

Datenblatt

Unternehmenssicherheit, auf die Sie sich verlassen können



LogMeln Rescue priorisiert Sicherheit genauso wie Geschwindigkeit und Benutzerfreundlichkeit. Tatsächlich ist Rescue branchenführend in Fernsupport-Sicherheit und verpflichtet sich entsprechend den höchsten verfügbaren Sicherheitsstandards zu kontinuierlichen Sicherheitsaudits und Produktverbesserungen.

Zentrale Sicherheitsfunktionen:

- AES-256-Bit-Verschlüsselung für die gesamte Kommunikation
- Berechtigungsbasiertes Modell
- Präzise Verwaltung von Technikerberechtigungen
- Integrationen für Identitätsmanagement
- Multifaktor-Authentifizierung
- Single Sign-On (SSO)

Weitere Informationen zu den Sicherheitsstandards von Rescue finden Sie im [Whitepaper zur Architektur](#) von Rescue.

Informationen zu LogMeln Rescue

Rescue ist eine leistungsstarke, benutzerfreundliche Remote-supportlösung, die vorübergehenden berechtigungsbasierten Zugriff auf PCs, Macs, Mobilgeräte und mehr ermöglicht. Mit Rescue können Organisationen ihren Teammitgliedern und/oder ihrer Kundschaft technischen Support über eine schnelle, zuverlässige, flexible und benutzerfreundliche Lösung bereitstellen.

Rescue unterstützt Compliance mit:

- SOC 2
- DSGVO und anderen Vorschriften zu personenbezogenen Daten
- HIPAA und anderen Vorschriften zu geschützten Gesundheitsdaten
- Weitere Informationen zu Sicherheit und Datenschutz finden Sie in unserem [Trust & Privacy Center](#).

Enterprise-Sicherheit für Unternehmen

Zusätzlich zu den zentralen Sicherheitsmaßnahmen bei Rescue bieten wir weitere Sicherheitsoptionen für Unternehmen und regulierte Branchen mit strengen Anforderungen hinsichtlich cloudbasierter Services, die für die Öffentlichkeit zugänglich sind. Zu diesen optionalen Sicherheitsschichten gehören die folgenden:



Paket mit Zugriffsbeschränkungen

Damit erhalten Organisationen, die kontrollieren möchten, auf welche Computer ihre Techniker:innen zugreifen können und welche Techniker:innen für Benutzer:innen verfügbar sind, zusätzliche Sicherheitsfunktionen. Wenn das Paket mit Zugriffsbeschränkungen aktiviert ist, wird anhand der IP-Filterung basierend auf Ihren Netzwerk-konfigurationen sichergestellt, dass Techniker:innen nur Sitzungen mit Benutzer:innen in einem bestimmten Netzwerk aufbauen können bzw. dass Benutzer:innen eines bestimmten Netzwerks nur von Techniker:innen Ihres Kontos unterstützt werden können.

- **Für Techniker:innen:**

Der Zugriff auf einzelne Netzwerke wird ermöglicht, indem Sie einen Bereich aus IP-Adressen konfigurieren, mit denen die Techniker:innen eine Sitzung herstellen können. Dadurch wird verhindert, dass Techniker:innen Rescue-Sitzungen außerhalb des vorgegebenen IP-Adressbereichs aufbauen.

- **Für Benutzer:innen:**

Services können so konfiguriert werden, dass Benutzer:innen Rescue-Sitzungen nur mit Techniker:innen eines bestimmten Kontos herstellen können und keine mit Personen außerhalb dieses Rescue-Kontos.



Überprüfung des PIN-Codes

Wenn Sie das Eingabeformular für die Rescue-PIN in Ihre selbst gehostete Website oder Calling Card integrieren, werden nur von Ihrer Organisation erstellte Support-Schlüssel im Eingabeformular akzeptiert. Andere Support-Schlüssel können nicht eingegeben werden.



Enterprise-Domain

Ein komplett separate Domain von der Standard-Rescue-Domain, die nach formeller Anfrage und Überprüfung in der Backend-Infrastruktur von Rescue pro Konto aktiviert wird. Wenn die Enterprise-Domain aktiviert ist, können Organisationen den Datenverkehr von allen „öffentlichen“ Rescue-Domains und zugehörigen Unter-Domains mit ihrer Firewall blockieren und nur Enterprise-Datenverkehr zulassen.

Weitere Kontrollmöglichkeiten mit Rescue:

- Kontrolle am Speicherort privater Daten und bei deren Löschung
- Vereinfachte Anmeldung mit Active Directory
- Möglichkeit, dass Benutzer:innen alle Technikeraktionen genehmigen können, darunter Fernsteuerung, Desktopansicht, Dateiübertragung, Systeminformationen, Neustart und erneuter Verbindungsaufbau
- Detaillierte Berichterstattung und Verfolgung von Änderungen in den Admineinstellungen