RingCentral

US

# The CISO guide to cloud communications security

Information protection, data privacy, compliance management, and more.

# Table of contents


**Introduction** ..... 3

CHAPTER 1

**The high stakes of data security** ..... 4

CHAPTER 2

**Cloud communication security essentials: The 3 use cases for a platform you can trust** ..... 6

1. Information security protection
2. Data privacy and compliance management
3. Security and administrative policy controls

CHAPTER 3

**RingCentral: a leading approach to trusted communications** ..... 9

AI Governance at RingCentral
Use of Artificial Intelligence
AI model training
Best-in class DevSecOps
Secure-by-design platform
High reliability and uptime

CHAPTER 4

**In-depth: Information security protection + data privacy and compliance management** ..... 12

ALWAYS ON

**1. Our secure infrastructure**

Physical security
Network security
Data encryption
Toll fraud prevention
Incident response
Protected data
Operations security
Supplier management
Data handling
Software development cycle

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

**3. In-depth: Security and administrative policy controls**

Phone
Message
Video
Contact Center
Access and identity
Encryption
Unified app

CHAPTER 5

**Innovation spotlight: End-to-end encryption for calls and meetings** ..... 19

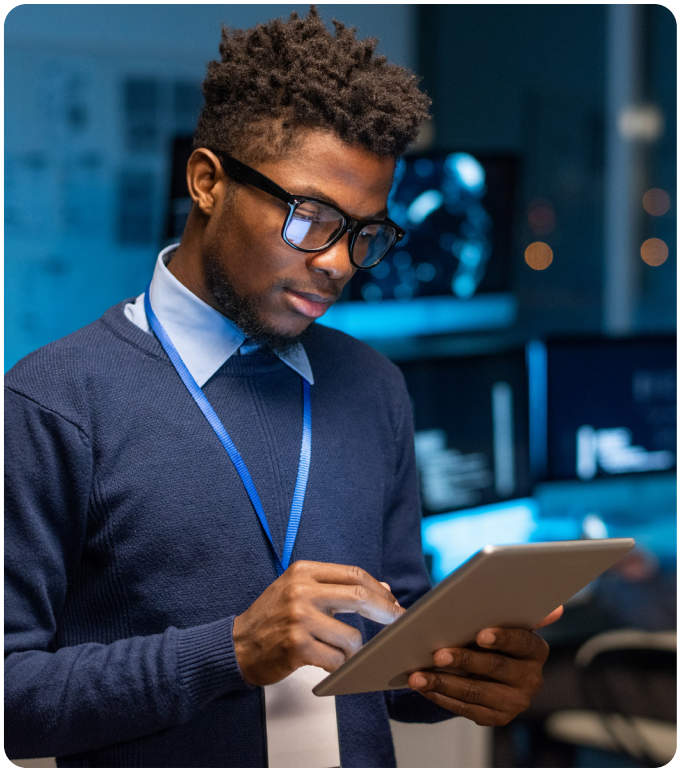
CHAPTER 6

**New for 2024: Enhancements in security and compliance** ..... 20

Native support for multi-factor authentication (MFA)
Two-factor device verification
Secure one-time code verification
Improved password requirements
One-click 'Force Logout' function
Updated data governance and privacy policies
Strengthened data protection policies

