Report on RingCentral's Engage Voice Product Relevant to Security, Availability, and Confidentiality (SOC 3 Report)

For the Period January 1, 2020 to June 30, 2020

Issued on December 18, 2020

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Service Auditors

To: RingCentral, Inc.

Scope

We have examined RingCentral's accompanying assertion, titled "RingCentral's Assertion" (assertion), that the controls within RingCentral's Engage Voice Product were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

RingCentral is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved. RingCentral has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, RingCentral is responsible for selecting, and identifying in its assertion, the applicable trust services criteria, and for having a reasonable basis for its assertion by performing an assessment of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within RingCentral's system were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

Cadence Assurance LLC

December 18, 2020
Salt Lake City, Utah

RingCentral®

Section II – RingCentral's Assertion

We, are responsible for designing, implementing, operating, and maintaining effective controls within RingCentral's Engage Voice Product throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). RingCentral's objectives for the system, in applying the applicable trust services criteria, are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2020 to June 30, 2020, to provide reasonable assurance that RingCentral's service commitments and system requirements were achieved based on the applicable trust services criteria.

RingCentral, Inc.
December 18, 2020

Attachment A – RingCentral's Description of the Boundaries of Engage Voice

Company Overview

RingCentral was founded in 1999 and is headquartered in Northern California. RingCentral is a leading provider of global enterprise cloud communications, collaboration, and contact center solutions. The RingCentral products empower employees to work better together, from any location, on any device, and via any mode to serve customers, improving business efficiency and customer satisfaction. The company provides unified voice, video meetings, team messaging, digital customer engagement, and integrated contact center solutions for enterprises globally.

System Description

The Engage Voice (EV) Product is a phone contact center solution from Connect First, acquired by RingCentral in January 2019. EV offers a cloud-based CCaaS (Contact Center as a Service) model that users can customize to fit their unique needs. EV comes packaged within an agent and supervisor interface (Agent), an admin interface (Admin), and an analytics interface (Analytics) used for tracking, monitoring, and analyzing contact center activities. Key services of EV include:

- *Agent* – An agent interface with inbound, outbound, blended voice, and live chat capabilities. A built-in softphone with Voice over Internet Protocol (VoIP), internal chat services, scripting, callback tools, agent stats, and supervisor monitoring and coaching tools.
- *Admin* – An administrator interface with configuration tools for inbound call routing, agent scripting, outbound dialing, IVR services, and live inbound and outbound customer chats.
- *Analytics* – An analytics interface with reporting tools that offer insight into contact center activities via historical reporting, scheduled reports, and customizable real-time reporting dashboards.

System Boundaries

The system boundaries within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting EV. Other products, including RingCentral Office, RingCentral Video, and Engage Digital, are not included in this report as they are covered in separate SOC 2 reports.

Subservice Organizations

EV uses Amazon Web Services (AWS) to support the cloud computing environment. This subservice organization is excluded from the scope of this report; the controls it is expected to provide are included in Attachment D, titled *Complementary Subservice Organization Controls*.

System Components

To deliver EV, RingCentral uses the following infrastructure, software, people, procedures, and data.

Infrastructure

The EV production infrastructure is primarily powered by Docker Containers. Production databases are primarily managed with PostgreSQL. Production storage devices are AWS S3 buckets. See Figure 1 for diagram of the Engage Voice architecture.

