

The CISO Guide to Cloud Communications Security

The essential security, data privacy and compliance requirements for your trusted UCaaS platform.



Table of contents

- Introduction 3
- UCaaS security essentials: The 3 use cases for a platform you can trust 5
- RingCentral: A leading approach to UCaaS trust 7
- In-depth: Information security protection + data privacy and compliance management... 9
 - Physical Security 10
 - Network Security 10
 - Data Encryption..... 10
 - Toll Fraud Prevention 11
 - Incident Response 11
 - Protected Data..... 11
 - Operations Security..... 12
 - Supplier Management 12
 - Data Handling 12
 - Software Development Cycle 12
- In-depth: Global data privacy and security certifications and attestations 13
- In-depth: Security and administrative policy controls 14
 - Video 14
 - Phone 15
 - Message 15
 - Access and Identity..... 15
 - Encryption 15
 - Unified App 16
 - Innovation Spotlight: Dynamic end-to-end Encryption 17
- Conclusion 18

Introduction

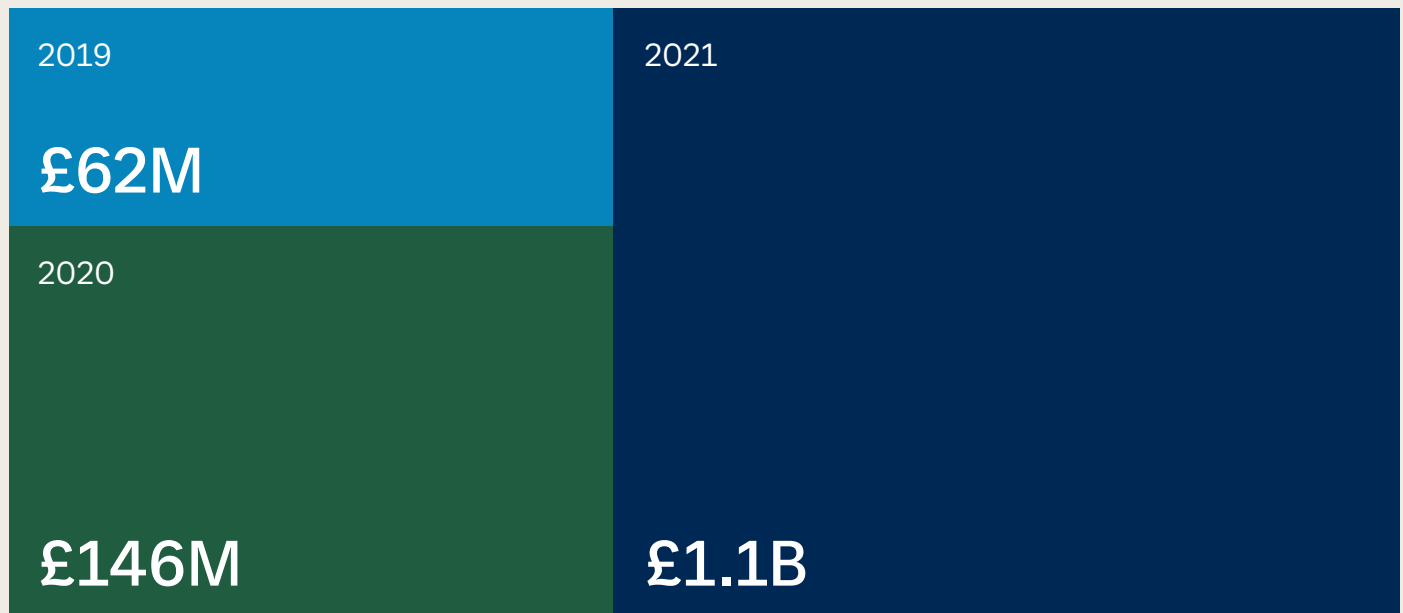
With UCaaS platforms accelerating innovation and sharing in productivity resources like chat, voice and video collaboration, it's crucial for organisations to scrutinise how their UCaaS vendor-of-choice handles security, data privacy and compliance to mitigate the rise of serious financial and brand threats.

These threats are growing at a record pace, so ensuring your UCaaS platform provides a leading approach to mitigating these risks should play a primary role in your buying considerations.

General Data Protection Regulation (GDPR) and its growing fines highlights how essential it is to scrutinise your vendor's data privacy processes and capabilities. In just Q3 of 2021 alone, business fines totalled more than £0.94B.

