RingCentral

Comprehensive Cloud Security

White Paper

Comprehensive Cloud Security

Enhancing enterprise security for UCaaS

Across industries, the cloud is transforming the way organisations communicate and collaborate—internally as well as with customers and partners. By accessing one centralised communications system in the cloud, businesses can leverage the benefits of voice over internet protocol (VoIP) telephony combined with productivity features such as team messaging, online meetings, mobility, and more.

The need for comprehensive cloud security

The 2019 Cloud Adoption and Risk Report by Skyhigh Networks found that organisations use approximately 1,935 cloud services each, although most think they only use 30. However, doubts persist when it comes to whether the cloud is secure enough for core enterprise applications. According to IDG's Cloud Adoption Survey in 2018, one of the primary concerns that inhibit cloud adoption remains security (Figure 1).

Moving your business communications and collaboration solution to the cloud means sending confidential voice conversations and sensitive data over the public internet and allowing sensitive or protected data to reside outside your firewall. Additionally, today's mobile and distributed workforces require access to the corporate phone system anywhere and from any type of device—and more and more that means an employee-owned smartphone, laptop, or tablet. These workers have also become accustomed to the convenience of using internet applications such as file hosting services, which are notoriously uncontrolled.

Security and compliance have become key considerations in communications systems now that phone and unified communications systems have become part of the data network. In addition to addressing telephony risks such as eavesdropping on conversations, toll fraud, or hacking into voicemail, enterprises must ensure communications are protected by the same types of data protection required to defend the corporate IT network.

While cybercriminals have previously focused on attacking computers and servers over data networks, today they may take down a phone system by overwhelming the service with distributed denial-of-service (DDoS) attacks that generate millions of calls

This document describes the comprehensive cloud security employed by RingCentral to help protect customers from growing cyber threats, eavesdropping on voice communications, toll fraud, non-compliance with privacy regulations, and other security risks. It details a multilayer cloud security approach that extends from physically secure and audited data centres to intrusion detection systems to advanced voice encryption technology.

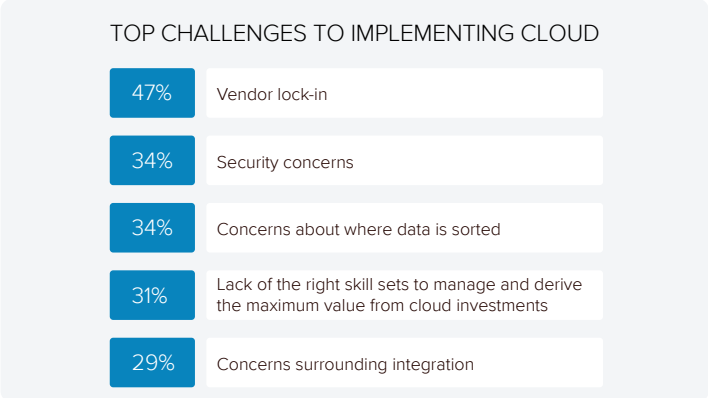

Figure 1. IDG's 2018 Cloud Adoption Survey.

every minute. Or they could hack into your contact centre to spoof legitimate phone numbers and trick callers into revealing National Insurance numbers, date of birth, and other private data. Attackers looking for access to financial or competitive data may also attempt to hack your business phones, mobile devices, and fax and voicemail systems as entry points into your data network and backend systems.

Many businesses are now responsible for demonstrating that their upstream business associates—such as cloud service providers—are compliant with mandated security practices and various government regulations. Therefore, 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—especially since having inadequate security can be incredibly costly. The 2018 Cost of a Data Breach Study, sponsored by IBM Security and conducted independently by the

Ponemon Institute, found that the average cost of a data breach globally is $3.86 million, a 6.4 percent increase from the 2017 report. To avoid these issues, make sure your cloud communications vendor has evidence of independently validated security, ideally in the form of an audited Service Organisation Control (SOC) 2 or 3 report. Without this type of comprehensive and certified security in place, your organisation will risk loss of valuable competitive information or the significant consequences of non-compliance with industry privacy regulations.

