RingCentral

RINGCENTRAL VIDEO SECURITY

White Paper

TABLE OF CONTENTS

RINGCENTRAL VIDEO SECURITY

With the launch of the RingCentral Video platform to unify collaboration across a modern business environment, ensuring secure and private communications is a top-of-mind concern for business users and IT professionals alike. RingCentral Video is a modern online meetings experience powered by the market-leading RingCentral unified communications platform. It combines high-quality video, audio, screen sharing, and team messaging into a collaborative online meeting hub that sparks conversations and fuels ideas—anytime, anywhere, on any device.

At RingCentral, our commitment to security has been proven to be second to none. Now we are extending that security commitment to RingCentral Video. That commitment starts with a global team of cybersecurity experts that participate not just in the planning and development of the platform but also its daily operations. RingCentral, as always, implements:

- Secure software development
- Strong access controls
- Resilient services
- Threat detection and mitigation
- Service operations controls
- Customer admin and user controls
- Built-in support for regulatory requirements
- Secure application programming interfaces (APIs)
- Pre-built integrations
- Transparency

The following RingCentral cloud security model illustrates the approach we take to achieve these security goals:

GOVERNANCE **Risk Management and Measurements**	User Service Administration	Customer Controlled
	Application Security	Designed In and Tested
	Access and Boundary Security	Logins, Registrations, and Data Entering the Service Cloud
	Data Security	Data Encrypted in Transit and At-Rest
	Platform Security	Infrastructure and Operations
	Threat Detection and Mitigation	Detect and Stop Account Takeover and Service Fraud
	Physical Security	Protected Environments and Environmental Controls
	Independent Verification	Third-Party Audits and Security Testing

RingCentral's cloud security model includes the eight risk management factors above, as well as how to measure them.

USER SERVICE ADMINISTRATION

CUSTOMER ADMIN CONTROLS

RingCentral, like most cloud service providers, operates under a shared security responsibility model. This framework identifies the shared responsibilities between the customer and the cloud provider. RingCentral is responsible for the service delivery, architecture, and security of the core service as well as the physical and environmental security of the infrastructure employed to deliver our service. This is a responsibility everyone at RingCentral takes very seriously.

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 international dialing plans, and working with RingCentral to identify suspicious activity.

Administrative controls made available to administrators include:

Roles and permissions

Role-based access controls provide an extra layer of security to help you enforce company security policies by providing complete oversight into which permissions are in use. The same level of access is unilaterally given to every user assigned to that role to ensure a consistent approach can easily be enforced and maintained.

Roles can be created for functions or positions in the company with all the appropriate permissions built in. RingCentral has defined seven standard, ready-to-use roles to 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 can be defined to support countless permission combinations, extending the 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.

Audit trail

Audit trails allow customers to track configuration changes made to a 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.

APPLICATION SECURITY

SECURE SOFTWARE DEVELOPMENT

RingCentral continuously implements best software development practices to ensure security throughout the development, build, deployment, and release phases of any software project, including:

- Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Runtime Application Security Testing (RAST)
- Application scanning
- Analysis of third-party libraries
- Signed commits
- Software composition analysis
- Application programming interface (API) scanning
- Penetration testing

We also digitally sign our executables for integrity protection.

DEVELOPER PLATFORM

Any developer of a public-facing application that runs on RingCentral Video is required to use Open Authentication (OAuth), which prevents the transmission of customer credentials to the application and developer server. Upon requesting access to the third-party application, 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 application is requesting, and customers may cancel the request at any time.

If a customer accepts the application request for permissions, the application 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 application and may be revoked by RingCentral or the customer at any time via the RingCentral Admin Portal.

For private applications that are intended to be used only by the organization that created them, 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 customer credentials. However, because there is no way to prevent customer credentials from being accessed should the application or server be hacked, this method is not recommended.

Every external developer on the RingCentral platform 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, updated or terminated should the application's security be compromised or it's discovered the intent of the application becomes malicious.

Beyond having a unique client ID and secret credentials, 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 employed or removed from the application's scope. This prevents broad permission requests from being misused or abused.