Evaluating how a UCaaS vendor will maintain your company's data privacy is an important area of focus, given that 62% of businesses are not "completely compliant" with the data regulations that apply to them, including GDPR.

Annual cost of GDPR fines



1. Pymnts.com. GDPR Fines Exceed \$1.1B in Q3. October 2021.

2. Business2Community. Data Compliance Survey: How Seriously Are Businesses Taking Data Privacy Laws?. July 2021.



The risk landscape for UCaaS security extends to other areas as well. Think of it this way: your UCaaS vendor's security infrastructure is, in essence, an extension of your environment.

Your vendor should be transparent about the investments they've made to safeguard your users and data from security threats and data loss, day in and day out.

If your UCaaS vendor's security is lax, then your organisation will be more vulnerable to a breach that can harm your brand value and bottom line. The cost of a single data breach has seen a significant increase in 2021, reaching an average total of £3.48 million per breach. And, according to the IBM Cost of Data Breach Report 2021, successful vishing or smishing attacks have set victims back by £187B in 2021.

This guide outlines how, with the right technical controls, a UCaaS platform can be built with security, privacy and compliance at the centre of its infrastructure investments and innovation strategy.

The guide also demonstrates how RingCentral is leading the way to deliver on that mission with a UCaaS platform you can trust. RingCentral, a Gartner® Magic Quadrant™ Leader for Unified Communications as a Service for seven years in a row, provides transparency and deep expertise to ensure your investment in your UCaaS platform is protected and secured against today's top threats.

£3.4M

Cost of data breach

Increased 143% over 2019

£187B

**Cost of vishing/
smishing**

Detected by IBM Cost of Data Breach Report 2021

£4500

**Cost of downtime
per min**

Estimated by Gartner IT

3. IBM Security. Cost of a Data Breach Report 2021. 2021.

UCaaS security essentials: The 3 use cases for a platform you can trust

What supported use cases do you absolutely need in order to get UCaaS security, privacy and compliance right every time? And to know, consistently, that your platform doesn't present a risk to your brand trust or bottom line?

The essential security formula



**Rigorous information
security protection**



**Comprehensive data
privacy and compliance
management**



**Best practice security
and administrative policy
controls**

In addition, reliability and uptime will serve as the underpin for your platform's foundation of trust by assuring your business continuity.

When it comes to keeping information assets secure, demonstrating cloud security, and committing to safeguard personal data, ISO/IEC 27001 standards are widely known as leading benchmarks for a vendor's information security.

1. Information security protection

From the business infrastructure to the design and processes used for the UCaaS platform itself, your UCaaS vendor must apply airtight security best practices that are always on to provide the peace of mind that your data is safe from compromise.

Your UCaaS vendor must demonstrate that they have applied best-of-breed technologies and stringent operational processes to ensure that your data has rigorous protection at all times.

This should also include details on the security practices of their platform's cloud infrastructure. An approach like this can't be bolted on as an afterthought once a security gap becomes an issue, it must be part of your vendor's DNA that is brought to bear in every aspect of the business.

2. Data privacy and compliance management



Your vendor must be ready to demonstrate their strong commitment to data security and provide details across several areas, including the physical security of their environment, data handling policy, and processes for regular security assessments.

In addition, you should look for validations from compliance attestations and certifications that help speak to the vendors' commitment to data security, such as: SOC 2 Certification, C5, ISO 27001 Certification and others.

With the feature-rich capabilities UCaaS platforms provide, there's a high likelihood of sharing confidential items or personally identifiable information (PII) over the platform, such as sensitive product plans, customer information and employee details.

In fact, that's one of the valuable, business-enabling aspects of UCaaS solutions, so it makes sense that your vendor should have a thoughtful data privacy and compliance management policy that is consistently being followed.

Your vendor should employ an exhaustive system to prevent the inadvertent or intentional compromise of protected data, and they should be transparent about how data is collected and used. This is imperative to establish trust in a vendor's data practices and to validate they're respecting your company's data privacy.

Your vendor should have the most stringent data privacy policies, which will ideally be documented in a comprehensive data privacy notice that is made publically available. In addition, review the vendor's transparency practice for regularly communicating the requests they have received about customer data along with details on how they responded to these requests.

These will provide the assurance you need that your vendor is keeping your data and organisation free of regulatory concerns.