**Conclusion** ..... 22

# Introduction



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

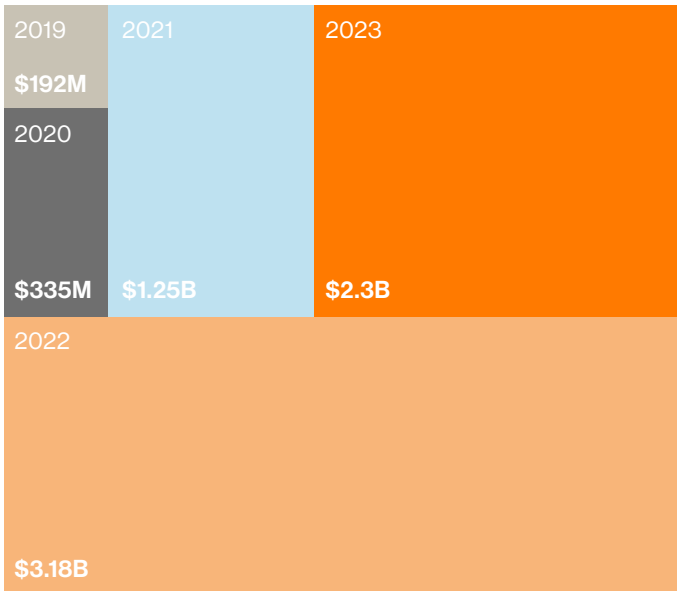
These threats are growing at a record pace, so ensuring your UCaaS platform provides a leading approach to mitigating these risks should play a primary role in your buying considerations.

General Data Protection Regulation (GDPR) and its growing fines highlight how essential it is to scrutinize your vendor's data privacy processes and capabilities. In 2022, the total amount of fines levied across the European Union (EU) under GDPR was $3.18 billion, more than double the amount issued in 2021. Additionally, in 2023, the EU imposed approximately $2.3 billion in fines for GDPR violations, surpassing the total for 2019, 2020, and 2021 combined.

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, CCPA, and CDPA.

# The high stakes of data security

### Annual cost of GDPR fines




**Sources:** https://www.dlapiper.com/en-au/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023

https://www.statista.com/chart/30053/gdpr-data-protection-fines-timeline/

As many organizations deliver on their strategy for business productivity and digital transformation, it's crucial for organizations to scrutinize how their cloud communication vendor-of-choice handles security, data privacy, and compliance to mitigate the risk of serious financial and brand threats.

These threats are growing rapidly, so ensuring your cloud communication platform provides a leading approach to mitigating these risks should play a primary role in your buying considerations.

For example, General Data Protection Regulation (GDPR) and its growing fines highlight how essential it is to scrutinize your vendor's data privacy processes and capabilities. In 2022, the total amount of fines levied across the European Union (EU) under GDPR was $3.18 billion[1], more than double the amount issued in 2021. Additionally, in 2023, the EU imposed approximately $2.3 billion in fines for GDPR violations, surpassing the total for 2019, 2020, and 2021 combined.

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

1. Publicly reported monetary fines converted from Euro to USD.

# USD 4.88M:

The global average cost of a data breach in 2024–up 10% over last year.

Percentage of enterprises suffering significant losses from mobile fraud.

**61%**

Percentage of businesses experiencing a significant or very significant business disruption due to data breach.

**70%**

# USD 5.01M:

Average costs for data breaches resulting in very significant business disruptions.

The risk landscape for cloud communication security extends to other areas as well. Think of it this way: your cloud communication 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 cloud communication vendor's security is lax, then your organization will be more vulnerable to a breach that can harm your brand value and bottom line. The cost of a single data breach significantly increased in 2024, reaching an average total of US $4.88 million per breach[2]. A staggering 61 percent of enterprises suffer significant loss from mobile fraud, with smishing and vishing being the most prevalent and costly.[3]

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

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

2. IBM Security. Cost of a Data Breach Report 2024.
3. Enea.com. Enea Study: Almost Two-Thirds of Enterprises Suffer Significant Losses Due to Mobile Fraud, February 2024.

CHAPTER 2

# Cloud communication security essentials: The 3 use cases for a platform you can trust

What supported use cases do you absolutely need in order to get cloud communication 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

## 1. Information security protection

Reliability and uptime will serve as the underpinning 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.



From the business infrastructure to the design and processes used for the cloud communication platform itself, your cloud communication 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 cloud communication 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.

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, ISO 27001 Certification, and others.

