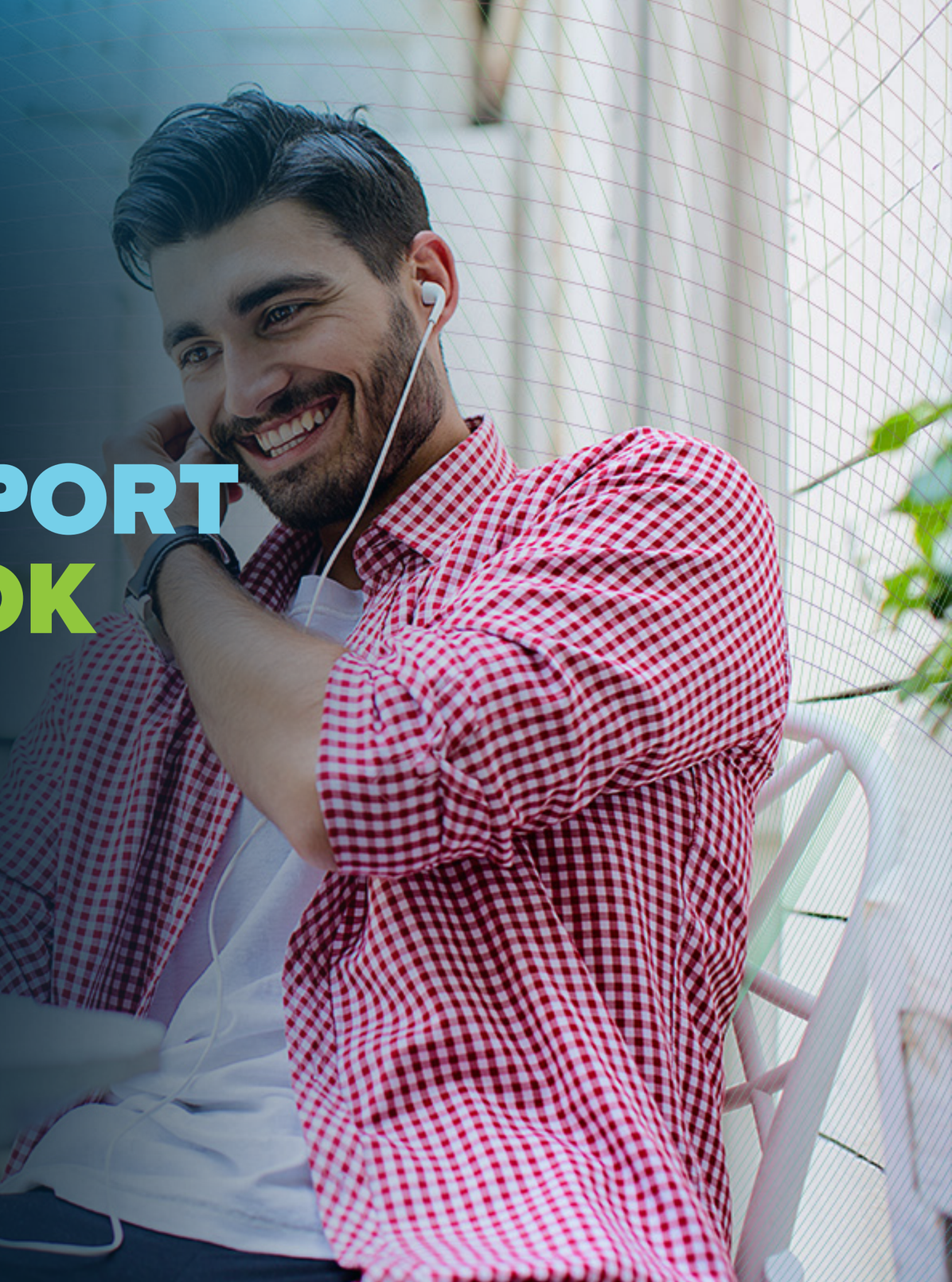
Rescue by LogMeIn

YOUR REMOTE SUPPORT SECURITY PLAYBOOK

Protect Against Cyberthreats while Supporting Remote Work



SECURELY WORK FROM ANYWHERE

The sudden shift to a flexible remote work environment due to the global pandemic has presented businesses with many challenges, not the least of which are security issues. As remote work becomes the new normal, now is the time to re-evaluate the security of your remote support tools.

