RingCentral: Secure Cloud Communications and Collaboration

White paper
# Table of Contents

**Key Security Considerations for UCaaS**

- Organizational and Operational Security

**RingCentral Cloud Security**

  - Data Center Security
  - Access Management
  - Data Encryption
  - Network Security
  - Distributed Denial of Service (DDoS) Attack Prevention
  - Vulnerability Management
  - Patch Management
  - Change Management

**Application Security**

  - Secure Software Development
  - Fraud Detection and Prevention
  - Business Continuity and Disaster Recovery

**Data Isolation**

  - Account Security as a Shared Responsibility
    - What is Shared Responsibility?
    - RingCentral’s Responsibility
    - Your Responsibility: Security in the Cloud

**Security Assessment and Privacy Compliance**

  - RingCentral Certifications
  - Customer Admin Controls
    - Roles and Permissions
    - Insider Threats
    - Mobile Security
    - Single Sign-On (SSO)
  - Audit Trail
  - Security for Apps and Developers

**Conclusion**
Of the many questions companies have when considering a move to the cloud, security undoubtedly sits at the top of the list. In particular, the sensitive nature of business communication—with employees and with customers—is a critical focus for security teams. After all, each day companies use phones, text, online meetings, fax, email, and other forms of communication to share strategies and secrets that define their competitive advantage.

In today’s world, there’s no higher priority for companies than the security of their customer data. For companies using on-premises solutions, the full responsibility for data security and regulatory compliance falls on their teams. That can be particularly challenging in highly regulated industries, such as financial services and healthcare, which have an even higher threshold to ensure that their solutions and vendors are compliant. With on-premises environments, organizations may struggle to find the resources or time to acquire the latest security measures required to meet today’s increasingly strict privacy regulations. Maintaining strong physical security across many business locations, each with its own on-premises system, only adds to the challenge.

With a cloud communications solution (commonly known as unified communications as a service or UCaaS), on the other hand, companies have access to greater security measures to protect customer information than with traditional on-premises systems. In addition, the shared security environment and policy platform the cloud can provide (in which the vendor and the customer share ultimate responsibility for data security) offers an inherent advantage to businesses without large IT departments or those spread across multiple locations (for more information, see Account Security as a Shared Responsibility on page 9). Customers benefit from the economies of scale provided by leveraging the UCaaS provider’s security expertise and hardened facilities. In this way, moving to a cloud communications solution can actually raise an organization’s security posture.

RingCentral has maintained a long-standing commitment to security, built on our deep expertise in operating and securing unified communications and SaaS products. This white paper provides insight into the security and trust built into RingCentral’s products and services.

### Key Security Considerations for UCaaS

When trusting operations and confidential data to another company, it’s critical to choose a trustworthy cloud vendor, which means an established company with ownership of its platform, many satisfied customers, and robust security. RingCentral recommends the following considerations when evaluating UCaaS providers.
Key Security Considerations for UC

- Secure Data Center
- Secure Voice
- Data Encryption
- Application Security
- Account Management and Administration
- Transparency

Additional elements to consider when evaluating a provider include detailed descriptions of their security practices and processes, as well as evidence of independent security assessments and validations, such as an audited Service Organization Control (SOC) 2 or 3 report.

Organizational and Operational Security

At RingCentral, security begins with our culture. Security and customer trust are core business values, and we build these into our services as well as invest in dedicated security and privacy teams. In addition, geographically distributed Tier 4 data centers and strong network security safeguard the service perimeter and the core infrastructure of our services. These measures, combined with our on-staff security experts, protect your data, shield your business from telecom fraud, and allow your IT department to focus on your core business functions, rather than worry about UCaaS security.

As part of our organizational structure, RingCentral has a dedicated security department, with security engineering, security audit/compliance, application security, security data science, and service abuse functions that report to the company’s Chief Security Officer (CSO).

In addition, RingCentral conducts employee background checks, delivers security awareness training to new hires (and as needed to current employees), and requires employees to acknowledge company policies each year, including our robust security policy.