## 2. Data privacy and compliance management

With the feature-rich capabilities cloud communication 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 cloud communication 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.

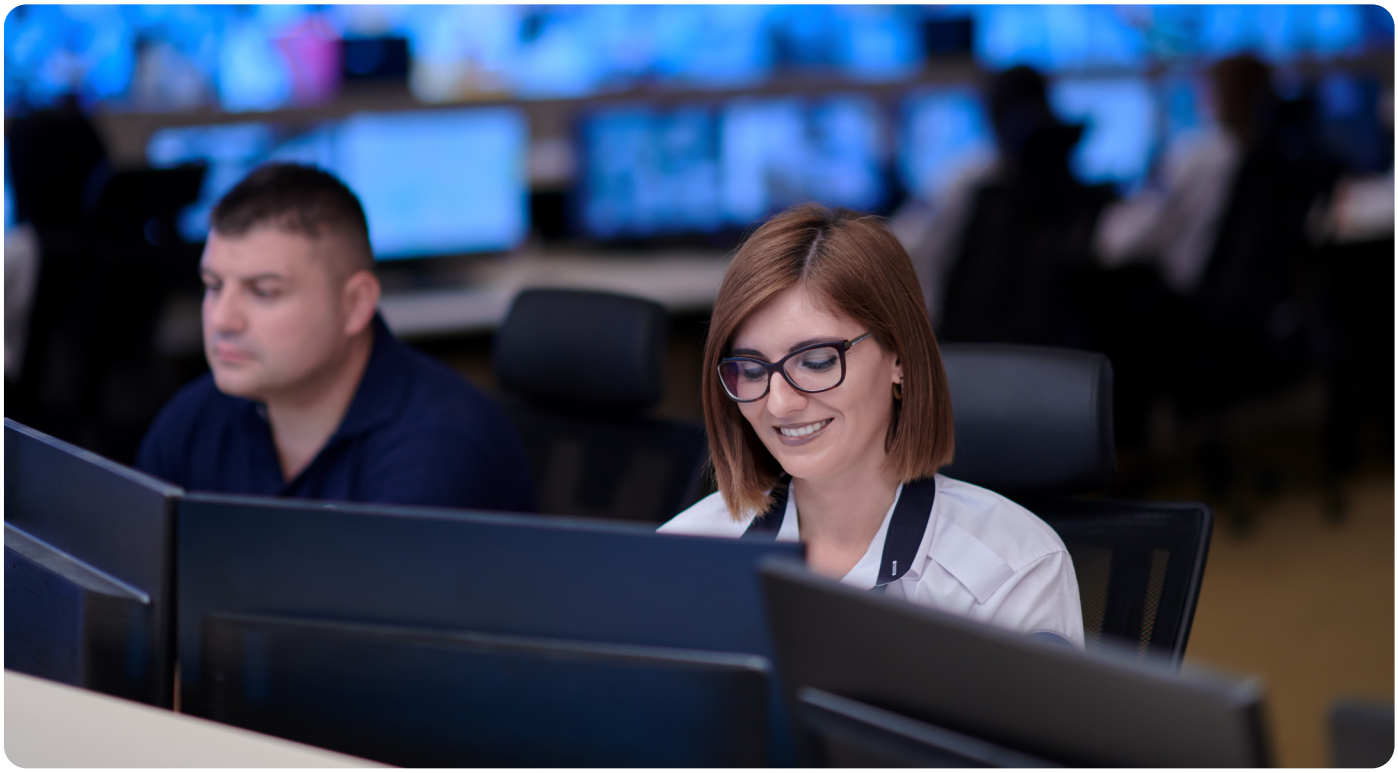
Your vendor should have the most stringent data privacy policies, which will ideally be documented in a comprehensive data privacy notice that is made publically available. In addition, review the vendor's transparency practice for regularly communicating the requests they have received about customer 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 organization free of regulatory concerns.