Beyond your baseline security requirements, there are new threats to consider. According to a 2020 study commissioned by LogMeIn, time spent addressing IT security concerns has increased to 5 to 8 hours per day in 2020 compared to 1 to 4 hours per day in 2019. What's more,100% of IT pros recently surveyed by IDG report that the work-from-anywhere era has exposed gaps in their security policies and practices, with nearly 1 in 5 citing considerable gaps that must be closed.

CAN YOUR CURRENT REMOTE SUPPORT TOOLS MEET THIS MOMENT?

Use this playbook to ensure that your solution has you covered.

Source: IDG, 2020 LogMeIn Helpdesk Rapid Response Research, August 2020.

HAS REMOTE WORK EXPOSED GAPS IN YOUR SECURITY POLICIES AND PRACTICES?

24% Yes, it has exposed considerable gaps we must close

76% Yes, it has exposed small gaps we can readily mitigate

0% No, we have seen no gaps

4 CRITICAL REMOTE SUPPORT SECURITY REQUIREMENTS FOR TODAY'S WORK-FROM-ANYWHERE ENVIRONMENT

1 DATA PROTECTION

Audit Readiness
Many companies rely on third-party security reports and certifications, like Service Organization Control 2 (SOC 2) and ISO/IEC 27000-series compliance. Ensure your solution partner conducts SOC 2 (type II) audits and shares a SOC 3 report and/or adheres to the ISO27K standards.

Banking-grade Data Transfer
Bank on the same level of security used in the financial industry. Your remote support tool should use TLS 1.2 transport security and AES-256-bit encryption to prevent transfer hacks and protect data at rest.

Multi-factor Authentication
Two-step verification secures access to your remote support tool and helps protect against malicious actors. Active Directory (AD), which enables single sign-on and user synchronization, will make it easy to ensure secure logins with the ability to enable and disable technicians as needed.

2 SECURE CONNECTION METHODS

Self-hosted PIN Page
The option to host your own PIN page instead of directing employees to the solution's public-facing page allows you to add your branding along with optional additional security layers.

Company PIN Code Validation
Only PINs generated from your remote support account will be accepted, so codes from any other source will not work. This helps to ensure that only your techs get access to your employees. For added protection, you can lock your PIN codes to only work on your site or through your end user's desktop calling card.

Domain Validation
Prevent malicious actors from scraping your PIN page HTML to set up a "dummy" page. This validates the PIN entry or channel form HTML against domain(s) green-lighted in the support solution to protect against phishing for information about your users.