Separately, physical access to RingCentral’s corporate information resources is controlled by access cards, which are used to identify, authenticate, and monitor all admittance attempts. We also adhere to stringent protocols that limit access to any physical premises to authorized personnel.
RingCentral: Secure Cloud Communications and Collaboration

All RingCentral employees and contractors receive in-depth training on data protection and confidentiality, as well as information security. This type of security training is mandatory and occurs at least annually. All employees and contractors must acknowledge and sign a data protection and confidentiality agreement. All employees and contractors also receive a certificate of completion following training and assessment.

RingCentral Cloud Security

It’s imperative to understand the security policy details of any important provider with whom your company works. Let’s take a closer look at the key elements of cloud security and how RingCentral protects your critical communications data.

Security is implemented three ways: via policies and governance practices (people); within the service development and operations processes (process); and in the application and infrastructure layers (technology).

The security of RingCentral’s cloud services encompasses multiple layers and many components, including policies and methodologies to service architecture; capabilities to detect potential toll fraud and service abuse; and user-controlled service administration. Security capabilities and settings reside in the application and infrastructure layers, within the service delivery and operations processes, and the company’s security policies and governance practices.

We employ a multi-layered security model, with security at the perimeter and service delivery layers (see diagram below). It also includes Transport Layer Security (TLS) on our web applications, as well as secure data centers and settings in the interface that customers control.

<table>
<thead>
<tr>
<th>Governance Risk Management and Measurements</th>
<th>Customer Controlled</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Service Administration</td>
<td>Designed In and Tested</td>
</tr>
<tr>
<td>Application Security</td>
<td>Data Entering the Service Cloud</td>
</tr>
<tr>
<td>Border Security</td>
<td>Data Encrypted in Transit and At-Rest</td>
</tr>
<tr>
<td>Data Security</td>
<td>Infrastructure and Operations</td>
</tr>
<tr>
<td>Platform Security</td>
<td>Detect and Stop Service Abuse</td>
</tr>
<tr>
<td>Toll Fraud Mitigation</td>
<td>Protected Environments</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Third-Party Audits and Security Testing</td>
</tr>
</tbody>
</table>

RingCentral’s cloud security model includes the above eight risk management factors, as well as how to measure them.
RingCentral: Secure Cloud Communications and Collaboration

Data Center Security

Our services are hosted globally in enterprise-class Tier 4 data centers and leading public clouds. We vet and select our data center locations with security top of mind. Our world-class network operations centers (NOCs) are continually monitored—24x7—and staffed by highly trained, on-site engineering specialists. Entry to each data center location requires biometric identification, as well as dual-person authentication and a built-in system of “man traps.” Security and safety systems are audited monthly for maximum insurance; each data center is certified SSAE 18 compliant.

Access Management

Access to RingCentral production environments is tightly controlled with Identity and Access Management (IAM) and multi-factor access controls. These robust access management measures enable only trained and authorized personnel to access our production environments.

Data Encryption

Data encryption protects sensitive customer and call data from unauthorized access. With RingCentral, all data is encrypted in transit and at rest, using applicable industry-leading encryption, standards, and protocols.

RingCentral addresses vulnerabilities in the VoIP data plane by safeguarding voice communications with an advanced secure voice technology that prevents eavesdropping on calls or tampering with audio streams between all endpoints—desk phones, as well as computers and mobile phones running a RingCentral mobile or softphone app. RingCentral uses two enterprise-grade security protocols to provide additional security for IP phone calls—TLS authentication and SRTP encryption:

- **Transport Layer Security (TLS)** is a cryptographic protocol that provides encryption on the Session Initiation Protocol (SIP) signaling data. This protocol secures the SIP signaling communication between supported endpoint devices and the RingCentral cloud servers.

- **Secure Real-Time Transport Protocol (SRTP)** is a profile of the Real-Time Transport Protocol (RTP) that provides encryption, message authentication, and integrity, as well as replay protection to the RTP packet stream that is transported between supported endpoint devices and the RingCentral cloud servers.

In addition, all portals have https access (e.g., service.ringcentral.com); all non-voice data is TLS encrypted; and hard phones use digital certificates to establish secure connections to download their provisioning data.