Security checklist for vendor selection

When your organisation moves to the cloud, the UCaaS vendor will house and manage all the telephony and data network infrastructure in remote data centres. By choosing the right cloud phone/UCaaS vendor, your organisation can gain the benefits of shifting the business communications systems to the cloud, while enhancing your enterprise security position. Before earning a spot on your short list, the vendor should demonstrate that it provides comprehensive cloud security, including:

- **Secure data centre:** All infrastructure should be housed in facilities with strong physical protection, redundant power, and tested disaster recovery procedures. The highest levels of security and reliability should be backed by independent certifications.
- **Secure voice:** All voice traffic within your corporate phone system should be encrypted to prevent eavesdropping on voice calls.
- **Data encryption:** To ensure protection of valuable intellectual property and competitive information and to ensure regulatory compliance, all data—from competitive proposals to patient private information to smartphone screens shots—should be encrypted in transit and at rest.
- **User access controls and management:** To ensure only authorised users access cloud communications accounts and services, the vendor should implement, at a minimum, strong password policies and ideally two-factor authentication as well as Single Sign-on (SSO) to avoid log-in fatigue.
- **Fraud prevention:** Toll fraud, healthcare fraud, and credentials theft represent significant financial and legal risks for businesses. The service provider should have protections built in to the service layer and should conduct continuous monitoring for dangerous anomalies or other indicators of fraud.
- **Account management and administration:** To prevent data loss, the solution should have provisions to instantly revoke user rights or demote administrator credentials of employees who leave the company or are terminated.
- **Robust network security:** In addition to all the protections for the network perimeters typically in place for data, the UCaaS vendor must now add unique protections designed to prevent attacks on voice infrastructure.

RingCentral's industry-leading security

Recognised as a leader in the 2015, 2016, 2017, 2018, and 2019 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. More than a decade in the making, the RingCentral platform combines voice, audio and HD video conferencing, fax, web meetings, group chat, collaboration, and contact centre capabilities, as well as integrations with leading cloud apps such as Salesforce, Microsoft Office 365, and G Suite. RingCentral securely and reliably handles billions of minutes of voice traffic every year and provides organisations peace of mind by instituting robust security measures at every level of our architecture and processes. Our multilayer cloud security approach extends from physically secure and audited data centres to intrusion detection systems to advanced voice encryption technology (Figure 2). This approach is open, meaning 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.

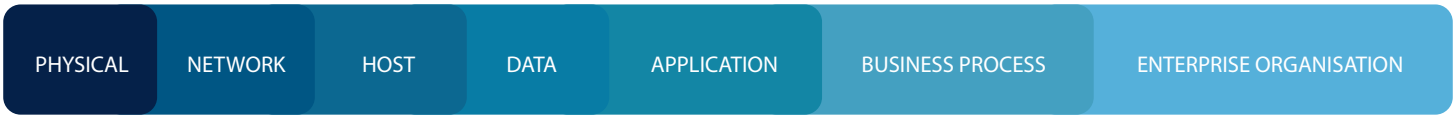

Figure 2. Seven layers of security: RingCentral provides organisations peace of mind by instituting robust security measures at every level of architecture and process. These include physical, infrastructure, host, data, application, and business processes, as well as recommended best practices of the enterprise level of your organisation.

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 authorisation
- Access authorisation
- Patch management
- Document portal
- Change management

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 centres 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.

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 organisations bother to encrypt voice traffic over traditional telephone lines.

However, with IP telephony—whether cloud VoIP or an on-premises 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 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) signalling data. This protocol secures the SIP signalling 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 centres

Located across the world, our Tier 4 data centres share hosted facility space with some of the world's largest technology companies and financial institutions. Our data centres, near the world's top internet exchange points, are collocated with major telecommunications carriers to ensure the fastest response times and interconnect services possible. The geographic diversity of our locations acts as an additional safeguard, minimising our risk of loss and service interruption due to natural disasters and other catastrophic situations.

These facilities are monitored 24/7 and certified SSAE 16 SOC 2 and SOC 3 compliant. The data centres 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.

Each RingCentral data centre 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 centre 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 centre 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 checks 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 organisations have or want to acquire all 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-premises systems—would not be cost effective. This is one way that moving to cloud-based business communications can raise an organisation's security capabilities.

