Security Overview

RingCentral recognizes that secure and reliable phone service is critical to business operations. As a cloud service provider, RingCentral offers a robust multi-tenant cloud communications service with several layers of built-in security.

Overview

Customer account security is a shared responsibility between RingCentral and customers. Security is implemented via policies and governance practices (people), within the service development and operations processes (process), and the application and infrastructure layers (technology).

The customer account security responsibilities are shared between customers and RingCentral. Customers manage their account policies, user permissions, and login information. RingCentral manages service delivery, architects and design security into the product, and ensures physical and environmental security of the service. RingCentral employs a multi-layered security model with: security at the perimeter, at the service delivery layer, SSL on our Web applications, Tier 1 data centers and customer controlled settings in the application interface.

In addition, RingCentral has a full-time security and fraud-prevention department with a security program that is based on industry best practices.

User Service Administration

Front-end settings that customers control to manage their account policies and their users include: adding or removing extensions, setting user permission levels, managing extension passwords, enabling international calling, allowing specific international call destinations, and blocking inbound caller IDs. In addition, customer admins and individual users can review call history, and upload and delete messages.

Application Security

RingCentral designs applications to be resilient both operationally and in terms of security. Security considerations are taken into account during design, development, and QA phases; security testing is performed throughout the year. At RingCentral, customer endpoints are viewed as an important part of the customer data ecosystem of any UCaaS service. To support the security of customer data on endpoints, mobile and desktop applications are offered that support encryption of customer data at-rest.

Network and Infrastructure Security

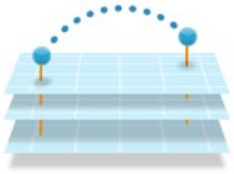
RingCentral's service perimeter is protected with firewalls and session border controllers. Two-factor authentication is used for administrative access to the service environment. Technology layers include intrusion-detection systems, system logs, and fraud analytics. Operational processes include system and service-level monitoring, system hardening, change management, and regular vulnerability scans.

Transmission Security

RingCentral utilizes SSLv3/TLSv1 to encrypt web session traffic and to encrypt phone provisioning sessions for RingCentral desk phones. In addition, desk phones, mobile applications, and desktop applications support encrypted calls using SIP over TLS for signaling and SRTP for media.

Physical and Environmental Security

RingCentral's services are hosted in data centers that undergo SSAE-16 and/or ISO 27001 audits. The data centers share hosted facilities space with some of the world's largest Internet companies and financial institutions. The geographic diversity of our locations acts as an additional safeguard, minimizing the risk of loss and service interruption due to natural disasters and other catastrophic situations.



Fraud Mitigation

RingCentral service includes multiple measures to prevent and detect toll fraud, including access control, detection controls, usage throttling, and customer-controlled settings to enable/disable international calling to approved destinations. In addition, RingCentral's security department performs active monitoring to detect and notify customers of anomalous calling patterns on their account.

Disaster Recovery

The RingCentral service is architected to support failover conditions in case of emergency. Our service is built with geographically distributed redundancy. Primary and backup locations remain online simultaneously, with a primary pod in active mode, and the secondary pod in standby mode. Database replication between locations is in real time, with failover being built into the service. If a primary location is unavailable, the backup location will continue service. In addition to infrastructure and application redundancy, we have geographically distributed operations such that service operations can continue if one location is not available.

Checklist for Protecting Your RingCentral Service

- Set strong passwords and PINs for your extensions.
  Tip: Use answers to security questions that are difficult to guess and don't make use of public or easily guessable information. Ex. Q: 'Where did you go to high school?' A: Jurassic Park. Or, another sample answer is, 'Go Gators!'
- Implement VoIP encryption on your account.
- Disable international calling on your account if it is not needed.
- If international calling is needed, restrict international destinations to those needed for your company business.
- Place VoIP phones behind firewalls.
- Block unauthorized network access to the phones login consoles.
- Block numbers for unwanted callers.
- Limit the users to whom you give admin-level permission.
- Only use email message forwarding for non-sensitive messages.
- Retrieve sensitive messages via an encrypted web session.
- Intermittently change extension passwords and PIN codes.
- Periodically review service usage to ensure it complies with your policies and appropriate use for your organization.

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com

KID-3763 02/2016