## 3. Security and administrative policy controls

From waiting rooms to meeting passwords, cloud communication 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 authorize attendees to join safeguard your organization 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.



CHAPTER 3

# RingCentral: a leading approach to trusted communications

RingCentral is setting the standard for trusted AI-powered communications in today's digitally driven business environment by providing secure and trusted communications for every user. We have maintained a long-standing commitment to security, building on our deep expertise in operating and securing cloud communications.

Security is ingrained in our DNA. We take a multi-dimensional approach, prioritizing the safety of your data by implementing best-in-class technologies and adhering to stringent processes. This foundation of security naturally extends to our use of artificial intelligence.

## AI governance at RingCentral

RingCentral has developed an AI governance program to support and develop trustworthy AI while fostering customer-centric innovation. The program includes a cross-functional AI Governance Council and an internal AI Policy based on the NIST AI Risk Management Framework focused on core AI principles for development and deployment of AI solutions that further responsible and ethical use of AI. Our principles for trustworthy AI are:

- **Safe:** At RingCentral we believe AI-enabled systems should not endanger human life, property, privacy, or the environment.
- **Secure:** AI-enabled systems should maintain confidentiality, integrity, and availability through protection mechanisms that prevent unauthorized access and use.

- **Transparent:** Information about AI-enabled systems and their outputs should be available to users interacting with the systems.
- **Explainable and Interpretable:** AI-enabled systems should enable the provision of information that describes how they function.
- **Privacy enhanced:** AI-enabled systems should be developed and used in compliance with privacy laws and RingCentral privacy policies.
- **Fair:** Development and use of AI-enabled systems at RingCentral should consider equality and equity by addressing issues such as harmful bias and discrimination.

## Use of artificial intelligence

RingCentral's AI platform, known as RingSense, uses its own proprietary AI models in combination with third-party AI services to provide our services. We value transparency and encourage IT leaders to refer to our subprocessor list for more information about third-party AI services and our AI whitepaper for more information regarding RingCentral's approach to trustworthy AI.

## AI model training

We have not and will not use RingCentral customer data to develop the AI model. Customers may fine-tune the output of the AI model for their account by providing direct feedback to the AI model. RingSense AI can be added to RingCentral services such as RingEX and RingCX. RingSense leverages generative AI to deliver AI-driven enhancements on recorded calls between RingSense users and external participants. RingSense can integrate with recording sources of the customer's choice, including RingEX or RingCX. For more information please see our RingSense Privacy Data Sheet.