Network Security

A voice over IP (VoIP) application inherently exposes both the control plane and the data plane, providing major attack targets for VoIP hackers. To prevent hackers from exploiting these vulnerabilities, RingCentral deploys best-of-breed network protections optimized for voice and data. These protections—together with RingCentral experts continuously monitoring systems for anomalies—help to prevent service disruption, data breaches, fraud, and service hijacking. In addition, an advanced suite of intrusion prevention technologies protects against malformed packets and fuzzing techniques, which can be used to confuse or overwhelm border controllers, resulting in service disruption, system restart interruption, and endpoint resets.

Advanced RingCentral border-session management is immune to many of the forms of attack that have disrupted the services of other VoIP and UCaaS vendors. RingCentral security also protects against spoofed messages by validating the value of “Call-ID,” “Tag,” and “branch” while processing control NOTIFY messages.
RingCentral: Secure Cloud Communications and Collaboration

RingCentral security also overcomes the typical set of firewall traversal problems in VoIP systems with network address translation (NAT) support for static IP configuration and “KeepAlive” SIP signaling. This maintains user addressability without providing attackers the opportunity to infiltrate further.

Distributed Denial of Service (DDoS) Attack Prevention

Similar to the DDoS attacks that take down corporate websites by overloading servers with millions of requests, VoIP DDoS attacks attempt to deny service to phone users. These attacks usually originate from multiple points (often thousands of compromised computers around the world—thus the “distributed”) and send massive voice data traffic to the target service. Attackers can also target proxy servers, user agents, and registration servers.

The motives for these attacks range from mischief to outright extortion. A new and more insidious frontier for cybercriminals is the “Dark DDoS” attack. These are used as a smokescreen or diversion to cause network disturbances and confuse IT teams while the real attack—typically an advanced persistent threat (APT)—infiltrates the network and steals sensitive corporate data. As far back as 2015, Akamai reported in the State of the Internet Security Report a 180% increase in DDoS attacks. Security firm Corero predicted the highly sophisticated, adaptive, and powerful Dark DDoS attack would grow exponentially.

Vulnerability Management

When it comes to securing production environments, cloud providers must find and fix potential flaws in their security architectures before outsiders do. That’s why RingCentral implemented system hardening practices and automated the ongoing vulnerability scanning of production servers and network device configurations. RingCentral scans servers, network devices, and other applicable systems to identify unpatched vulnerabilities and issues of noncompliance to established security configurations. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. In addition, RingCentral performs internal and third-party security testing of its application releases.

Patch Management

RingCentral includes patch management as part of its vulnerability testing efforts. Authorized personnel are trained in system administration to include patch management techniques. An organizational hardware and software inventory is maintained, as well as an electronic database of information on patches required and deployed on the systems or applications. Patches are tested on non-production systems prior to installation on any production systems.

Change Management

RingCentral has a thorough change management process in place. By maintaining strict oversight of system changes, RingCentral is able to strengthen its overall decision-making by ensuring that employees carefully consider system changes prior to deployment and continue to learn from prior changes.

RingCentral’s change-control policy includes regular meetings to review and manage changes to our production environment. Prior to deployment into production, change requests are documented and approved by multiple stakeholders. Upon deployment, verification procedures are followed to ensure success. In the event that verification steps fail, we have thorough roll-back procedures and policies in place.
RingCentral: Secure Cloud Communications and Collaboration

Application Security

RingCentral performs static and dynamic security code testing of all its applications prior to its release into production. This includes code testing of service web, mobile apps and desktops, and integrations. We also run vulnerability scans, and all our applications undergo penetration testing once a year.

RingCentral’s secure software development best practices include internal design reviews, threat modeling, and thorough risk assessments through the entire process—from design to post-launch operations. We have a secure SDLC process in place. RingCentral also follows other best practices, such as bug remediation policy, secure coding guidelines and regular security-driven coding training (for information on our bug bounty program, see “Secure Software Development” below).

