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, 2023 to May 31, 2024

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, 2023 through May 31, 2024, 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 (With Revised Implementation Guidance – 2022)(AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2023 through May 31, 2024, to provide reasonable assurance that Kaseya's service commitments and system requirements were achieved based on the trust service criteria for security, availability, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022), in AICPA Trust Services Criteria.

Subservice Organizations

Kaseya and its business units (ie., products) utilize the following subservice organizations to provide services and application delivery:

- Bamboo HR for Human Resources Information System (HRIS)
- Atlassian for source code repository, version control and project management
- Salesforce for customer relationship management and support ticketing
- MacQuarie Cloud Services PTY Ltd, Faction, Inc., Access Alto (Equinix, Inc.), Zayo, Inc., Tierpoint, Aligned Energy, Cologix, Cyxtera, and Norris Networks for data center services
- Amazon Web Services (AWS) and Microsoft Azure for Infrastructure-as-a-service and cloud computing
- Laceworks, Inc for cloud security management services
- JumpCloud, Inc for Identify Management services

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 AICPA. 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, 2023 through May 31, 2024, 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

St. Petersburg, FL

June 18, 2024

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, 2023 through May 31, 2024, ("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 (With Revised Implementation Guidance – 2022)*(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, particularly 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 TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*(AICPA *Trust Services Criteria*).

Kaseya and its business units utilize subservice organizations for the following services and applications:

- Bamboo HR for Human Resources Information System (HRIS)
- Atlassian for source code repository, version control and project management
- Salesforce for customer relationship management and support ticketing
- MacQuarie Cloud Services PTY Ltd, Faction, Inc., Access Alto (Equinix, Inc.), Zayo, Inc., Tierpoint, Aligned Energy, Cologix, Cyxtera, and Norris Networks for data center services
- Amazon Web Services (AWS) and Microsoft Azure for Infrastructure-as-a-service and cloud computing
- Laceworks, Inc for cloud security management services
- JumpCloud, Inc for Identify Management services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kaseya, to achieve Kaseya's service commitments and system requirements based on the applicable trust services criterion of security, availability, and confidentiality. The description presents Kaseya's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Kaseya's controls. The description does not disclose the actual controls at the subservice organization. The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Kaseya, to achieve Kaseya's service commitments and system requirements based on the applicable trust services criteria. The description presents Kaseya's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Kaseya's controls.

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

a. The description presents Kaseya's system that was designed and implemented throughout the period of June 1, 2023 to May 31, 2024, 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, 2023 to May 31, 2024, 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, and if the subservice organization and user entities applied the complementary controls assumed in the design of Kaseya's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Kaseya's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Kaseya's controls operated effectively throughout that period.

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

Company Overview

Kaseya is a leading provider of security and cloud-based software solutions purposed built for Managed Service Providers (MSPs) and Mid-Market Enterprises (MMEs). Through its customer-centric approach and renowned support, Kaseya delivers best-in-breed technologies that empower organizations to seamlessly manage IT infrastructure, secure networks, backup critical data, manage service operations, and grow their businesses. Kaseya offers a broad array of IT management/security solutions, including well-known names: Kaseya, Datto EDR (Infocyte), IT Glue, RapidFire Tools, Unitrends, Spanning Cloud Apps, TruMethods, ID Agent, Graphus, RocketCyber, audIT, and Vonahi. These innovative solutions fuel Kaseya's IT Complete platform, which is designed to maximize efficiencies and enable businesses through a single pane of glass. IT Complete empowers IT professionals to centrally command hardware, software, security, data, compliance, operations and more from within a comprehensive, integrated, intelligent (AI utilization-optimized), and affordable platform. Headquartered in Miami, Florida, Kaseya is privately held with a global presence in over twenty-five (25) countries.

Products and Services Overview

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 and access management solutions.

