

RingCentral Cloud Communications Security

White Paper



RingCentral Cloud Communications Security

Modern businesses are increasingly concerned about comprehensive security, as threats continue to grow. Employees are more mobile and using differentiated services, requiring in-depth security at all levels. Coupled with the major shift of enterprise adoption in global cloud solutions, the pressure and responsibility of protecting corporate data has subsequently increased.

The cloud workplace offers a powerful, flexible, and reliable platform for productivity applications, but also an equally compelling platform for business communications solutions including phone, fax, voice, short message service (SMS/MMS) text, video conferencing, and team collaboration chat. With the ability to operate within an immersive collaborative cloud workspace, teams can get more work done more effectively, yet demands security be a top priority for IT and business leaders.

Inadequate security can have significant cost and penalties on an organization's bottom line. 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 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 (PHI)—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.

Because businesses are using the cloud to unite their global workforces and enable their remote and mobile staff, this white paper dives into the measures that RingCentral has taken to protect its Cloud Communications and Collaboration solution components and user data. With this white paper, you will gain insight into the level of detail, robust security, and trust that is included in the RingCentral Global Network.

In today's world, there is no higher priority for companies than the security of their customer data. When businesses implement on-premises solutions, they take on full responsibility for data security and regulatory compliance. Companies in highly regulated industries, such as financial services and healthcare, have an even higher threshold to ensure that their solutions and vendors are compliant. But few IT organizations can afford 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, is neither practical nor cost effective.

With a hosted cloud communications solution, companies have access to greater security measures to protect customer information than with traditional on-premises PBX systems. A shared security environment and policy platform offers an inherent advantage to businesses without large IT departments or those spread across multiple locations. 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 business solution can actually raise an organization's security posture.

Cloud communications

PBX systems are designed to route calls within buildings via wires and connect those calls to a public telephone system. They were never designed to accommodate mobile devices outside of the building network. This requires limited solutions, such as requiring mobile users to dial in to the PBX to access company voicemail. These connectivity issues create a range of challenges for internal communications, customers, and enterprises as a whole.

For the enterprise as a whole, the PBX paradigm presents serious security concerns. Critical corporate data could be compromised if just one mobile device is lost, stolen, or hacked. PBX systems are designed to route calls within buildings via wires and connect those calls to a public telephone system. They were never designed to accommodate mobile devices outside of the building network. This requires complicated problem solving, such as requiring mobile users to dial in to the PBX to access company voicemail.

Extending trust to the cloud

Cloud 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.

Securely deploying collaboration software

Enterprise IT departments planning to deploy RingCentral 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.

Robust security

With a hosted cloud solution such as UCaaS, companies have access to greater security measures to protect customer information than with traditional on-premises PBX systems. An enterprise-class UCaaS provider will typically house all customer data in secure tier 4 data centers with strong physical and network security audited by independent third parties. The data centers should be managed by highly trained, on-site engineering specialists, including experts in various aspects of security and regulatory compliance.

The RingCentral solution provides industry-leading UCaaS security to protect customers from growing cyber threats, eavesdropping on voice communications, 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 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 security conscious organizations bother to encrypt voice traffic over traditional telephone lines.

Data infrastructure and global network security measures

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

- Call 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

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

Hardened, geographically dispersed data centers

Tier 4 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 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 provide healthcare organizations that need to protect patient data with a HIPAA setting, or can 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.

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 HIPAA setting 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 FINRA cybersecurity requirements, 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 (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 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.

Single Sign-on

As business applications—including communications—move from on-premises to cloud-hosted solutions, users experience password fatigue due to disparate logins 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-premises 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.

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, 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 Phone™ 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.

HIPAA Conduit setting

In addition to implementing the security practices mandated by HIPAA, such as encryption of data at rest, RingCentral enables customers to protect Protected Health Information (PHI) in faxes, voicemails, and call recordings through the use of a HIPAA setting. With the setting in place, all voicemails, faxes, and call recordings are deleted within 30 days. This ensures that the provider may use the RingCentral service without impacting its HIPAA compliance. This setting does not implement HIPAA-required protections. Instead, it makes them non-applicable by limiting RingCentral's role to that of a "mere conduit" through which PHI passes. Note: Qualifying customers who require a contractual agreement regarding safeguards on PHI can apply to enroll in a Business Associate Agreements (BAA) program as well.