## 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

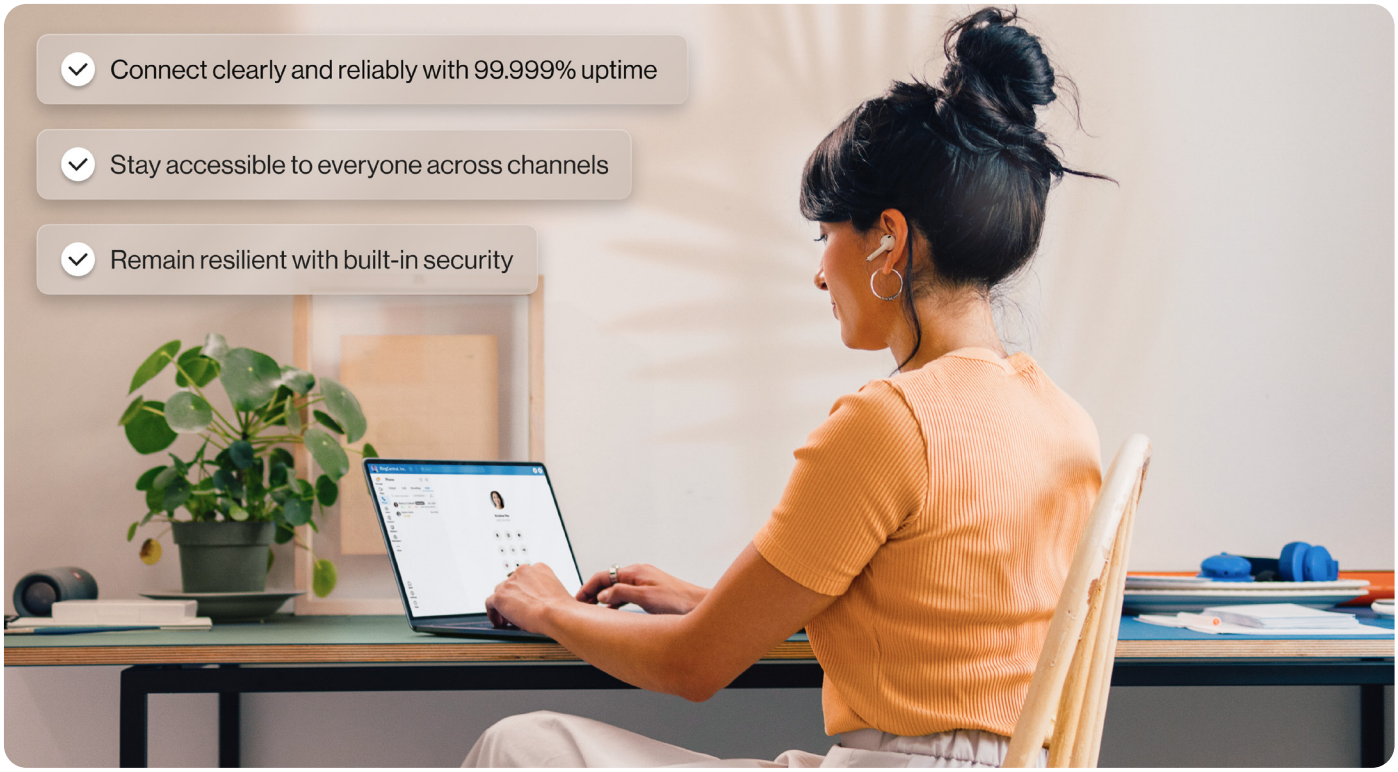
We tirelessly pursue a shared responsibility model where we maintain third-party certifications and attestations that validate our information security policies and practices along with customer controls, so you can directly manage your use case needs.

## High reliability and uptime

Experts are proactively monitoring and optimizing 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 percent uptime offered in over 45+ countries for our cloud phone system. And we've consistently met that promise for over five consecutive years.

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



CHAPTER 4

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

To give you deeper insight into our stringent practices, let's take a look at the people, processes, 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 world-class 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 center, 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 program 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 program.


## 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 dialed, and dial-pattern recognition
- Anomalous and or suspicious usage traversing our network
- Unauthorized 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 program 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 program follows industry best practices across our global organization, 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.

