LogMeIn Rescue

Datasheet

Elevate Your Enterprise Security with Unparalleled Protection

Ensure that your organization's data, endpoints, and users remain protected against evolving cyber threats with LogMeIn Rescue's enhanced security package. Out of the box, Rescue already includes security functionality to lockdown your environment. This package is designed to provide additional, layered, comprehensive protection for enterprises seeking unmatched protection and peace of mind. Whether you're leading IT operations, managing customer support, or safeguarding sensitive user data, Rescue's enhanced security package is tailor-made for organizations prioritizing security without compromising efficiency.

The Power of Rescue's New Enhanced Security Package

Comprehensive Protection

From internal IT teams to enterprise-scale scenarios, Rescue's enchanced security package keeps your data safe and your teams productive with multi-layered security solutions.

User-Centric Design

Built for ease of adoption, Rescue's security features are intuitive and non-disruptive for your teams, ensuring seamless implementation with no compromise on usability.

Blocks Bad Actors

Advanced security functionalities — such as advanced device and IP-based restrictions — ensure trust with colleagues, customers, and partners while keeping bad actors out of your systems.

Business-Driven Security

Rescue's enhanced security package is a strategic tool that integrates with business goals, helping you meet compliance, customer trust, and operational efficiency objectives.

What Is Included?

1 Device-Based Restricted Access Package

Restricts access by remote support tools based on authenticated devices, ensuring only pre-approved devices can initiate or receive support sessions. Protects against unauthorized access and potential breaches.

- Protects both personal and corporate devices on and off the network.
- Offers IT administrators unmatched control and monitoring — a step beyond traditional IP-based methods.
- Helps organizations meet regulatory compliance by ensuring sensitive systems are only accessed by authorized devices

2 IP-Based Restricted Access Package

Implements IP filtering to restrict Rescue sessions based on pre-configured IP ranges. Ensures only verified networks can engage with your systems.

- Technician Restriction thwarts potential abuse by limited support to specific IP ranges.
- End-User Restriction blocks bad-actor access by only allowing support sessions from known networks.
- Login Restriction locks down your Rescue account by prohibiting access from external, unapproved IPs.

3 Generic Enterprise Domain

Provides a separate enterprise domain for authenticated users, blocking the publicly used logmeinrescue.com domain for enhanced control and better security.

- Delivers advanced isolation for enterprise users while preventing unauthorized attempts by non-enterprise or trial users.
- Provides an exclusive and protected environment.

4 Company Pin Code Validation

Ensures only PIN codes generated by your Rescue account will be accepted in your entry form. This applies to PIN entries on client websites or applications.

- Prevents fraudulent attempts to trick end-users into accepting malicious support sessions.
- Protects against scams and builds trust with end-users by ensuring secure, company-controlled PIN generation.

5 Allowed Hosts for External PIN Entry

Limits Rescue PIN entry to pre-approved domains and redirects users attempting PIN entry on alternative or malicious domains. Protects end-users who may unknowingly input PIN codes on fraudulent or copycat websites.

- Blocks unverified domains that could cause harm to a device or environment.
- Enhances end-user and organization safety and ensures business continuity without unnecessary interruptions.

Rescue's enhanced security package equips your organization with advanced tools to lock down your remote operations while safeguarding productivity.

LogMeIn Rescue

Book a Demo