Kaseya US, LLC

SOC 3

Independent Service Auditor's Report on Management's Description of a Service Organization's System Relevant to Security, Availability, and Confidentiality

June 1, 2021 to May 31, 2022

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

INDEPENDENT SERVICE AUDITOR'S REPORT

The Management of Kaseya US, LLC
701 Brickell Avenue, Suite 400
Miami, FL 33131

Scope

We have examined Kaseya US, LLC's ("Kaseya", or "the Company") description of controls for its information technology general controls system and related transactions throughout the period June 1, 2021 through May 31, 2022, based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the June 1, 2021 through May 31, 2022, to provide reasonable assurance that Kaseya's service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in DC section 200, *2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids).

Kaseya LLC's Responsibilities

Kaseya 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 Kaseya's service commitments and system requirements were achieved. In section II, Kaseya has provided its assertion titled "Assertion of Kaseya US, LLC Service Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. Kaseya is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the description of the suitability of the design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. 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 suitability of the design and operating 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, Kaseya's controls over the system were effective throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

Ascend Audit & Advisory

July 18, 2022

ASSERTION OF KASEYA US, LLC SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of Kaseya's information technology general controls system ("system" or "the system") throughout the period June 1, 2021 through May 31, 2022, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report* (AICPA, Description Criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Kaseya Service Organization's system, particular information about system controls that Kaseya has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in DC section 200, *2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA Trust Services Criteria).

We confirm, to the best of our knowledge and belief, that:

a. The description represents Kaseya's system that was designed and implemented throughout the period of June 1, 2021 through May 31, 2022, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
      - *Software* – The programs and operating software of a system (systems, applications, and utilities).
      - *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - *Procedures* – The automated and manual procedures involved in the operation of a system.
      - *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

      (3) The boundaries or aspects of the system covered by the description.

      (4) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities and other parties.

      (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that Kaseya's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. The controls stated in the description operated effectively throughout the period June 1, 2021 through May 31, 2022, to provide reasonable assurance that Kaseya's service commitments and system requirements were achieved based on the applicable trust services criteria.

By: /S/ Jason Manar

Jason Manar
Chief Information Security Officer

July 18, 2022

DESCRIPTION OF THE KASEYA US, LLC INFORMATION TECHNOLOGY GENERAL CONTROLS SYSTEM

Company Overview

Kaseya is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations to efficiently manage, secure, automate, and backup IT. Kaseya products offer the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya and the Company's lines of business (i.e., business units) which include Unitrends, Spanning Cloud Apps, RapidFire Tools, IT Glue, ID Agent, Graphus, Trumethods and RocketCyber. The platform empowers businesses to command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions.

Products Overview

Kaseya Business Unit Descriptions, Products, and Services:

Kaseya founded in 2000 is the classic parent company that offers Remote Monitoring Management, Professional Services Automation (PSA), Network Monitoring, IT Service Desk, and Identity & Access Management solutions. Key product solutions include:

- Kaseya Virtual System Administrator (VSA) – Remote monitoring and management
- Business Management Solutions (BMS) – Professional services automation / Vorex – IT operations and support
- Traverse – Network and systems monitoring

Unitrends & Spanning Cloud Apps joined the Kaseya family in 2018 and offer backup solutions for MSPs and internal IT organizations for different technology solutions. Key product solutions include:

- Unitrends –Recovery Series Appliances
- Unitrends Cloud & Disaster Recovery – Cloud Backup, DraaS, Forever Cloud
- Unitrends Backup Software – Virtual Appliance (UB), VM Backup Essential (vBE), Boomerang
- Unitrends – MSP
- Spanning – Backup for Microsoft Office 365
- Spanning – Backup for Google G Suite
- Spanning – Backup for Salesforce

RapidFire Tools is the IT network and security assessments reporting tool for compliance with internal threat detection. RapidFire Tools joined the Kaseya family in 2018. Key product solutions include:

- Network Detective
- Compliance Manager
- Cyber Hawk

ID Agent is a dark web monitoring and identity theft protection application. ID Agent joined the Kaseya family in 2019. Key product solutions include:

- Dark Web ID
- Bullphish ID
- AuthAnvil (Passly)

Graphus is an automated phishing defense platform that protects from cybercriminals posing as trusted contacts. Graphus joined the Kaseya family in 2020. Key product solutions include:

- Graphus – Microsoft O365
- Graphus – Google G Suite

Kaseya Powered Services are a set of services that provide MSPs the ability to build profitability, security, compliance, and backup practices. Key services include:

- Comprehensive Sales & Marketing Programs and Strategies
- Marketing & Content Resources
- On-Demand Training & Tools
- Strategic Playbooks
- Goal Assist

ITG Software, ULC is a cloud-based service provider that offers a structured way to document IT systems. This business unit's software is designed for both IT service providers and corporate IT departments. ITG Software joined the Kaseya family in 2018.

RocketCyber, LLC is a cloud-based Managed Security Operations Center (SOC) platform that delivers continuous cybersecurity monitoring across endpoints, cloud applications, and network devices to empower Managed Service Providers (MSPs) to deliver security services to small and medium businesses. RocketCyber joined the Kaseya family in February 2021.

