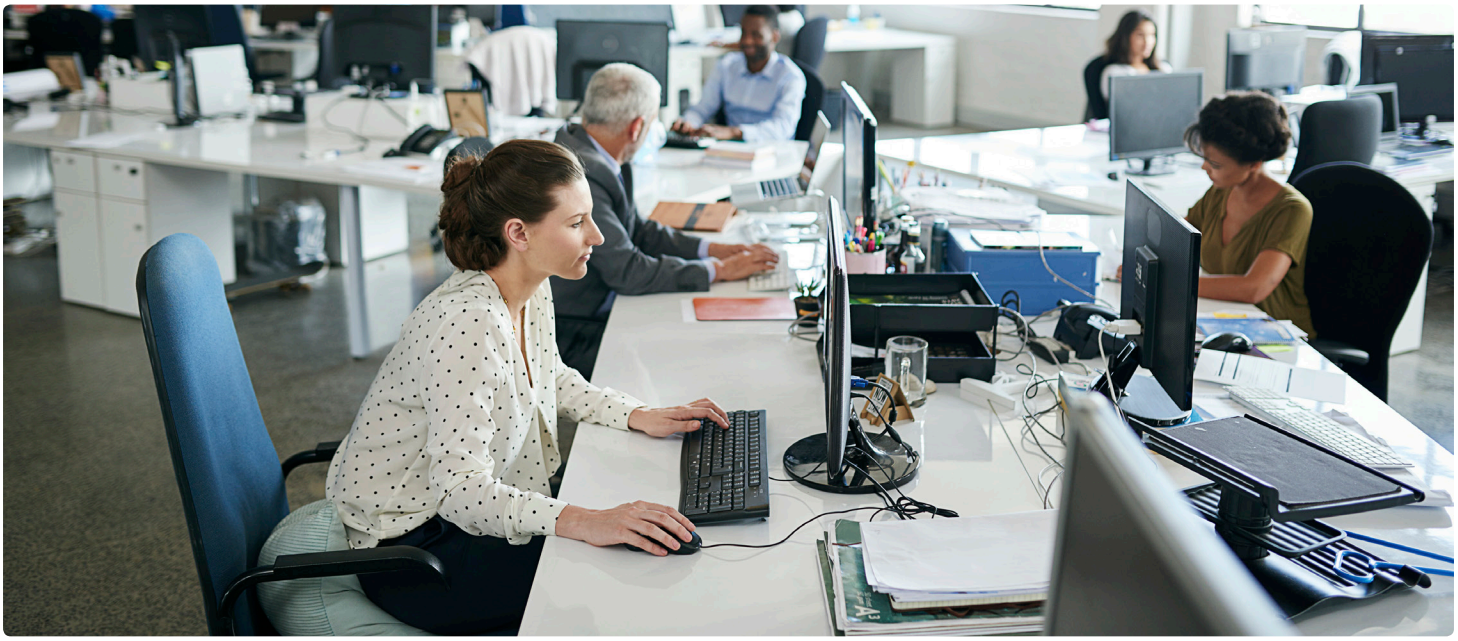
RingCentral App Security

Cloud workplace collaboration originated with knowledge workers leveraging popular consumer productivity applications such as Skype™ and Google Docs™ to share files and exchange ideas. These ad hoc point solutions have evolved into mature cloud-based collaboration software offerings, also known as team messaging apps. They expand the humble instant message window into an immersive collaborative workspace with the context and content teams need to get more work done more effectively. Users can share files and calendars, track tasks, participate in group chats, and more.



As an integrated feature of RingCentral Office®, the RingCentral app takes cloud collaboration to the next level by integrating team messaging with a company-wide unified communications (UC) platform. Access to a centralized communications system in the cloud gives teams the benefits of seamlessly integrated UC features. For instance, with one click, RingCentral app users can escalate a group chat session to an audio or HD video conference.

This white paper looks at the measures that protect the RingCentral app system components and user data. It also details the robust security included in RingCentral Office and the RingCentral Global Connect Network™.