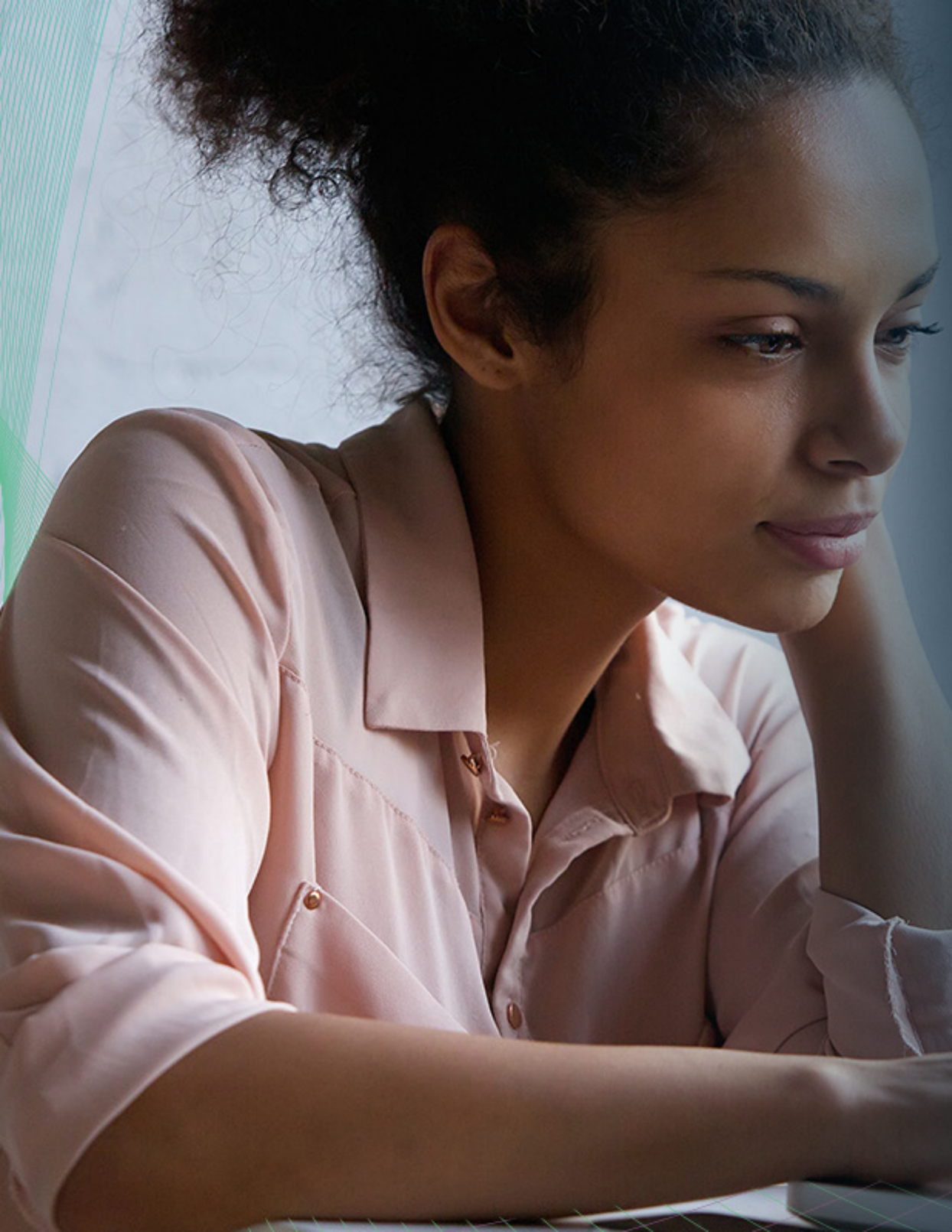
IP Restrictions
Ensure your remote help desk techs are adhering to company policies. Set IP restrictions so they can only log into the solution from within your VPN/network or from an approved list of IP ranges.

Restricted Access Package
Take IP Restrictions a step further to ensure that users within your VPN/network can only receive support using PIN codes generated from within your account. Alternatively, restrict your technicians to only provide support to users within a designated range of IPs.

Restricted Domain Access
As a measure to ensure that your employees receive support exclusively from domains greenlighted on their firewall and deny remote support access to anyone else.

ENSURE PEACE OF MIND

End user trust is just as important as the features and functions of your remote support tool. The ability to add your logo to the support experience lets employees know they're in the right place to get help. Look to customize your:



3

ROBUST ADMINISTRATION

Agent Management, Roles and Permissions
Manage technician access by defining the roles and permissions that techs need to do their jobs. Ensure your admins can define permissions for different tech groups, for example the ability to allow or deny techs to execute scripts or transfer files and get real-time usage reports.