Secure Software Development

Simply put, security begins with code. RingCentral enforces security and incorporates best practices at every stage of the Software Development lifecycle. We employ multiple security schemas and layers for our developers and customers, including utilizing the latest security standards, employing a zero-trust model, and requiring developers to undergo numerous stages of testing and validation. This encompasses numerous protections and stages both within the process of developing and graduating an application, as well as for our customers.

The security team also mandates regular security-driven coding training to keep the team updated and ahead of the curve at all times.

Industry-leading tools and systems are used and deployed to scan applications and identify vulnerabilities, such as OWASP Top 10 vulnerabilities and CWE Top 25 software errors, on a regular basis. Any issues identified during the process are resolved, and measures are taken to ensure they don’t recur.

In addition to these internal measures to ensure secure code development and testing, RingCentral also partners with third-party vendors for annual penetration testing. All layers and all environments are in scope for this penetration test.

RingCentral also runs a private bug bounty program. There are currently over 300 researchers invited to participate in the program. Researchers’ findings are triaged by RingCentral and assigned to our security team for further review. The RingCentral security team assesses the severity of the report and assigns it to the proper team. All RingCentral products are in scope.

Monitoring

RingCentral’s security monitoring practices enable us to proactively identify any security misconfigurations or vulnerabilities before they become issues, while also ensuring we maintain regulatory compliance. RingCentral’s security monitoring program focuses on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior. All security logs are collected and monitored through our centralized logging system (SIEM).

Fraud Detection and Prevention

RingCentral’s 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.

RingCentral uses a CDR analytics engine that creates alarms when it detects suspicious traffic. We also maintain an in-house fraud search engine to identify additional account information connected to known fraudulent accounts. On top of this, RingCentral keeps an up-to-date blacklist database of fraudulent phone numbers, CC tokens, and device IDs that alert RingCentral if any of these items are used on a new or existing account. The attempted usage of any of these items results in account disabling. We also generate several reports throughout the day to assist in the identification of anomalous and potentially fraudulent usage.

**Business Continuity and Disaster Recovery**

It’s critical for any cloud provider to ensure that critical data remains accessible—even in the event of disruptions. RingCentral houses its core technology infrastructure and global network in multiple geographically diverse, state-of-the-art, Tier 4 data centers, minimizing the risk of loss and regional service interruption due to natural disasters and other catastrophic situations.

Within each major data center, RingCentral provides high availability, redundant architecture. Access to the internet is ensured through the purchases of multiple internet transits at each data center. All of RingCentral's service components are designed with high availability, fault tolerance, and fault impact segregation in mind. Customer data—including service configurations, messages, etc.—is fully replicated across our data centers in real time.

In the event of a failure, RingCentral's automated systems, in conjunction with an always-on, world-class network operations center (NOC), ensure rapid transition to back-up systems as needed to maintain uninterrupted service availability. RingCentral also performs disaster recovery tests periodically to gauge the system’s high availability for the best, most seamless customer experience possible.

**Data Isolation**

RingCentral provides a multi-tenant environment for our customers and maintains a high degree of security to ensure that one customer’s data is never available to another customer. We use a multi-tenant SQL architecture and dynamic database views to form application layer boundaries between customer instances.

**Account Security as a Shared Responsibility**

**What is Shared Responsibility?**

When customers use RingCentral services, they are operating under a shared security responsibility model. Shared responsibility is a framework adopted by many cloud providers—including Amazon AWS, Microsoft, and Salesforce—to identify the shared responsibilities of both the customer and the cloud provider.

**RingCentral’s Responsibility**

As the cloud provider, RingCentral is responsible for the service delivery, architecture and designing security into the product, as well as ensuring physical and environmental security of the service. We employ a multi-layered security model that includes: security at the perimeter and service delivery layer, SSL on our Web applications, Tier 4 data centers, and customer-controlled settings in the application interface.
Your Responsibility: Security in the Cloud

Our customers are responsible for managing their account policies, granting the correct roles and permissions to users, properly implementing single sign-on, tracking administrative changes made on their RingCentral account, controlling users’ international dialing plans, staying alert for suspicious activity, etc.