Securely deploying collaboration software

Enterprise IT departments planning to deploy the RingCentral app will naturally have questions regarding security. Moving your business communications and collaboration to the cloud means sending sensitive data over the public internet—and allowing sensitive or protected data to reside outside the corporate firewall.

With the rampant rise in cybercrime and other types of hacking, as well as the advent of stricter privacy regulations, security and compliance have also become key considerations in communications systems. Essentially, desk phones, smartphones, and UC systems have become part of the data network.

As a result, in addition to addressing telephony security risks such as eavesdropping on conversations or hacking into voicemail, enterprises must ensure all communications are protected by the same types of data security required to defend the corporate IT network. In fact, protecting phones and UC applications actually requires more sophisticated security.

Inadequate security can have significant cost and penalties

The loss of valuable competitive information or falling into non-compliance with government and industry regulations due to inadequate security can be incredibly costly. For instance, violations of the Payment Card Industry Data Security Standard (PCI DSS) governing credit card payments may result in fines up to USD $500,000/incident. Even more alarming is the fact that many IT professionals and business leaders are unaware of stiff new criminal penalties for data breaches. Under HIPAA, for example, a breach that discloses patients' protected health information—even where there was reasonable cause or the company had no knowledge of violation—can result in up to one year in jail. Additionally, businesses are now responsible for demonstrating that their upstream business associates—such as cloud service providers—are compliant with the security practices mandated by these regulations.

Extending trust to the cloud

Cloud-based services transfer the cost and time required to purchase and manage infrastructure to outside experts. This approach frees internal teams to focus on enhancing the business. Hosted team messaging solutions and cloud phone systems provide similar benefits.

However, trusting operations and confidential data to another company can quite naturally raise some eyebrows. This is why it is critical to choose a trustworthy cloud vendor, which means an established company with ownership of its platform, many satisfied customers, and robust cloud security. This vendor should also be able to show evidence of independently validated security, ideally in the form of an audited Service Organization Control (SOC) 2 or 3 report.

RingCentral app security

Cloud collaboration is taking the enterprise by storm. Unfortunately, in many organizations, users have gotten the jump on IT, and are downloading a disparate mix of consumer-grade apps. Users appreciate the features and user friendliness of these apps. However, while vendors have addressed concerns for consumer privacy with a focus on encryption, these apps do not typically meet IT's broader needs for security and control, such as PCI compliance, for example.

RingCentral app system component: infrastructure

The RingCentral app is hosted by Amazon Web Services (AWS) under an infrastructure as a service (IaaS) cloud computing model. Cloud security is the highest priority at AWS, and RingCentral customers benefit from an AWS data center and network architecture built to meet the requirements of the most security-sensitive organizations. The RingCentral app Amazon Virtual Private Cloud (Amazon VPC) is logically isolated from other virtual networks in the AWS cloud. Its virtual network closely resembles a traditional network with the benefits of using the scalable infrastructure of AWS. The main security features include:

- **Firewalls**
  The RingCentral app's network and application perimeter is secured by several overlapping layers of protection. A Fortinet virtual appliance provides the system with a firewall, security gateway, intrusion prevention, and web application security. Access to our security appliance requires authentication from the RingCentral Office production network and an SSL-VPN connection. The system is also protected by security groups, which ensure that only known application ports are available to the internet.
- **Access management**
  Access to the RingCentral app's production network is tightly controlled. Only authorized and approved users are given access to the production network. The RingCentral app uses AWS's Identity and Access Management (IAM) web service to securely control access to the RingCentral app VPC and related infrastructure components. RingCentral controls who can use its AWS resources (authentication) and what resources they can use and in what ways (authorization) in support of deployments, maintenance, and monitoring. RingCentral also uses Active

Directory and security groups to manage and secure the system. All access is given based on "least privilege" and "need to know" bases. All access requests and approvals are recorded in the ticketing system.

Security groups and rules

The RingCentral app uses security groups, which act as virtual firewalls, to control inbound and outbound traffic. Each singular instance (within each subnet) is assigned a minimum of one security group. Rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic have been designed for each security group. Access to the RingCentral app security groups is controlled through AWS's IAM service. Security Groups prevent individuals with development accounts from bypassing Active Directory authentication (e.g., by copying their SSH keys to access development instances). RingCentral further uses a network address translation (NAT) instance in its public subnet within the RingCentral app VPC to enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services, while preventing the instances from receiving inbound traffic initiated by someone on the internet.