3. Security and administrative policy controls

From waiting rooms to meeting passwords, UCaaS platforms should include comprehensive security capabilities to protect the platform and user experience. Administrative options, such as requiring authentication for meeting attendees, controls on who can enable screen sharing and requiring waiting rooms to authorise attendees to join, safeguard your organisation from data loss and bad actors.

In addition to providing in-depth security and policy controls, your platform should take the guesswork out of which ones to enable by providing best-practice recommendations. This will make it easy to secure your everyday communications.

RingCentral: A leading approach to UCaaS trust

RingCentral is leading the way as the market standard in trusted, unified communications for today's digital and modern business by providing secure and safe communications for every user. We've maintained a long-standing commitment to security, built on a deep expertise in operating and securing unified communications and SaaS products.

Security is in our DNA. We take a multi-dimensional approach to put the safety of your data first by applying innovative technologies and rigorous processes.

World-class security organisation

Built by IT security veterans with over 100 years of experience and a dedicated software development team focused on ensuring platform and data security.



Best-in-class DevSecOps

From our product design to the operations of our business, we employ rigorous security and data best practices in everything we do. We provide our customers with a robust security platform by integrating security principles into the development process from the get-go.

Secure-by-design platform

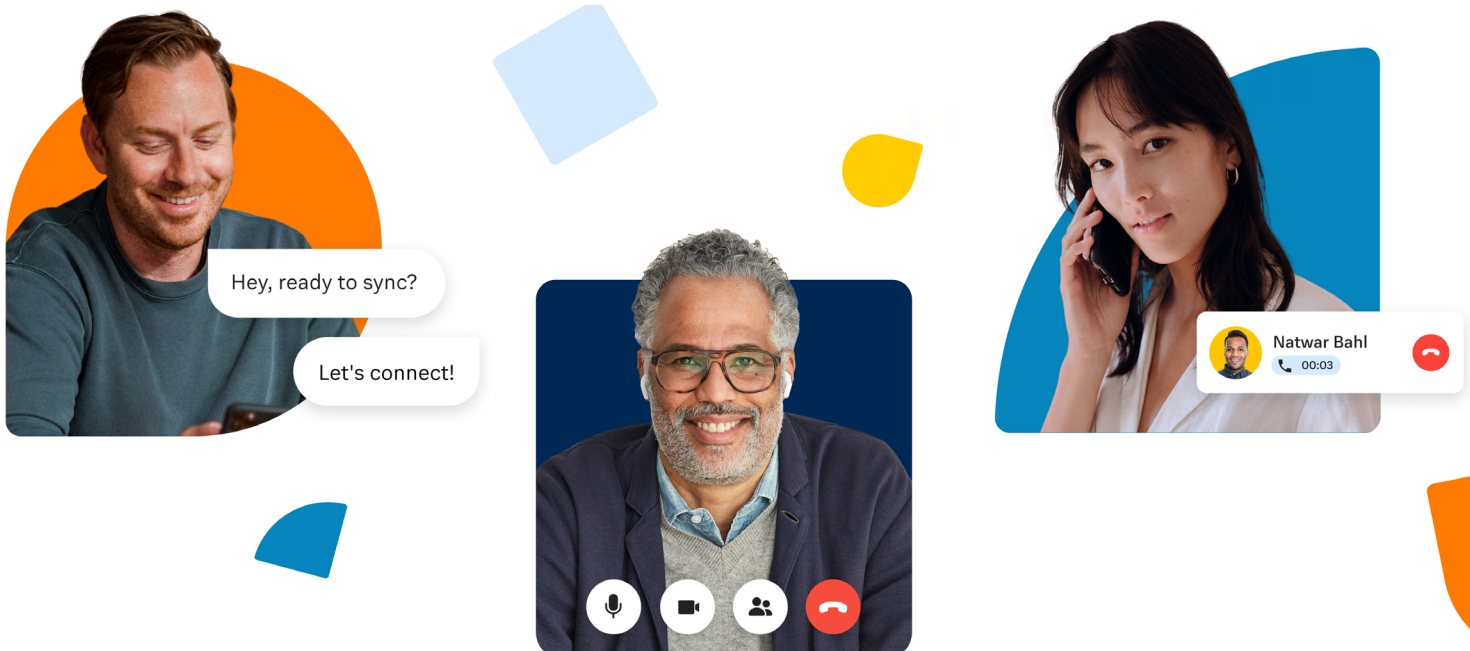
We tirelessly pursue a shared responsibility model where we maintain third-party certifications and attestations that validate our information security policies and practices along with customer controls, so you can directly manage your use case needs.