Security Assessment and Privacy Compliance

In addition to the security measures deployed as part of the physical and cloud infrastructure, RingCentral undergoes independent verification and audits of our security controls by major partners and third parties. These assessments ensure our customers’ compliance needs are met. Special efforts are undertaken to comply with regulations posed by specific industries.
RingCentral Certifications

SOC 2 Type II

The SOC 2 report validates the effectiveness of our operating controls as a service organization against the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. RingCentral annually undergoes a third-party audit to certify our services against this standard.

A copy of the most recent report is available upon request from your Account Manager or Sales Representative.

SOC 3

Unlike a SOC 2 report, a SOC 3 report can be freely distributed to the public for general use. RingCentral has undergone a third-party audit to certify our services against this standard.

To view RingCentral’s SOC 3 report, click here.

HITRUST

RingCentral Office and the RingCentral app have earned Certified status for information security by HITRUST. HITRUST CSF Certified status indicates that these RingCentral apps have met industry-defined security requirements and are appropriately managing risk. RingCentral joins an elite group of global organizations that have earned this certification.

RingCentral Office HITRUST certification is available here.
To better serve our customers in the highly regulated healthcare industry, RingCentral has implemented HIPAA security safeguards. We annually undergo a third-party SOC 2+ audit—which includes an assessment of controls mapped to the HIPAA Security Rule requirements—that demonstrates the implementation of the security safeguards and requirements outlined in the HIPAA Security Rule.

A copy of the most recent report is available upon request from your Account Manager or Sales Representative.

**Skyhigh’s CloudTrust™**

RingCentral Office has earned the Skyhigh’s CloudTrust™ rating of Enterprise-Ready, the highest rating possible from Skyhigh. Skyhigh provides this status to cloud services that fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

**GDPR**

RingCentral offers customers a robust Data Processing Addendum (“DPA”), governing the relationship between the customer and RingCentral. Our DPA contains strong privacy commitments that few software companies can match and has been updated to confirm our compliance with the GDPR.

To learn more about GDPR and our compliance instance, [click here](#).

In addition, to assist our FINRA-regulated customers with their compliance, we implement the applicable SEC cybersecurity requirements, ensuring all call recordings, call logs, fax exchanges, SMS, MMS, audio and web conferencing, and team messaging communications are in compliance.
Customer Admin Controls

Roles and Permissions

Role-based access controls act like an extra layer of security to help you enforce company security policies by giving you complete oversight into which permissions are in use. With roles, the same level of access is unilaterally given to every user assigned to that role, greatly reducing the chances of producing outlier users with unauthorized levels of access.

Roles can be created for functions or positions in the company with all the appropriate permissions built in. Seven standard, ready-to-use roles make it simple to quickly grant the right level of system access to many users at the same time, virtually eliminating errors that can happen when permissions are set individually.

Custom roles support countless permission combinations, extending your range of granular control over how users can access RingCentral features. For each role, you can select the precise permissions you want to grant and update your selections at any time.

Insider Threats

RingCentral implements measures that allow customers to prevent insider threats via comprehensive administrative controls. This aspect of cloud communications—especially when company policies require employees to make and receive calls from the mobile app—optimizes security and prevents former employees from leaving with valuable customer contacts or competitive information.

The RingCentral cloud service includes front-end settings that customers control to manage their policies and end users. These settings include:

- Adding/removing user extensions
- Setting user permission levels
- Managing extension PINs
- Enabling/disabling international calling
- Allowing specific international call destinations
- Blocking inbound caller IDs
- Disabling message attachments in email notification

Mobile Security

Because mobile devices are easily lost or stolen (and often BYOD), the RingCentral service gives administrators comprehensive mobile app control.

Mobile application management is delivered through enterprise-class user and service controls. These controls are particularly valuable with the RingCentral mobile app, which provides web meetings, video conferencing, and collaboration on smartphones and tablets.