By default, new internal RingCentral app users are given both Active Directory credentials and limited access to an empty home directory with no write permissions and restricted privileges. This ensures that no unauthorized files can be installed via SSH into the RingCentral app VPC. RingCentral app users requiring development accounts are provided with an IAM account with an API key pair. Individuals logging in to development instances are provided with a centrally mounted network file system (NFS) home directory to which they have complete access. IAM and Security Groups control development account access as described above.

RingCentral Office security

As a feature of the RingCentral Office cloud communications service, the RingCentral app relies on and benefits from the extensive security of the RingCentral system. Recognized as a Leader in the 2015, 2016, 2017, and 2018 Gartner Magic Quadrant for Unified Communications as a Service (UCaaS), Worldwide, RingCentral has a proven track record of supplying cloud business communications services to hundreds of thousands of customers worldwide. It securely and reliably handles billions of minutes of voice traffic every year. RingCentral provides organizations peace of mind by instituting robust security measures at every level of our architecture and processes. These include the physical, infrastructure, host, data, application, and business processes, as well as recommended best practices as the enterprise level of your organization (Fig 1).

Two-factor authentication

Access to the RingCentral app system infrastructure requires two-factor authentication, which comprises an RSA SecurID software token residing on a RingCentral app corporate-owned device together with valid RingCentral VPN credentials.

Data encryption

All traffic between clients (mobile and web) is required to be encrypted using industry standards. In the event that RingCentral app customers have email systems that do not support SMTP with TLS, their email would not be encrypted.

All customer data is stored on Amazon resources that utilize encryption at rest as described within AWS's Service Organization Control (SOC) report. Our application logs are encrypted as well.

Additionally, we use AWS's Key Management Service (KMS) to create and control the encryption keys used to encrypt data, together with AWS's Hardware Security Module (HSM) to protect the security of our keys. Logs of key usage are maintained by AWS's CloudTrail.

VPN

A secure VPN border segments production systems from RingCentral corporate systems. Access to the RingCentral app production network is restricted to authorized personnel as described above. RingCentral Operations staff must enter their production VPN credentials to access the production network and production systems.

An independent auditor's SOC 2 reporting on controls at a service organization is available for the RingCentral app. It provides greater detail under non-disclosure of the service's security and availability.

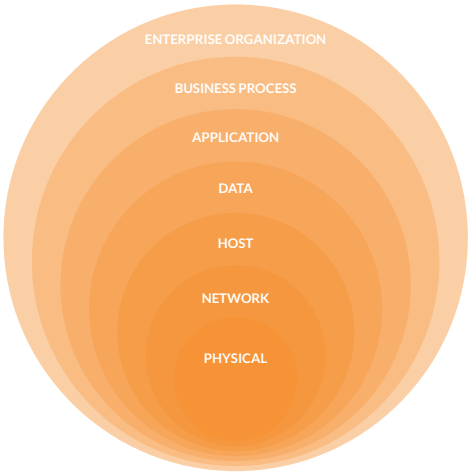


Fig 1. Seven layers of security: RingCentral provides organizations peace of mind by instituting robust security measures at every level of our architecture and processes. These include the physical, infrastructure, host, data, application, and business processes, as well as recommended best practices as the enterprise level of your organization.

Data infrastructure and global network security measures

Some of the specific security measures that protect the RingCentral system and global network include:

- Logging
- Monitoring
- Network protection
- Intrusion detection
- Third-party vulnerability testing
- Vulnerability management
- System user authentication
- Network device and production environment access and authorization
- Access authorization
- Patch management
- Document portal
- Change management

Industry-leading UCaaS security

The RingCentral platform provides industry-leading UCaaS security to protect customers from growing cyber threats, eavesdropping on voice communications, non-compliance with privacy regulations, and other security risks. It details a multilayer cloud security approach that extends from physically secure and audited data centers to intrusion detection systems to advanced voice encryption technology. This approach is also open. It includes interoperability with security standards like the Security Assertion Markup Language (SAML) to enable mixing and matching of solutions from best-of-breed security providers, seamless integration with ID management, and strong authentication and Single Sign-on (SSO).