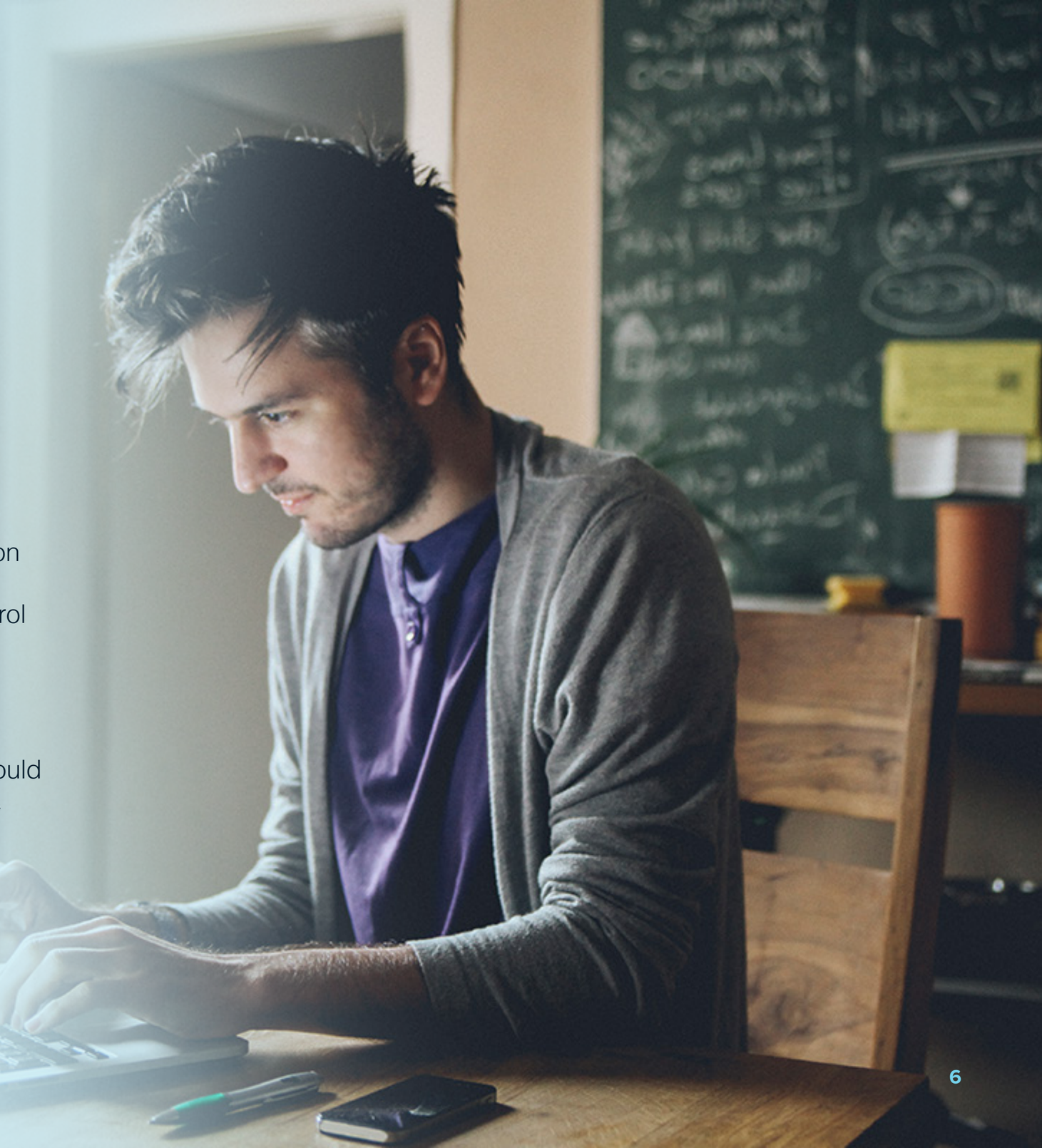
Comprehensive Insight
Knowing how your remote support solution and technicians are performing are key to understanding how you can keep improving and ensuring that data is protected. Look for comprehensive auditing, logging and reporting capabilities.

Full Permissions-Based Functionality
Protect your business and give end users peace of mind by requiring their explicit permission to provide remote support operations. Only then will technicians be able to access employee devices, even during unattended access sessions.

4 ZERO COMPLIANCE COMPROMISES

GDPR (Location specific)
If you are operating in the European Union, ensure your solution enables you to meet the standards and requirements General Data Protection Regulation (GDPR) by providing you with control over the data it stores.

HIPAA (Industry specific)
Your support solution may not be able to control the content shared by users during a support session, but the solution should be designed to meet strict security standards and help HIPAA regulated entities comply with relevant regulatory guidelines.



SUPPORT AND WORK SECURELY – ANYWHERE

Empower IT teams to do their best work from anywhere over any network. LogMeIn Rescue lets you meet strict security guidelines while flexing to meet diverse work environments.

Learn More

03.03.2021/LMI1852/PDF