshooting and support for their remote workers. This requires robust remote access that not only gives them the ability to remotely control a computer, but also provides background access for helpful diagnoses without interruption to the end-user.

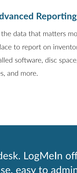
TIP: Consider a solution that combines alerts with advanced scripting capabilities. Setting up self-healing alerts helps your company to stay secure 24/7 without the IT team needing to work 24/7.

3
Support Mobile Devices:

Disruptions in PC supply chains and employees' increased reliance on personal computers and mobile devices have forced IT teams to expand their BYOD policies.

This allows remote employees to keep working on the devices they prefer and are already accustomed to when it is not feasible to provision company-sanctioned hardware. But it can result in a gap between user devices and what IT can proactively manage.

To confidently enable BYOD, IT helpdesks need to be able to remotely support any device quickly and securely. Specifically, IT teams should offer:



iOS & Android Support:

Make sure that you can fully support mobile users by pulling system information, assuming remote control, and pushing device configurations. Connections should be fast and frictionless, no matter the device.

Mobile SDK:

Integrate remote support functionality into your iOS or Android apps with mobile SDK integrations. This gives IT teams fast access to the features they need to support remote employees directly within the company's mobile app.

TIP: Consider a solution that lets you identify and solve the most common issues encountered by mobile users with one click. This functionality allows you to see system information and alerts at a glance without having to navigate the end user's device.

4
Protect Against Phishing & Scamming

The increase in remote work due to the global pandemic has given rise to new cyber-security threats, with mobile attacks growing in popularity. IT teams need to provide fast, secure and seamless remote support that closes out any potential opportunities for scammers to take malicious action. Here are two ways to do that:

Self-hosted PIN Page with Added Protection:

Start remote support sessions from your own web domain so remote employees know they're in the right place for help. On top of that, consider adding company PIN code validation, so PINs generated from outside your account won't work, and domain validation, so sessions on a "dummy" page are nonstarters. These additional measures help prevent your remote employees from unknowingly entering malicious sessions.

IP Restrictions & Restricted Access:

Ensure remote technicians are adhering to company policies and procedures by setting IP restrictions that allow them to only log into your remote support tool from an approved list of IP ranges. Take it a step further by restricting access to users in your company. If the PIN isn't generated from your account, the remote support session will not start.

TIP: Branding helps build trust, so ensure your company name and logo are front and center on any webpage or applet that employees see when they receive support. They will be confident that they are in the right place to get help.

5
Increase IT Visibility:

Gain insight into your remote employee's computer and software so that you can perform computer audits and inventory no matter where you or your employees are located. To increase visibility, ensure that you have a system in place for:

Performing Asset Management:

IT teams must have visibility into their entire endpoint infrastructure to identify unauthorized or junk software installed on employees' computers, keep software inventory, and confirm software versions are on the latest version for optimized security.

Executing Advanced Reporting:

Keep a pulse on the data that matters most. Have a plan in place to report on inventory, CPU usage, installed software, disc space, software changes, and more.

Remove complexity and headaches for your remote help desk. LogMeIn offers IT professionals remote access and support that is easy to use, easy to administer, and scales to fit your business. With LogMeIn, you can remotely support a variety of computers and mobile devices, access their work computers, and maintain day-to-day IT operations and security from anywhere.

Learn how LogMeIn can support your remote workforce.

Central by LogMeIn Rescue by LogMeIn

08.05.2020-EAN3171.PDF