High reliability and uptime

Experts are proactively monitoring and optimising our platform 24/7/365 to ensure the availability of your service remains at the highest level possible.

We stand by this commitment with an industry-leading service level agreement (SLA) of 99.999% uptime offered in over 45+ countries. And we've consistently met that promise for 12 consecutive quarters.

With over 15 geographically dispersed data centres and media points of presence, RingCentral provides a global infrastructure that ensures 24/7 business continuity for your company, from anywhere.



In-depth: Information security protection + data privacy and compliance management



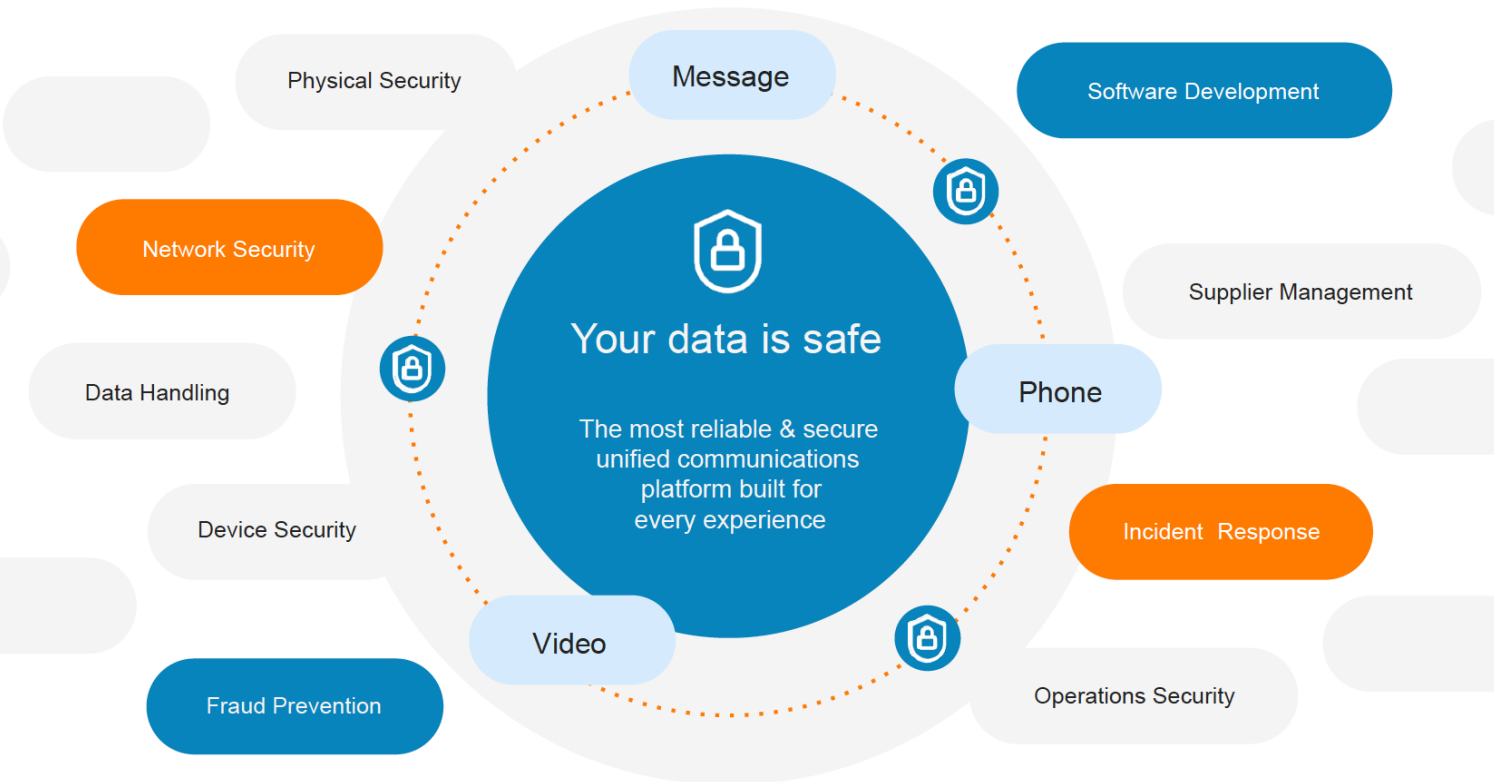
Always-on
Information Security, Privacy & Compliance Management



Customisable / Dynamic
Security & Policy Controls



To give you deeper insight into our stringent practices, let's take a look at the people, process, and technologies we have in place to provide the ultimate customer experience that is safe, compliant and secure.