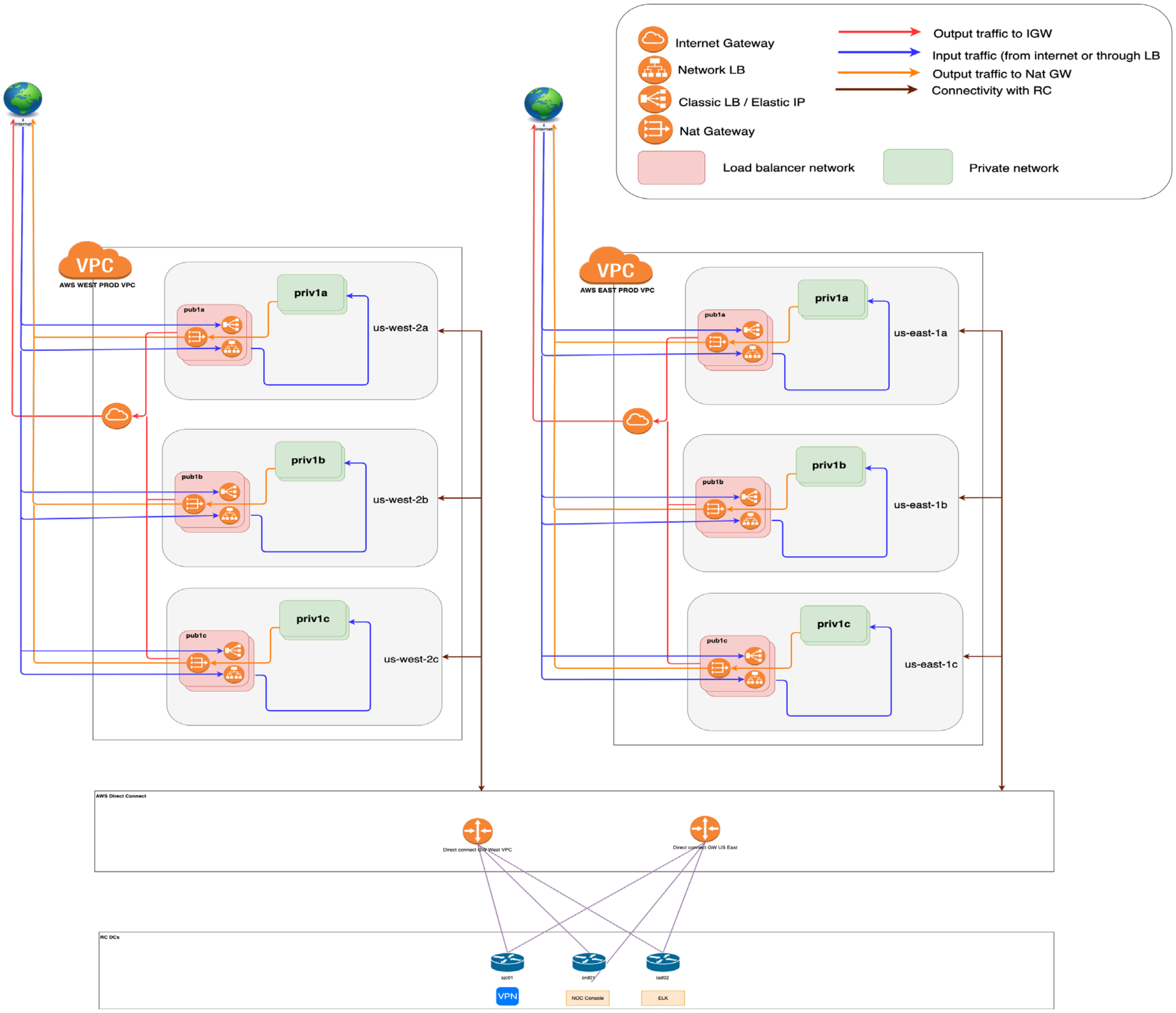

Figure 1: Overview of Engage Voice

Software

EV is supported by the following software and types of software:

- Threat Management
- Logging
- Monitoring
- Network Protection
- Intrusion Detection
- Vulnerability Testing and Vulnerability Management
- System User Authentication
- Patch Management
- Document Portal
- Change Management

People

The RingCentral Operations department is responsible for system security, confidentiality, and availability. RingCentral's Security team maintains, develops, operates, monitors, and reviews security and fraud-related controls. The team also defines and maintains the company Security Policy and supporting standards. The roles and responsibilities of the Operations team are as follows:

- Engage Digital Engineering
- Engage Digital Operations
- Network Operations (NetOps)
- Security

The roles and responsibilities of the Information Technology (IT) division include the Corporate IT Infrastructure and the IT Global Service Desk (GSD) teams. The Engineering division includes System Operations (SysOps), Development Operations (DevOps), and the Network Operations Center (NOC) teams.

Global Support Services (GSS) is responsible for assisting customers troubleshoot issues with their account and service usage related problems. GSS utilizes the Admin Web Utility to access customer accounts. Human Resources (HR) is responsible for onboarding, background checks, recruitment, training, evaluations, compensation, and development.

Nordigy and ABSoft act as subcontractors and execute controls on behalf of RingCentral under the oversight of RingCentral's management. RingCentral communicates its security, confidentiality, and availability requirements of Nordigy and ABSoft through its contracts. These subcontractors provide resources for the following services:

- *Nordigy* – Engineering, operations, product development, quality assurance (QA)
- *ABSoft* – QA

Procedures

RingCentral maintains the following key security-related policies and procedures to operate EV:

- Information Security Policy
- Active Directory-SSL VPN Access Policy
- User Accounts Management on Databases
- Access Control Policy
- Change Management Policy
- Secure SDLC Policy
- Backup Retention Policy
- Security Incident Response Guide
- Incident Management Policy
- Security Incident Response Plan
- Risk Assessment Policy
- Engage Digital Data Retention Policy and Procedure

Data

Key types of service data collected by EV include:

- Account data (customer name, email address, etc.)
- Usage data
- Call detail records (CDRs)
- Metadata (including time, recipient, sender, and location) associated with faxes, voicemails, and call recordings

Key types of content data collected by EV include:

- SMS and chat messages
- Call recordings
- End user information (address book, contact information)
- Authentication credentials

Internal Control Framework

RingCentral has adopted the following control framework to meet its security, availability, and confidentiality commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Additionally, complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at RingCentral, to achieve RingCentral's service commitments and system requirements based on the applicable trust services criteria. See Attachment C for identified complementary user entity controls.

