Data Sheet

Enterprise Security

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.

Rescue is architected with security being the most important design objective. This means being committed to continuous security audits and applying the highest security protocols available in a remote support solution. Core security features include:

- 256-bit encryption securing all communications
- Permission based model
- Granular technician privilege management
- Identity management integration
- Multi-factor authentication

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

Additional Enterprise Security Layers

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

Enterprise Domain

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

Restricted Access Package

This provides 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 will occur and technicians and end users will only be able to establish Rescue sessions with those networks previously configured.

- For technicians, access to individual networks will be opened by configuring a range of IP addresses that the technicians can establish a session with. This will prevent technician 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

This functionality ensures that all PIN-based Rescue sessions begin via specified entry forms. For organizations integrating the Rescue PIN entry form into their self-hosted website, enabling this feature ensures that PIN codes created by that organization will only work on that organization's entry form and no other PIN codes will be accepted in that form.