1. Our secure infrastructure

RingCentral’s security posture consists of numerous controls that reflect the best practices from established information security industry standards. Collectively, these stringent controls allow us to achieve top security practices for our customers. Some of these controls include:

Physical Security

We maintain appropriate physical security controls on a 24-hours-per-day, 7-days-per-week basis, and to the extent that RingCentral operates or uses a data centre, we ensure that physical security controls are in alignment with industry standards such as ISO 27001 and SSAE 16 or ISAE 3402.

Network Security

We maintain a multi-layered network security programme that includes industry-standard firewall protection, intrusion detection systems (IDS), intrusion prevention systems (IPS), DDoS attack and other web threat blocking, two-factor authentication for access to RingCentral’s networks and others. In addition, we run internal and external network vulnerability assessments against our information processing systems at least quarterly to consistently evaluate our network security programme.

Data Encryption

RingCentral encrypts data in transit and at rest, using applicable industry-leading encryption standards and protocols. We apply two, enterprise-grade security protocols to provide additional security for IP phone calls – TLS authentication and SRTP encryption.



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

To address potential vulnerabilities in the VoIP data plane, RingCentral safeguards voice communications with an advanced secure voice technology that prevents call eavesdropping or tampering with audio streams between endpoints.

Toll Fraud Prevention

Our service abuse and fraud management team is regularly monitoring and on the lookout for fraud. We use a range of tools for detection, which encompass:

- Volume, velocity, historical and current trends on specific ranges, numbers dialled and dial-pattern recognition
- Anomalous and or suspicious usage traversing our network
- Unauthorised access of extensions/mailboxes, digital lines, SIP devices and IVRs

Our team responds to alerts from carriers when there is detected activity of anomalous usage, such as high risk and high cost of international ranges, reports of scams (e.g., a RingCentral customer number has been reported of committing scam, defraud, phishing, etc.), as well as any reports of harassment, unsolicited calls or call annoyance.

Incident Response

Our incident response capabilities are designed to comply with statutory and regulatory obligations that cover incident response. To deliver on this, we maintain incident response capabilities to respond to events potentially impacting the confidentiality, integrity or availability of your services or data, including protected data.

Protected Data

We maintain a written information security programme that includes policies for handling



protected data in compliance with the agreement and with applicable law. In addition, it includes administrative, technical and physical safeguards that are designed to protect the confidentiality, integrity and availability of protected data.

Operations Security

Our rigorous operations security programme follows industry best practices across our global organisation, including in-depth security measures for asset management, configuration management, malicious code protection, vulnerability and patch management, as well as log monitoring.

Supplier Management

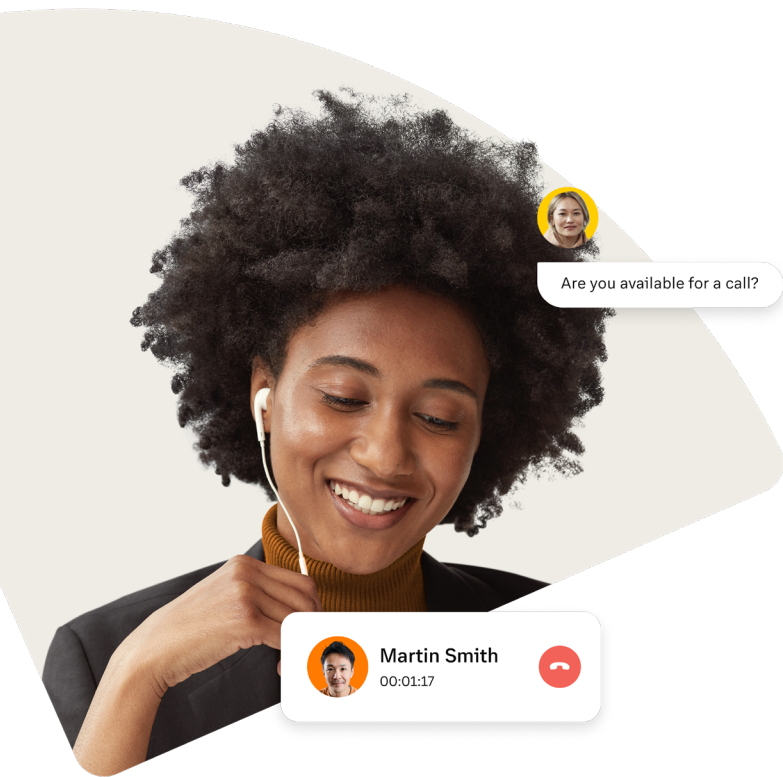
We hold our third-party suppliers to our same high security standards, and we consistently monitor for publicly disclosed vulnerabilities and exposures for impact to our supplier's information systems and products.