Control Environment

An organization's control environment represents the attitude, awareness, and actions of the board of directors, executive management, and other key stakeholders concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, operations, and organizational structure.

The board of the directors meets quarterly to review company financial and operational results and discuss organizational risks such as security and identity theft. The board of directors is comprised of senior management and external advisors, who are independent from the company's operations. Annually, the security team communicates significant findings to the executive leadership team.

RingCentral's Security and Governance Council meets quarterly and reports to the board annually. This council, under the direction of the board of directors, oversees the security activities of RingCentral. The committee members are from a cross section of business lines. The council is charged with establishing overall security policies and procedures for RingCentral. The importance of security is emphasized within RingCentral through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out these policies.

Risk Assessment

RingCentral regularly reviews the risks that may threaten the achievement of the criteria for the security, availability, and confidentiality categories set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*.Changes in security threats and risks are reviewed by RingCentral, and updates to existing control activities and information security policies are performed as necessary.

Control Activities

Controls have been implemented to help address system and data risks. Controls have been designed and implemented in the following areas:

- Onboarding and Terminations
- Logical Access
- Encryption
- Network Security

- Vulnerability Management
- Configuration Management
- System Monitoring
- Incident Management
- Change Management
- Business Continuity and Recovery
- Availability
- Data Management

Information and Communication

RingCentral has an Information Security Policy to help ensure employees understand their individual roles and responsibilities. Formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes help ensure key personnel are notified in the event of problems. Additional methods of communication further help to ensure employees understand their roles and responsibilities and important information and events are communicated to management.

The Security team implements a security and fraud prevention program based on industry best practices. Customers report security incidents via the Customer Support team, which escalates incidents related to fraud and service abuse to the Fraud team. Carrier partners report incidents directly to the Fraud team via emails. The Security team utilizes tools and documented procedures for detecting and resolving security incidents. Procedures are maintained to act upon security breaches that threaten system security. The procedures are defined in the Security Incident Response Guide. In addition, RingCentral's Security team staffs dedicated personnel for handling fraud cases inbound from customers.

RingCentral has also established methods of communicating information about RingCentral, its products and services, and its policies to customers. The primary conduit of communicating to customers is RingCentral's website including RingCentral's online End-User License Agreement Terms of Service (EULA ToS), RingCentral's Privacy Notice, RingCentral's Security website, RingCentral support sites, customer communications from RingCentral's Customer Marketing department, RingCentral's blog, and the company's social media channels.

Monitoring

RingCentral has implemented the monitoring controls to periodically evaluate operating effectiveness of its internal controls. These controls include certification assessments, penetration tests, and vulnerability scans. High-risk findings from those assessments are shared with executive leadership and corresponding remediation actions are tracked to resolution.

Attachment B – Principal Service Commitments and System Requirements

RingCentral designs its policies, procedures, and processes to help ensure security, availability, and confidentiality commitments to customer data. RingCentral commitments are documented and communicated to customers in contractual agreements and the Privacy Policy located on the RingCentral website.

RingCentral has adopted the following control framework to meet its commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Attachment C – Complementary User Entity Controls

RingCentral's controls were designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities RingCentral believes should be present at each customer, and has considered in developing its controls reported herein. RingCentral customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by RingCentral EV customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- User entities are responsible for managing their user permissions and login information (CC6.3).
- User entities are responsible for designating user accounts with administrator privileges (CC6.3).

Attachment D – Complementary Subservice Organization Controls

RingCentral uses a subservice organization in conjunction with providing EV. RingCentral utilizes AWS for management and hosting of production servers and databases. Controls managed by this third-party subservice provider are not included in the scope of this report. Expected subservice provider controls that have an effect on specific criteria are included below.

Criteria	Expected Controls for AWS
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to hosted systems requires users to use a secure method to authenticate. User content is segregated and made viewable only to authorized individuals. Network security mechanisms restrict external access to the production environment.
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New user accounts are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to physical facilities is restricted to authorized users.

Criteria	Expected Controls for AWS
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms restrict external access to the production environment. Encrypted communication is required for connections to the production system.
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Access to hosted data is restricted to appropriate users. Hosted data is protected during transmission through encryption and secure protocols.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configuration changes are logged and monitored. Vulnerabilities are identified and tracked to resolution.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Security events are monitored and evaluated to determine potential impact per policy.

Criteria	Expected Controls for AWS
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Operations personnel log, monitor, and evaluate incident events identified by monitoring systems
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Operations personnel respond to, contain, and remediate incident events, and update stakeholders, as needed.
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are documented, tested, and approved prior to migration to production. Access to make system changes is restricted to appropriate personnel.
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Operations personnel monitor processing and system capacity.
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental protections, software, data back-up processes, and recovery infrastructure are implemented.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	System failover and backup procedures are tested.