As an additional layer of application security, each application must pass through an 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 that are not being used. Developers are also unable to modify their application type or permissions requested once the application has been made public.

BORDER SECURITY

RingCentral implements security layers 3, 4, and 7 consistent with the Open Systems Interconnection (OSI) model at our service entry points and distributed load balancing to balance traffic across server pools. In addition, distributed denial of service (DDoS) mitigation measures are in place to ensure high availability and service resilience.

DATA SECURITY

Data is encrypted in transit and at rest. RingCentral Video employs WebRTC as a foundational element. As a browser technology, WebRTC requires applications to employ encrypted signaling transport protocols; data streams are encrypted using Datagram Transport Layer Security (DTLS), and media streams are encrypted using Secure Real-time Transport Protocol (SRTP).

Since RingCentral Video is built on top of WebRTC, all the advantages and best practices employed by browser vendors in their security models are also baked into the RingCentral Video application. Browsers that support WebRTC protocols are updated automatically on a bimonthly basis. RingCentral Video offers a frictionless user experience with one-click video calling and guest access with no installation—while simultaneously offering robust security and compliance protocols to protect customers' critical data.

PLATFORM SECURITY

Secure infrastructure, defense in-depth security layers, and service operations controls underlie our platform security. 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. RingCentral implements system hardening practices and ongoing automated vulnerability scanning of servers and device configurations.

RingCentral has a thorough change management process in place. Our change-control practices include 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 rollback procedures and policies in place. We implement configuration monitoring, flow monitoring, EDR, and other monitoring measures.

THREAT DETECTIONS AND MITIGATIONS

RingCentral's service includes multiple measures to prevent and detect service interruptions, account takeover, service abuse, and telecom fraud, including service operations monitoring, access controls, detection controls, usage throttling, and customer-controlled international dialing plans. RingCentral implements Unified Communications Threat Management (UCTM) capabilities to aid in the detection and mitigation of robo calls and other forms of nuisance calling.

In addition, RingCentral's security department performs active monitoring to detect and notify customers of suspicious login activity, unrecognized devices, and anomalous calling patterns on their account.

PHYSICAL SECURITY

Our services are hosted globally in enterprise-class Tier 4 data centers and leading public clouds. Security and availability are top-of-mind considerations when selecting our service delivery locations. These environments include state-of-the-art physical security, environmental controls, and facility operations.

Network operations centers (NOCs) are continually monitored 24/7 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, and each data center is certified SSAE 18 compliant.

INDEPENDENT VERIFICATION

In addition to the security measures throughout product development, production environments, and service operations, RingCentral also engages outside auditors to review our security controls. These assessments ensure our safeguards are verified and tested, with visibility available to our customers. Special efforts are undertaken to comply with specific industry regulations and data privacy laws. They include:

RINGCENTRAL CERTIFICATIONS

HITRUST

RingCentral Video has earned Certified status for information security by HITRUST. HITRUST CSF Certified status indicates that RingCentral Video has met HITRUST's defined security requirements and is appropriately managing cyber security risk. RingCentral joins an elite group of global organizations that have earned this certification.

HIPAA

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—which demonstrates the implementation of the security safeguards and requirements outlined in the HIPAA Security Rule. RingCentral offers HIPAA Business Associate Agreements to covered entities.

A copy of the most recent report is available upon request from your account manager or sales representative.

McAfee's CloudTrust Program

RingCentral has earned a McAfee CloudTrust rating of Enterprise-Ready, the highest rating possible. McAfee 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.

General Data Protection Regulation (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.

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 global security team, our multi-layered approach to security—revolving around multiple disciplines spanning everything from software development to access controls—ensures that customers' data and communications are 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 application 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 while remaining committed to providing them with the highest levels of security, data confidentiality, compliance, availability, and control.

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, collaboration, and contact center solutions. More flexible and cost-effective than legacy on-premises systems, the RingCentral platform empowers employees to work better together from any location, on any device, and via any mode to serve customers, improving business efficiency and customer satisfaction. The company provides unified voice, video meetings, team messaging, digital customer engagement, and integrated contact center solutions for enterprises globally. 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

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