Rescue

SECURITY OVERVIEW

ENTERPRISE SECURITY YOU CAN RELY ON

Rescue prioritizes security as much as speed and ease of use. In fact, Rescue is an industry leader in remote support security, with a commitment to continuous security audits and product enhancements that uphold the highest security standards available.

Core security features include:

- AES 256-bit encryption securing all communications
- Permission based model
- Granular technician privilege management
- Identity management integration
- Multi-factor authentication
- Single sign-on (SSO)

For more information on Rescue's security standards, please review Rescue's architecture white paper.

Rescue supports compliance with:

- SOC 2
- GDPR and other PII regulations
- HIPAA and other PHI regulations
- Learn more about our Trust & Privacy.

About Rescue
Rescue is a powerful, easy-to-use remote support solution that provides temporary, permission-based access for PCs, Macs, mobile devices, and more. Rescue helps organizations provide technical support to employees, customers, or both, with a solution that is fast, reliable, flexible, and easy to use.

Additional Enterprise Security Layers

In addition to the core security measures within Rescue, we offer additional security options for enterprise organizations and regulated industries with strict requirements for using cloud based services that are accessible by the public. These optional layers of security include:

Restricted Access Package

This provides provide additional security for organizations that want to control whose computer their technicians can access and vice-versa. With the Restricted Access Package enabled, IP filtering based on your network configurations ensures technicians can only establish sessions with end users in a given network, or end users of a given network can only be supported by technicians from your account.

- **For technicians:**
  Access to individual networks will be opened by configuring a range of IP addresses with which the technicians can establish a session. This will prevent technicians from establishing Rescue sessions when outside the pre-approved IP range.

- **For end users:**
  Services can be configured so end users will be restricted to establishing a Rescue session with technicians in a specific account, preventing session initiation with anyone outside that Rescue account.

Company PIN Code Validation

By integrating the Rescue PIN entry form into your self-hosted website, only PIN codes created by your organization will be accepted in your entry form. No other PIN codes will be accepted in that form.

Enterprise Domain

A fully separate domain from the standard Rescue domain that is enabled in the Rescue's backend infrastructure on an account basis, after a formal request and vetting. When enabled, the Enterprise Domain allows organizations to block traffic from all 'public' Rescue-owned domains and related subdomains at your firewall, allowing only your enterprise traffic to pass.

More ways Rescue puts you in control:

- Control where private data is stored and when it's deleted
- Simplify sign-on with Active Directory
- Give end users the ability to approve all agent actions, like remote control, desktop view, file transfer, system information, and reboot and reconnect
- See detailed reporting and track changes made in your admin settings

GoTo
Rescue, built by GoTo.
Remote support made easy.