Administrators can instantly revoke the remote user’s access to the cloud network—and thereby to customer contacts, CRM info, and other corporate information. Almost no data resides on the device itself. In addition, customer admins can review the user’s entire activity on desk phones and mobile devices, including call history. These capabilities make it safe to deploy BYOD across an enterprise, employ virtual contact center agents, and extend trust to third parties.
Single Sign-On (SSO)

We offer SSO capabilities in RingCentral apps, making logins seamless across the board. While SSO is convenient for users, it also presents new security challenges. If a user’s primary password is compromised, attackers may be able to gain access to multiple resources. In addition, as sensitive information makes its way to cloud-based services, it is even more important to secure access by implementing two-factor authentication.

Admins can define policies that enforce unique controls for each individual SSO application, which would entail duo checking the user, device, and network against an application’s policy before allowing access to the application. For example, admins could require that CRM users complete two-factor authentication at every login, but only once every seven days when accessing RingCentral.

Audit Trail

Audit trails allow customers to track configuration changes made to their RingCentral account for auditing and troubleshooting purposes. Login attempts, phone number changes, license purchases, and other changes to admin/employee settings and permissions can be identified.

Security for Applications and Developers

For public-facing apps (apps available to be used by anyone), the developer is required to utilize Open Authentication (OAuth), which prevents the transmission of customer credentials to the app and developer server. Instead, upon requesting access to the app, customers are directed to RingCentral, where they will enter their username and password on RingCentral’s site. During this process, customers are informed of the exact permissions the app is requesting, and customers may cancel the request at any time.

If a customer accepts the app’s request for permissions, the app and developer server then receives a bearer token that may be used to act on the customer’s behalf. This token expires if not refreshed by the app and may be revoked by RingCentral or the customer at any time through the RingCentral admin portal.

For private apps, or apps that are intended to be used ONLY by the creating company/developer, developers may use their username and password to request a bearer token. This process helps obfuscate the customer credentials and prevents multiple use and placement of the customer’s credentials; however, because there is no way to prevent customer credentials from being accessed if the app or server is hacked, this method is not recommended.

When it comes to external developers on the RingCentral platform, every developer is required to have a developer account where they register and set permissions for their applications. Each application is assigned a client ID and a client secret. This allows each application to be monitored individually and, if need be, for corrective action (including termination of the application) to be taken if an application’s security is found to be compromised or the intent of the application becomes malicious.

Beyond having a unique client ID and secret, developers must set the specific permissions their application will use. If an application requests more permissions than is needed, it will not be able to be used in production until either those permissions are utilized or removed from the application’s scope. This prevents broad permission requests that may be misused or abused.

As an additional layer of application security, each application must pass through our extensive graduation process, which includes a manual review of the submitted application’s name, description, requested permissions, and rate limits. It also includes automatic checks to ensure the application does not have failing API calls or high error-rates, while also ensuring the application doesn’t use any permissions not requested or have
any permissions requested not being used. Developers are also unable to modify their application type or permissions requested once the application has been made public.

**Conclusion**

At RingCentral, we recognize security as a critical component to every organization’s internal and external communications. As such, we’re committed to providing customers with the highest levels of integrity, confidentiality, compliance, and control.

Combined with a robust back-end infrastructure and dedicated security teams, our multi-layered approach to security ensures that customers’ data and communications are always defended at every stage. This not only protects your business from attacks, but also allows your IT department to focus on business functions rather than phone and UCaaS security.

Today’s organizations need technology vendors that continuously improve their security capabilities while delivering world-class services. We are proud to be one of those vendors and seek to provide our expertise in helping our customers advance their business needs.

For more information, please contact a sales representative.

Visit ringcentral.com or call 855-774-2510.

---

RingCentral, Inc. (NYSE:RNG) is a leading provider of global enterprise cloud communications and collaboration solutions. More flexible and cost-effective than legacy on-premises systems, RingCentral empowers today’s mobile and distributed workforce to communicate, collaborate, and connect from anywhere, on any device. RingCentral unifies voice, video, team messaging and collaboration, conferencing, online meetings, and integrated contact center solutions. RingCentral’s open platform integrates with leading business apps and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

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

©January 2020 RingCentral, Inc. All rights reserved. RingCentral and the RingCentral logo are registered trademarks of RingCentral, Inc. Other third-party marks and logos displayed in this document are the trademarks of their respective owners.