Rescue

YOUR REMOTE SUPPORT SECURITY PLAYBOOK

Protect against cyberthreats while supporting end users anywhere.

Securely support from anywhere

Companies and customers are growing increasingly concerned about security in today's digital-first world. Malicious actors have upped their game and cyberthreats are on the rise, causing many organizations to re-evaluate the security of their remote work tools.

Beyond your baseline security requirements, there are new threats to consider. According to a 2022 study commissioned by GoTo, about half of support leaders (49%) report an increased risk of cyberattacks compared to two years ago. To meet support goals, they are prioritizing the ability to securely connect to end users and providing technicians with reliable and secure support tools — just not at the expense of a simple support experience.

Can your current remote support tools meet this moment?

Use this playbook to compare your solutions to Rescue.

Most important objectives to meeting support goals:

87% Secure remote connections

84% Reliable and secure support tools

82% Simplified support

Source: IDG, Remote Customer Support Marketpulse Research for GoTo, January 2022.

4 critical remote support security requirements for today's remote end users and technicians:

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 (SSO) 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 end users 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 technicians get access to your end users. For added protection, you can lock your PIN codes to only work on your site or through a one-click short cut on your end user's desktop.

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) previously green-lighted in the support solution to protect against phishing for information about your users.

IP restrictions
Ensure your remote technicians 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 end users receive support exclusively from allowed domains 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 them know they're in the right place to get help.

Look to customize your:

- PIN page
- Downloadable applet
- Desktop icon

3 Robust administration

Technician management, roles, and permissions
Manage technician access by defining the roles and permissions that they 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 take remote control 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 and perform certain actions on the end user's device.

4 Zero compliance compromises

GDPR (Location specific)
Ensure your solution enables you to meet the standards and requirements for your location, like 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.

From safe connection methods to seamless resolutions, peace of mind comes from having a secure remote support tool you can rely on. Rescue lets you meet or exceed strict security guidelines to better protect your end users and business.

Learn More

Rescue, built by GoTo.
Remote support made easy.