Data Handling

RingCentral maintains data classification standards for both public data (i.e., data that is generally available or expected to be known to the public) and confidential data (i.e., data that is not available to the general public, including protected data).

Software Development Cycle

We apply secure development lifecycle practices, including during design, development and test cycles, and we ensure that our products are subject to security reviews, including threat considerations and data handling practices.



ALWAYS ON

2. In-depth: Global data privacy and security certifications and attestations

Our third-party attestations and certifications speak to our commitment to data security. RingCentral is built on a secure cloud platform with a robust portfolio of security and compliance certifications, including:

- SOC 2 attestation
- SOC 3 attestation
- ISO 27001 and ISO 27017-18 certifications
- STIR/SHAKEN (Spam blocking)
- HITRUST certificate
- HIPAA attestation of compliance
- GDPR
- PCI-certified merchant
- PIPEDA
- C5



This means your data is secure, private and compliant across mobile, video, and phone, making RingCentral the most reliable and secure unified cloud communications platform built for every experience. You can see the full list and learn more about our independent certifications [here](#).

3. In-depth: Security and administrative policy controls

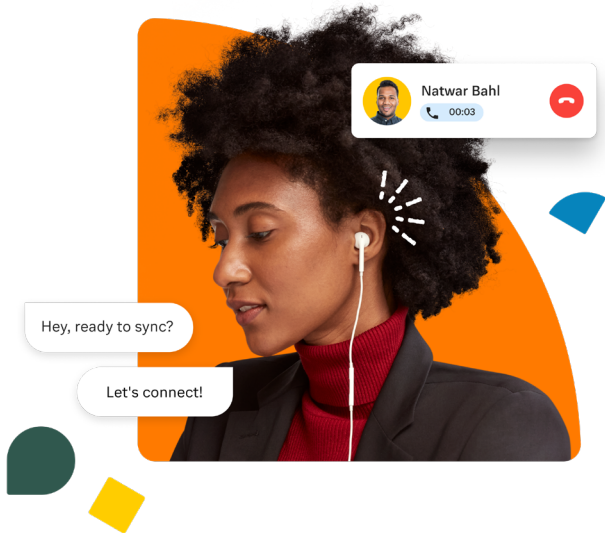
The RingCentral platform provides our customers with leading-edge security and policy controls that ensure a safe and secure experience for your users. Our platform puts a comprehensive set of administrative controls across video, message and phone at your fingertips, such as requiring your meeting attendees to authenticate, limiting who can enable screen sharing and requiring waiting rooms for your users to approve attendees who can join. These provide you with security capabilities to safeguard your organisation from data loss and bad actors.

Video



- Single sign-on (SSO)
- Available via desktop & mobile app, and browser (via WebRTC)
- Require password
- Restrict screen sharing
- Enforce waiting rooms
- Restrict meeting attendance to authenticated users
- Allow user to enable meeting recordings
- Enable moderator turn on/off video for all participants
- Moderator remove participants
- Moderator mute participants
- Virtual background for privacy
- Hide meeting ID
- Control data file sharing