## 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
- FINRA

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

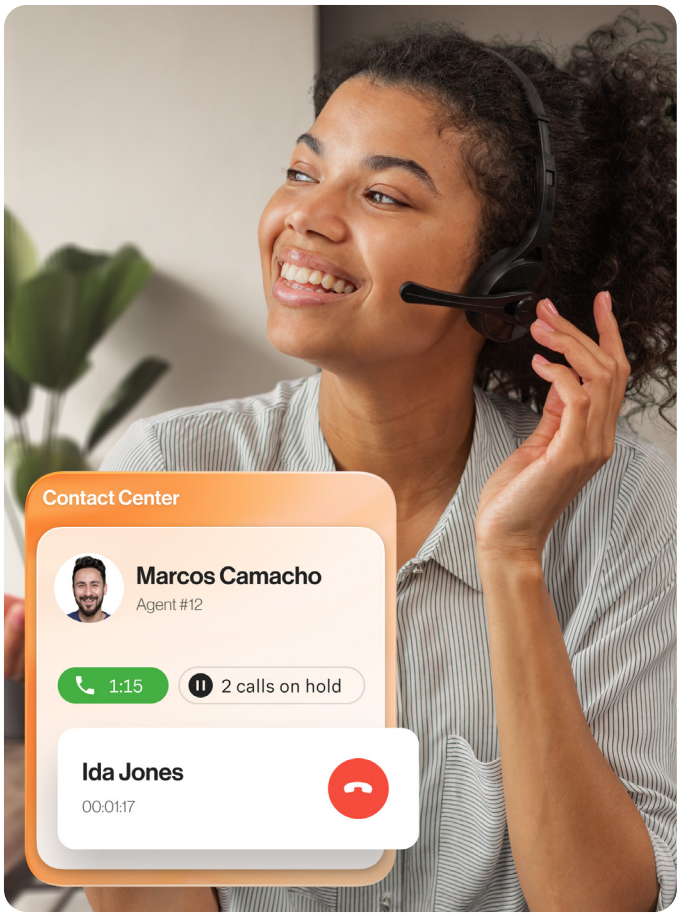
The RingCentral platform provides our customers with leading-edge security and policy controls that ensure a safe and secure experience for your users. Our platform puts a comprehensive set of administrative controls across business communications, collaboration, and customer experiences at your fingertips.These provide you with best-in-class security capabilities to safeguard your organization from data loss and bad actors. Features include, but are not limited to:

### Phone

- Single sign-on (SSO)
- Block phone numbers
- AI-based spam blocking
- Next-gen POTS replacement solution
- Enhanced Business SMS with TCR compliance
- RoboCall mitigation using STIR/SHAKEN standards
- Number masking
- RingOut—calling on third-party devices with your business phone number
- Emergency response locations for E911 calls
- Voicemail routing based on business hours
- Analytics portal
- 99.999% SLA uptime
- End-to-end encrypted calls
- TLS encryption/SRTP secure voice

### Message

- 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 compliant




## Video

- Single sign-on (SSO)
- Available via desktop & mobile app, and browser (via WebRTC)
- Require password
- Restrict screen sharing
- 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
- End-to-end encrypted meetings
- TLS encryption/SRTP secure voice

## Contact center

- Secure access for leads database
- Secure call transfers, voicemail option
- Encrypted inbound/outbound/blended calls
- Secure call termination
- Encrypted real-time analytics
- Secure call requeuing