Secure voice

Eavesdropping on phone calls offers a lucrative target for hackers as it can compromise everything from private business information to celebrity secrets. The voice communications of financial institutions, government agencies, healthcare providers, and contact centers also contain a wealth of confidential account information, health records, and payment card data. The rise of industrial espionage—which includes listening in on conversations to obtain trade secrets and competitive information over vulnerable phones—can even impact a nation's economy. In 2015, the FBI launched a major awareness program around the growing threat of what it calls "economic espionage," which it estimates results in the loss of hundreds of billions of US dollars of competitive information to foreign competitors every year.

Intercepting voice conversations carried over legacy phone systems requires either physically accessing phone lines or compromising the Public Switched Telephone Network (PSTN) nodes or the on-site PBXs. As a result, only a few high securityconscious organizations bother to encrypt voice traffic over traditional telephone lines.

However, with IP telephony—whether cloud VoIP or an on-premise IP-PBX system—calls travel as data packets over the internet, making them susceptible to all the attacks that occur on public networks. Thus, VoIP services must address concerns both in securing the control plane (which allows two speaking parties to set up, modify, and terminate a phone call) and the data plane (the actual voice and media packets). For example, someone snooping on a line from an IP-PBX would have access to all the call data and could reconstruct the entire communication. Or, by hijacking the control plane, the call could be routed to the attacker rather than to the intended destination. In other words, while this configuration is more efficient than the PSTN network architecture and offers benefits such as lower cost, routing traffic over the internet is inherently less secure than placing a call over traditional circuit switched networks (legacy phone systems).

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 is among the first in the industry to use 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.

SRTP is ideal for protecting VoIP traffic because it can be used in conjunction with header compression and has no effect on IP quality of service (QoS)—does not result in any degradation of voice quality. These capabilities provide significant advantages, especially for voice traffic using low-bitrate and adaptive voice

codecs such as G.729, iLBC, and Opus, which RingCentral has adopted to deliver improved voice quality.

Hardened, geographically dispersed data centers

Tier 1 data centers located on both US coasts house the core RingCentral technology infrastructure and inter-work with international data centers to provide our global network. These facilities are monitored 24/7 and certified SSAE 16 SOC 2 and SOC 3 compliant. The data centers are managed by highly trained, on-site engineering specialists, including experts in various aspects of security and regulatory compliance with privacy regulations such as the PCI DSS and the California Security Breach Information Act (SB-1386). RingCentral can also enter into a HIPAA Business Associate Agreement (BAA) with qualified customers.

Each RingCentral data center is supported by redundant power and protected by an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility. All equipment areas are monitored and recorded using CCTV, and all access points are controlled. Every data center is staffed with security officers on duty 24 hours a day. Visitors are screened upon entry to verify identity, and then escorted to appropriate locations. Access history is recorded for audit by customers. All employees also receive stringent background checks before gaining access to sensitive areas.

Data center physical security features include:

- 24/7/365 security and monitoring
- All doors secured with biometric readers
- Kinetic and key locks on closed cabinets
- Critical areas have windowless exteriors
- CCTV digital camera coverage with detailed surveillance and audit logs
- Bullet-resistant protection
- CCTV integrated with access control and alarm system
- Motion detection for lighting
- Equipment check upon arrival

This shared security environment and policy platform offers an inherent advantage to businesses without very large IT departments. These customers benefit from economies of scale provided by leveraging RingCentral security expertise and hardened facilities. Few IT organizations have or want to acquire all of the latest knowledge of security and compliance applicable to phone and UC systems. And having that know-how plus strong physical security at many business locations—each with its own on-premise systems—would not be cost effective. This is one way that moving to cloud-based business communications can actually raise an organization's security capabilities.

Encryption of data at rest and in transit

Data encryption protects sensitive customer and call data from unauthorized access. In addition, numerous state, federal, and industry regulations regarding customer and patient privacy mandate encryption of data and auditable record keeping and reporting. The RingCentral solution ensures that customer calls and messages are secure with encryption in transit and at rest.