System Description

Principal Services Provided

Kaseya is an enterprise technology solution catering to managed service providers (MSPs), small to midsize business (SMB), and internal IT organizations. Kaseya provides a purpose-built platform of software solutions for managing, operating, and maintaining Information Technology for businesses.

Principal Services Commitments and System Requirements

Kaseya designs its processes and procedures to meet the objectives of the company's technology services. Those objectives are based on security, availability, and confidentiality of service commitments that Kaseya makes internally, to other (user) entities, and for compliance with relevant laws and regulations. Corporate policies define Kaseya's organization-wide approach to how systems and data are protected, how information and systems are maintained and made available for operation, and how the company objectives are being met.

Kaseya's principal service commitments as they relate to the system description and the applicable trust service categories of security, availability, and confidentiality are standardized and include, but are not limited to, the following:

- Kaseya follows structured hiring and employee management processes to ensure designated control and procedures are followed
- Vendors used to support Kaseya applications or have access to client data are evaluated to ensure they meet security requirements of Kaseya when performing duties on behalf of Kaseya
- Kaseya security requirements and compliance to relevant laws and regulations are identified and monitored
- Controlled access to the production infrastructure and client data
- Segregation of client data
- Monitoring of system performance and critical application services

Components of the System

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Policies and Procedures (automated and manual)
- Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five (5) components comprising the System.

Infrastructure

The Kaseya Information Technology (IT) environment includes global data centers located in Massachusetts, Virginia, New Jersey, Colorado, Georgia, and Florida of the United States. It also has data centers in Ireland, United Kingdom, Germany, Australia, and Canada. Housed within these data centers are the supporting operating system platforms (Windows and Linux), networking components (firewalls, routers, switches), and data storage devices. Kaseya also utilizes cloud technologies from Amazon Web Services (AWS) and Microsoft Azure across global regions.

Corporate infrastructure is segregated and managed by the Kaseya Global IT Team. Development, Staging, and Production infrastructure is segregated and managed by the Infrastructure Operations Team.

Software

Software utilized by IT and Operations to manage and support the Kaseya IT environment includes:

- Virtualization Hypervisor
- Backup Management
- Remote Management and System Monitoring
- Network Monitoring
- Security Monitoring
- Change Management
- Help Desk Support

People

IT and Operations personnel provide the following core support services for the Kaseya IT environment components listed above:

- Systems and Network Monitoring
- Security
- Database Administration
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

In order to provide these services, IT and Operations operate in functional areas: Network Management Services, Systems Management Services, Development, and Support. Below is a brief description of each of these functional areas:

- Network Management Services: This functional area deals with Fault, Configuration, Accounting, Performance, and Security (FCAPS) - It keeps the network up and running smoothly and monitors the network to spot problems as soon as possible, ideally before users are affected, keeping track of resources on the network, and how they are assigned.

- Systems Management Services: This functional area deals with server systems operations and maintenance to support global operations.

- Development: This functional area supports new product developments, client customizations, new releases, and updates for client software.

- Support: This functional area deals with maintenance, repairs, and upgrades attending to user support.

Policies and Procedures

Kaseya has documented policies and procedures to support the operations and controls over its IT Environment. Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- System security administration
- Server security configuration
- Computer operations
- Network operations
- Disaster recovery policy and planning
- Change management
- Incident response policy and incident management
- Physical security
- Backup and secured storage
- Environmental protection policy
- Acceptable use policy
- Information security policy

Data

Kaseya treats customer data as protected information (PI). Protected information is highly guarded and secured to preserve confidentiality, integrity, and availability of the data. Security controls include role-based access control, multi-factor authentication (MFA), encryption, backup, and monitoring.

Global IT and Operations Teams are also responsible for the overall availability of data including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving issues.

Disclosures

Security Incident

Kaseya experienced a sophisticated cyberattack attack on July 2, 2021 (mid-day) which impacted fifty-seven (57) On-Premises customers. The Incident Response Team learned of the potential attack (mid-day) and immediately followed the established incident response process and engaged third party security investigators to determine the root cause of the attack.

Upon detection, Kaseya immediately shut down VSA SaaS servers as a precautionary measure. The Company also contacted VSA On-Premises customers, advised them of the attack, and instructed them to shut down VSA servers. The Company notified law enforcement and government cybersecurity agencies and maintained continual contact and updates throughout the incident response process. As a result of action taken, the security incident was contained to a small percentage of the Kaseya's customers and only VSA On-Premises customers.

During the next several days, the root cause and source of the vulnerability was determined. An emergency release patch was developed for the VSA platform with updates and estimated times to resolution communicated to customers and other stakeholders every four (4) to five (5) hours, daily. These updates included actions to be taken by customers for incident containment, along with documentation and instructions to prepare for the upcoming VSA SaaS release and VSA On-Premises patch.

On July 11, 2021 restoration of VSA SaaS including the new release began and the patch for VSA On-Premises became available. By July 12, 2021, 100% of SaaS customers were back online while the Company assisted VSA On-Premises customers with completion of patch installations.