Phone



Message

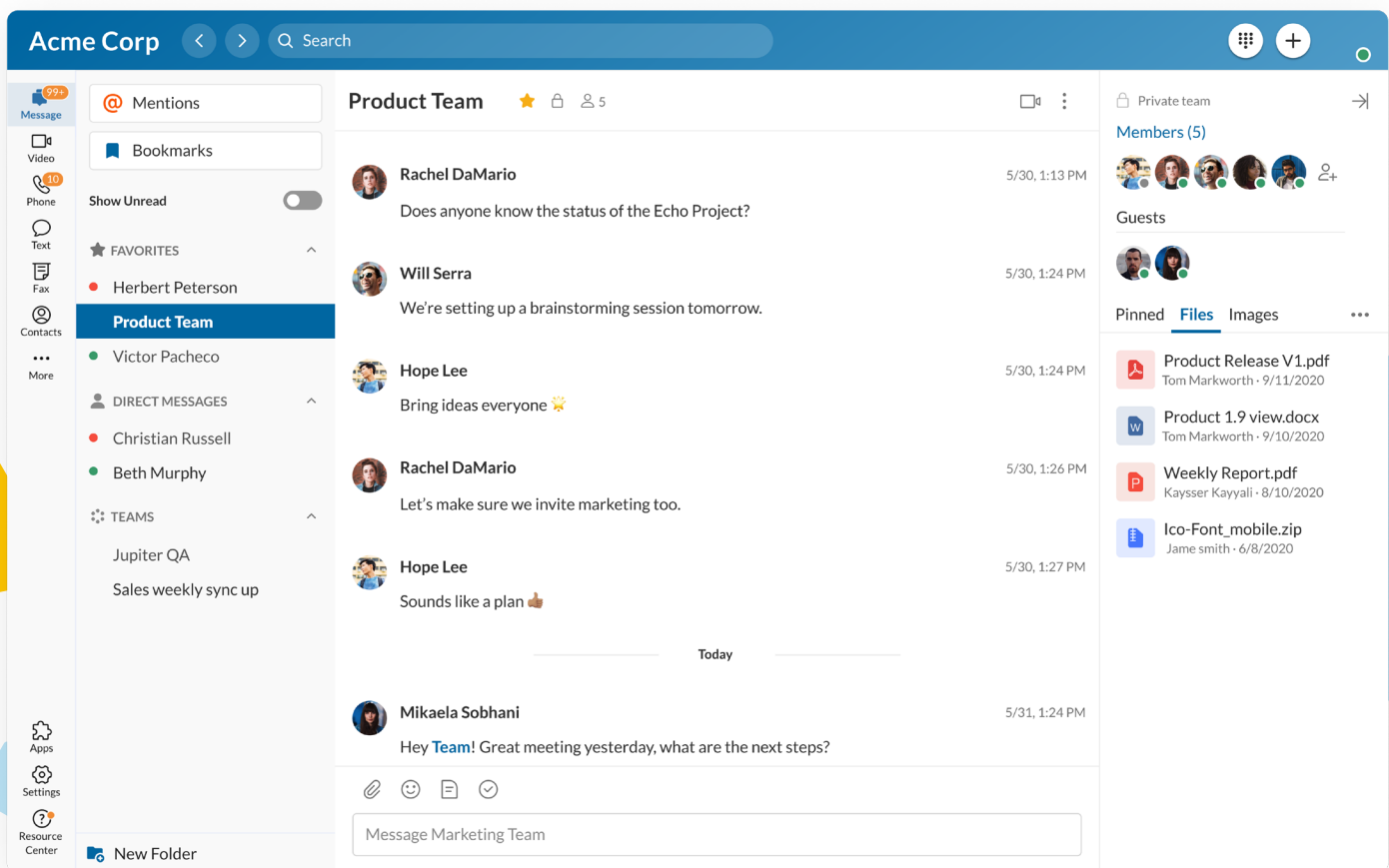
Access and Identity

Encryption

- Audit trail to track changes
- Video meeting insights
- Enable E2EE before meeting
- Dynamically turn on E2EE
- TLS encryption/SRTP secure voice
- Single sign-on (SSO)
- Block phone numbers
- AI-based spam blocking
- RoboCall mitigation using STIR/SHAKEN standards
- Number masking
- RingOut – calling on third-party devices with your business phone number
- Emergency response locations for E999 calls
- Voicemail routing based on business hours
- Analytics portal
- 99.999% SLA uptime
- TLS encryption/SRTP secure voice
- Allow/block list – external guest domains
- Allow/block list – webmail accounts
- Clear guest identification within 1:1 and group chats
- Enforce policies
- SEA FINRA 17a-4
- Single sign-on (SSO)
- Enforced multi-factor authentication (MFA)
- Device PIN enforcement
- User management
- Data-at-rest
- Data-in-transit
- TLS encryption/SRTP secure voice
- E2EE via Message Layer Security (MLS)

Unified App

- Single sign-on (SSO)
- Available via desktop & mobile app, and browser (via WebRTC)
- Require password
- Restrict to authenticated users
- Session timer to logout inactivity
- Authorised apps manager
- VoIP country blocking
- Centralised IT management of free and paid users
- Audit trail to track changes



Innovation spotlight: Dynamic end-to-end encryption



This dynamic layer of privacy enables your users to get the same level of privacy that they'd experience in a face-to-face conversation held in a conference room.