## Access and identity

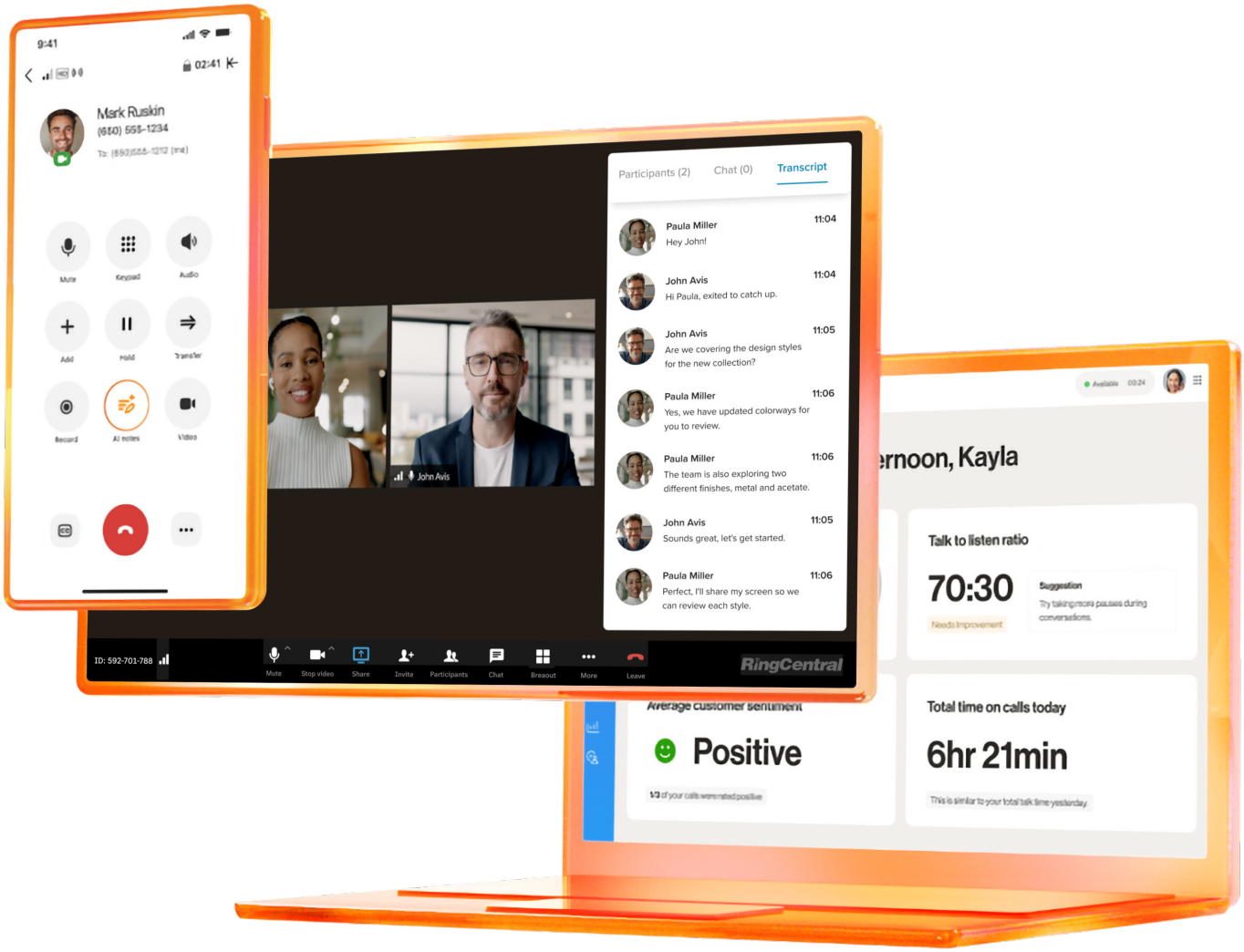
- Single sign-on (SSO)
- Enforced multi-factor authentication (MFA)
- Device PIN enforcement
- User management

## Encryption

- 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
- Authorized apps manager
- VoIP country blocking
- Centralized IT management of free and paid users
- Audit trail to track changes
- Mobile Application Management vis MS Intune



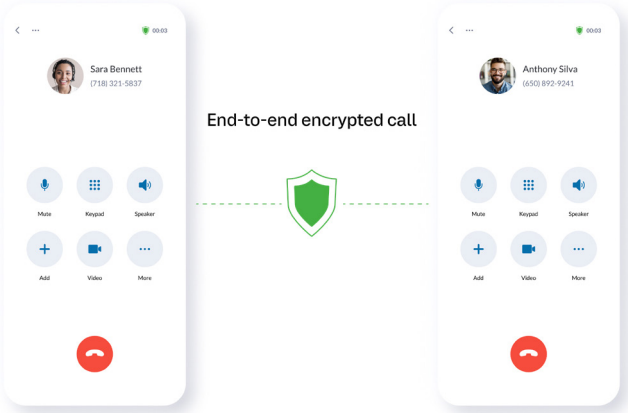
# Innovation spotlight: End-to-end encryption for calls and meetings

## Best-in-class end-to-end encryption

Goes beyond 1:1 calls and supports up to 50 participants

Multi-modal and available on any device (desktop and mobile)

Available whether the conversation is ongoing, scheduled, or spontaneous




This scheduled, spontaneous, or ongoing layer of privacy gives your users the same level of privacy that they'd experience in a face-to-face conversation held in a conference room.