These protections include encrypted data transfer, physical protections at data centers, comprehensive digital tracking with clear audit trails, secure file storage, and other methods to help customers defend against data loss and comply with regulations such as HIPAA, the Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley (GLBA) acts, as well as PCI mandates for protecting online transactions.

Network security: protecting service applications

Whether it is hackers attempting to disrupt service or breach confidential data, most successful attacks target the application layer. This threat vector applies to corporate web servers and databases as well as cloud communications service applications. A voice over IP 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 that are 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 security also overcomes the typical set of firewall traversal problems in VoIP systems with network address translation (NAT) support for static IP configuration and "Keep-Alive" SIP signaling. This maintains user addressability without providing attackers the opportunity to infiltrate further.

User management and rights revocation

Whether it concerns control over Sales staff, a key employee in Finance, or virtual contact center employees, enterprise-grade security requires methods to prevent insider threats, which include enabling administrators to revoke the user rights of former employees. This aspect of cloud communications—especially when company policies require employees to make and receive calls from the mobile app—improves 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 extensions, setting user permission levels, managing extension PINs, enabling/disabling international calling, allowing specific international call destinations, and blocking inbound caller IDs.

Because mobile devices are easily lost or stolen (and often BYOD), the RingCentral service gives administrators robust 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—and 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

As business applications—including communications—move from on-premise to cloud hosted solutions, users experience password fatigue due to disparate logons for different applications. Single Sign-on (SSO) technologies seek to unify identities across systems and reduce the number of different credentials a user has to remember or input to gain access to resources.

While SSO is convenient for users, it 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-hosted services, it is even more important to secure access by implementing two-factor authentication.

The RingCentral Duo Access Gateway (DAG) provides strong authentication and a flexible policy engine on top of RingCentral logins using the SAML 2.0 authentication standard. It authenticates users leveraging existing on-premise or cloud-based directory credentials and prompts for two-factor authentication before permitting access to RingCentral.

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 Salesforce users complete two-factor authentication at every login, but only once every seven days when accessing RingCentral.

HIPAA

Our enterprise-grade security is built to protect the data and communications of organizations, their partners, and patients. By being HITRUST certified and offering HIPAA Business Associate Agreements to covered entities, RingCentral delivers a solution ideal for healthcare organizations.

Other security measures

Personnel practices

RingCentral conducts background checks on all prospective employees. Once hired, all employees receive initial security training and additional training on an ongoing basis. RingCentral requires all employees to read and sign a comprehensive information security policy covering the security, availability, and confidentiality of RingCentral Office and the RingCentral app.

Personnel and physical security/environmental controls

As noted previously in this paper, the RingCentral app is hosted by AWS, which maintains the physical security and media handling controls for its data centers. Separately, physical access to our corporate information resources is controlled by access cards, which are used to identify, authenticate, and monitor all admittance attempts. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. As defined in the Information Security Policy, our personnel are encouraged to challenge strangers on premises. Physical security procedures require personnel authorized to enter secured areas escort any personnel that does not have appropriate security clearance. Terminated employees have their access badges revoked immediately. Visitors are required to sign in with their name, firm name, and employee authorizing access. Logs of visitors are maintained for a minimum of three months.

Proactive fraud mitigation

RingCentral prevents toll fraud through access control, detection controls, and usage throttling, and gives the customer granular control over who gets to make international calls and to where. Plus, our global security department actively monitors customers' accounts to detect irregular calling patterns and prevent fraudulent charges.

Security audits

All systems are audited on a periodic basis, and audit reports are available to customers by contacting their account manager or sales representative.

Conclusion

With the rapidly growing popularity of team messaging apps, many enterprises are looking to deploy secure and standardized solutions. The RingCentral app serves IT's needs for security, simplified management, control, and cost-effectiveness. At the same time, it delivers the features and ease of use that employees want. Organizations can also gain important synergies by deploying the RingCentral app as an integrated component of the RingCentral cloud phone system.

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

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

58737514 12/2018