Encryption of data at rest and in transit

Data encryption protects sensitive customer and call data from unauthorised 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 centres, 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 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 optimised 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 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 signalling. 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 centre 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 include employees’ own devices under bring your own device (BYOD) policies, 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 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 centre agents, and extend trust to third parties.

Eliminating the human component of hacking and fraud

Even if your cloud phone service provider implements the highest level of security, cybercriminals can still hack into voicemail systems by using default passwords and easily guessed passwords. They can then use the password pattern to hack into other voice mailboxes in the network. Once they have control of the voice mailbox, they can change the outgoing message to one that dupes automated operators to accept collect calls, or the hackers take advantage of remote notification services to forward the call to an international number.

Even with the sophisticated security capabilities in the RingCentral platform, poor security habits by employees can make your company vulnerable to toll fraud. RingCentral security extends to advising customers on key steps they can take to prevent fraud by establishing policies that require users to:

- Change default passwords
- Make passwords complex
- Not use obvious passwords
- Not use a standard formula for all enterprise passwords
- Change passwords regularly
- Regularly check voicemail greetings
- Check voicemail during holiday/vacation periods
- Block international calls when possible
- Disable automated features that are not used

In addition, IT can add to these measures by making global settings to delete sensitive voicemail messages as soon as users have listened to them. Not storing voicemails is the easiest and most effective way to protect them. IT staff members should also immediately report anomalies. It may not be obvious that a phone has been hacked until an employee reports an odd occurrence, such as a saved voicemail message that has been deleted or forwarded to an unusual number.

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 must 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.

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.

RingCentral carrier-grade reliability includes security features that help to ensure customers' service is not disrupted by any threat. While there is no concrete way to prevent VoIP DDoS attacks—whether the service is on-premises or hosted in the cloud—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 measures designed to prevent DDoS include:

- Session border controllers with anti-DDoS measures
- Protecting against spoofed messages by validating the value of "Call-ID," "Tag," and "Branch" while processing control
- NOTIFY messages
- A caller identification system that authenticates calling numbers via certificates
- The ability to tag and block sources of malicious calls
- Technology layers that include:
  - Intrusion detection systems
  - System logs
  - Fraud analytics
- Internal operational processes that provide:
  - Service-level monitoring
  - System hardening
  - Change management
  - Regular vulnerability scans
- A dedicated team of security experts that monitors and mitigates attempted DDoS attacks in real time, 24/7

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 MVP and the RingCentral app.

Personnel and physical security/environmental controls

The RingCentral app and RingCentral Contact Centre™ is hosted by AWS, which maintains the physical security and media handling controls for its data centres. 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 unauthorised physical intrusion. As defined in the Information Security Policy, our personnel are encouraged to challenge strangers on premises. Physical security procedures require personnel authorised to enter secured areas to 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 authorising 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. In addition, our global security department actively monitors customers' accounts to detect irregular calling patterns and prevent fraudulent charges.

RingCentral has a full-time security and fraud-prevention department with a security programme that is based on industry best practices. This programme provides intelligent communications fraud detection, which includes RingCentral staff monitoring customers' service for anomalous calling that may be toll fraud.

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: The best security policy is selecting a cloud communications provider with comprehensive and layered defences

No technology is more essential to a business than its communications system. However, as organisations adopt UCaaS and telecommunications become more data-centric, phone systems have become susceptible to the same kind of attacks that target data networks.

Your best security policy is choosing a cloud service provider that has designed its infrastructure, products, and network with security in mind. RingCentral provides all of these, including an enterprise-class mobile app that has security built in.

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

For more information, please contact a sales representative. Visit ringcentral.com.au or call 1800 957 188.

RingCentral

RingCentral, Inc. (NYSE: RNG) is a leading provider of global enterprise cloud communications, collaboration, and contact centre 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. That is the promise of Work as One™. The company provides unified voice, video meetings, team messaging, digital customer engagement, and integrated contact centre solutions for enterprises globally. RingCentral's open platform integrates with leading business apps and enables customers to easily customise business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

RingCentral PTY LTD. Level 28, 161 Castlereagh Street, Sydney, NSW 2000, AU

393107168 09/2019