Before RingCentral's end-to-end encryption (E2EE), those who wanted private, end-to-end encrypted calls, and video meetings were stuck using multiple products that lacked sufficient compliance oversight. This often forced them to evade corporate policies and use non-sanctioned apps.

With RingCentral's E2EE for calls, chats, and meetings,no third party, (not even RingCentral) can access a company's communication data. E2EE provides intuitive controls to turn everyday conversations into end-to-end encrypted conversations at the individual and team level.

RingCentral's end-to-end encryption (E2EE) provides unparalleled security and privacy for privileged conversations, as well as protection against third-party intrusion and a host of attacks. E2EE removes the need for multiple encryption products, modernizes the user experience, and reduces privacy concerns within privileged conversations.

We are the only UCaaS provider with enterprise-ready End-to-End Encryption for all forms of business communications-whether it's a scheduled, spontaneous, or ongoing 1:1 conversation, or a meeting with up to 50 participants.

# New for 2024: Enhancements in security and compliance

At RingCentral, we are committed to continually improving our security measures to protect our customers' data and ensure compliance with regional regulations. Here are the latest enhancements we've introduced to our security framework.

## Native support for multi-factor authentication (MFA)

We are excited to announce the native support for Multi-Factor Authentication (MFA) through authenticator apps. This enhancement allows users to enable MFA without depending on existing Single Sign-On (SSO) providers such as Okta. By integrating MFA natively, we offer an additional layer of security, ensuring that unauthorized access is effectively mitigated.

## Two-factor device verification

To further bolster security, we have introduced native support for two-factor device verification for logins from new devices. This feature is now enforced for all customers, ensuring that any attempt to access your RingCentral account from a new device requires additional verification. This proactive measure significantly reduces the risk of unauthorized access from unrecognized devices.

## Secure one-time code verification

Our commitment to secure customer interactions extends to our support virtual agents. We have introduced secure one-time code verification for authenticating with RingCentral support virtual agents. This new method ensures that only authorized users can access support services, providing an additional safeguard against unauthorized support requests.

## Improved password requirements

Recognizing the importance of strong passwords in preventing unauthorized access, we have enhanced our password requirements. The new policy enforces increased password composition complexity, requiring users to create passwords that include a mix of letters, numbers, and special characters. This improvement significantly strengthens the security of user accounts.

## One-click 'Force Logout' function

To empower users and administrators with greater control over active sessions, we have introduced a one-click 'Force logout' function. This feature allows users or admins to log out from all sessions instantly. Whether in response to a security concern or for routine management, this function ensures that any suspicious or unintended sessions can be promptly terminated.

## Updated data governance and privacy policies

In our ongoing effort to comply with regional regulations, we have updated our data governance and privacy policies. These updates ensure that our data processing and storage procedures align with local regulations and sovereignty requirements. By adhering to these standards, we guarantee that our customers' data is handled with the highest level of care and compliance.

## Strengthened data protection policies

Data protection remains a top priority, and we have strengthened our policies for encryption and secrets management. Our enhanced measures ensure that data is securely stored and remains within the designated regions. By implementing industry-leading encryption practices, we protect sensitive information from unauthorized access and potential breaches.

# Conclusion

Cloud communication platforms play a critical role in fostering an organization's collaboration to drive growth. Partnering with a cloud communication 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 Center.

# About RingCentral

RingCentral Inc. (NYSE: RNG) is a leading provider of AI-driven cloud business communications, contact center, video and hybrid event solutions. RingCentral empowers businesses with conversation intelligence, and unlocks rich customer and employee interactions to provide insights and improved business outcomes. With decades of expertise in reliable and secure cloud communications, RingCentral has earned the trust of millions of customers and thousands of partners worldwide. RingCentral is headquartered in Belmont, California, and has offices around the world.

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral

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



09/2024