RingCentral made end-to-end encryption (E2EE) available for our flagship MVP video product. With our steadfast commitment to deliver meaningful innovations for our customers and their users, we continued on that milestone to provide E2EE capabilities that your users can dynamically turn on during a meeting, which also protects your traffic from man-in-the-middle attacks.

When a RingCentral Video call uses end-to-end encryption, only the intended participants can view your video conferencing content, including audio, video and in-meeting chat. With RingCentral's dynamic E2EE, you can adjust if you want to turn E2EE 'on' or 'off' during a conversation, on the fly with a push of a button. This simple and powerful control allows communications to become more private should the conversation unexpectedly progress to a more confidential matter.

With alternative vendor solutions, users must pre-determine if a conversation will enable E2EE prior to a call.

At RingCentral, we understand that administrative setup is cumbersome and does not always fit how private conversations spontaneously materialise in real life business or personal situations, so we have built a more flexible E2EE experience for our customers.

Our unique approach uses a fit-for-purpose IETF standard called MLS, or Message Layer Security. What makes MLS so powerful is that it was developed in the public domain with an explicit goal in mind: to enable scalable, secure messaging and communication, making it far more scalable than the E2EE solutions used by other companies.

RingCentral values the importance of providing capabilities that support the practical nature of your work environment; for example, where colleagues want the flexibility to brainstorm or collaborate "off the record." RingCentral's E2EE capabilities, such as guest browser joining and turning on the E2EE feature mid-meeting enables practical use cases for your users' needs. This dynamic layer of privacy enables your users to get the same level of privacy that they'd experience in a face-to-face conversation held in a conference room.

Conclusion

UCaaS platforms play a critical role in fostering an organisation's collaboration to drive growth. Partnering with a UCaaS vendor that places a priority on the security, privacy and maintained compliance of your data will meet your business needs, safely and securely. When you take a close look at buying criteria that assures your continued trusted customer experiences, you'll get your winning platform with RingCentral.

RingCentral offers a fundamentally different approach to global trust for your unified communications platform. From our industry-leading five 9s in uptime reliability to our comprehensive information security protection and global privacy management, you don't have to worry about your data being compromised or falling short of regional regulation standards.

Our innovations and commitment to security, data privacy and compliance have earned RingCentral recognition as a trailblazer in the market, including seven consecutive years being named as a Leader in the Gartner Magic Quadrant for Unified Communications as a Service (UCaaS).

Our approach delivers "always-on" information security protection and data privacy management that keeps your data safe and compliant with the law. And our platform provides a comprehensive toolset for your administrators and users with a breadth of dynamic and real-time controls.

To learn more visit the [RingCentral Trust Centre](#).

For more information, please contact a sales representative. Visit ringcentral.co.uk or call 0800 098 8136.

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact centre solutions based on its Message Video Phone™ (MVP™) global platform. More flexible and cost effective than the on-premises PBX and video conferencing systems it replaces, RingCentral helps employees communicate across devices from wherever they are. RingCentral offers three key products. RingCentral MVP combines team messaging, video meetings, internet phone and other functionalities in a single interface. RingCentral Video™, along with its team messaging feature, enables Smart Video Meetings™. RingCentral Contact Centre gives companies the tools they need to connect with customers across channels. These are available on an open platform that integrates with hundreds of third-party apps and makes it simple to customise workflows. RingCentral is headquartered in Belmont, California, USA, and has offices around the world.

RingCentral

RingCentral UK Ltd. 85 Uxbridge Road, 4th Floor, Ealing, London, W5 5TH, UK. ringcentral.co.uk

© 2022 RingCentral, Inc. All rights reserved. RingCentral and the RingCentral logo are registered trademarks of RingCentral, Inc. Other third-party marks and logos displayed in this document are the trademarks of their respective owners.