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 outright extortion to simple lulz. 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 an 180% increase in DDoS attacks. Security firm Corero predicted the highly sophisticated, adaptive, and powerful Dark DDoS attack would grow exponentially.

RingCentral app security

Businesses looking to modernize their team communications have a lot of options and many of these apps seem like they do roughly the same thing. The RingCentral app is part of a movement toward using modern messaging that works as well on smartphones as on computers and gives coworkers an alternative to email for team communications and collaboration. This type of application goes by many names, including team messaging, team collaboration, persistent team chat, and workstream communications and collaboration.

RingCentral app system component: infrastructure

The service 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:** RingCentral'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. It 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

RingCentral 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 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 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 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.

Two-factor authentication

Access to the RingCentral system infrastructure requires two-factor authentication, which comprises an RSA SecurID software token residing on a corporate-owned device together with valid RingCentral VPN credentials. All traffic between clients (mobile and web) is required to be encrypted using industry standards. In the event that RingCentral 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.

Other security measures

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.

Personnel and physical security/environmental controls

As noted previously in this paper, the RingCentral app system 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.

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 the RingCentral services.

Compliance with FINRA Cyber Security Controls and HITRUST CSF Certification

RingCentral has compliance in security controls established by the Financial Industry Regulatory Authority, Inc. (FINRA) for cloud service providers. In addition, RingCentral has earned Certified status for information security by the Health Information Trust (HITRUST) Alliance.

FINRA, a private corporation that acts as a self-regulatory organization for member brokerage firms and exchange markets, ensures over 4,200 organizations remain compliant. Through compliance with applicable FINRA cyber security controls, RingCentral's financial customers, including banks, brokers, and traders, can trust that RingCentral Office products meet regulatory requirements for security and reliability. All RingCentral call recordings, call logs, fax exchanges, SMS, MMS, audio and web conferencing, and instant chat messages meet the cyber security controls of FINRA.

Similarly, with the HITRUST CSF Certified status, RingCentral meets key healthcare regulations and requirements for protecting and securing sensitive private healthcare information. HITRUST CSF Certified status indicates that RingCentral has met industry-defined requirements and are appropriately managing risk, alongside an elite group of organizations worldwide that have earned this certification. By including relevant standards and frameworks, and incorporating a risk-based approach, the HITRUST CSF helps organizations address cyber security challenges through a

comprehensive framework of prescriptive and scalable security controls.

It is essential that our customers have confidence that our products meet the highest standards of security and data protection. At RingCentral, it is our top priority to continue to innovate, while ensuring that we keep focused on the latest security and compliance standards. HITRUST CSF Certification sets the highest standard for compliance of healthcare security requirements, and have become the benchmark which organizations apply to safeguard ePHI data.

For financial customers, the cyber security controls of FINRA will enable them to:

- Communicate securely using RingCentral products
- Ensure RingCentral cloud communications technologies remain suitable for the needs of securities brokers and dealers doing business in the US

For customers in the healthcare industry, HITRUST CSF Certified status ensures that RingCentral:

- Meets HITRUST requirements for protecting and securing sensitive private healthcare information
- Implements a comprehensive framework of prescriptive and scalable security controls for our healthcare customers

Conclusion

With RingCentral, customers are provided with dedicated security and fraud teams that protect them around the clock, while geographically, physically, and logically hardened data centers and strong network security safeguard the perimeter as well as core infrastructure of the cloud phone service. Having these protections combined with leading experts on staff not only protects your data—and protects your business from fraud—but also allows your IT department to focus on business functions rather than phone and UCaaS security.

With the rapidly growing popularity of cloud communications solutions, many enterprises are looking to deploy secure and standardized solutions. RingCentral 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.

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

©2018 RingCentral, Inc. All rights reserved. RingCentral, RingCentral Office, 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.