Classic Kaseya products and services (i.e., business units) are:

Virtual System Administrator (VSA & VSA X) – provides remote monitoring management (RMM) and endpoint management services for IT administrators. Key features include:

- Discover and monitor IT assets
- View endpoint connectivity in the network topology map
- Automate software patch management
- Leverage remote endpoint management to quickly resolve issues

Business Management Solutions (BMS)/Vorex – is a next-generation professional services automation solution for MSPs and internal IT teams to manage service desk, billing, CRM and more. Key features include:

- Service Desk
- CRM
- Automated Billing
- Inventory Management
- Quoting
- Project Management
- HR
- Mobile Application
- Native Integrations

Traverse – provides network performance monitoring for MSPs and IT professionals for on-premise, cloud, and hybrid platforms. Key features include:

- Topology Discovery
- Service Containers
- Netflow Analysis
- Network Configuration
- Event Manager
- Predictive Analytics
- SLA Manager

Products and services (i.e., business units) added to the Kaseya family of solutions are:

Unitrends & Spanning – joined the Kaseya family in 2018 and offers 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 an 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
- VulScan

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 for Microsoft O365
- Graphus for Google G Suite
- Goal Assist

IT Glue – is a cloud-based service that offers a structured way to document IT systems. This software is designed for both IT service providers and corporate IT departments. ITG Software joined the Kaseya family in 2018. Key product features include:

- Relationship Mapping
- Secure Password Management
- 30+ Native Integrations
- Enterprise-Grade Security
- Automated Account Backup
- IP Access Control
- Cross-Account Migration Service
- 1-Click Password Rotation

RocketCyber – is a cloud-based managed security operations center (SOC) platform that delivers continuous cybersecurity monitoring across endpoints, cloud applications, and network devices to empower MSPs to deliver security services to small and medium businesses. RocketCyber joined the Kaseya family in February 2021. Key product features include:

- SIEMless Log Monitoring
- Threat Intelligence & Hunting
- Breach Detection
- Intrusion Monitoring
- NextGen Malware
- PSA Ticketing

TruMethods – provides a powerful, high-value virtual CIO (vCIO) software platform to allow MSPs to build more strategic relationships with customers. TruMethods joined the Kaseya family in May 2021. Key product solutions include:

- Building comprehensive IT standards
- Accessing a library of industry compliance guidelines
- Completing impact assessments
- Delivering a strategic roadmap to clients

Passly – is an identity and access (IAM) solution that integrates with VSA for a suite of three services:

- Two Factor Authentication
- Password Saver
- Single Sign on

Connect Booster – is an automated billing platform which automates billing and collections tasks and collects customer payments eliminating manual billing process. Key product features include:

- Automated Variable Billing
- Automated Dunning Notices
- Automated Statements
- Automatic Card Updater

Datto EDR (Infocyte) – is a cloud based endpoint detection and response (EDR) security solution that continuously monitors devices (e.g., laptops, workstations, tablets, etc.) to detect and respond to cyber threats. The solution is designed for MSPs or IT professionals. Infocyte HUNT uses forensic state analysis to discover the post-compromise activity of cyber attackers and malware that have bypassed other defenses and reduces attackers' time to help organizations defend networks and critical information. Key product features include:

- Click-to-respond
- Detect fileless attacks with behavioral analysis
- Alerts mapped to MITRE ATT&CK framework
- Smart recommendations
- Scalable remote response actions
- Integrated with remote monitoring and management
- Supports Windows, MacOS and Linux operating systems

audIT – is SaaS software solution that allows enterprises to take the information collected with fact finding meetings, data tools, or business reviews and create beautiful and intuitive sales-ready presentations. audIT presentations can be composed of up to four categories. Each category is broken down into nine (9) or less configurable items resulting in a 36-point technical analysis to allow an MSP to historically retain these and generate comparative reports demonstrating the value that can be effectively provided. The four (4) audit presentation categories are:

- Infrastructure
- Security
- Managed Support and Services
- Telecommunications

Vonahi – is a comprehensive network automation platform that empowers IT teams to streamline network management tasks and optimize network performance. With Vonahi, users can automate routine network operations, monitor network health in real-time, and troubleshoot issues efficiently. Key product features include:

- Network Device Provisioning
- Automated Configuration Management
- Network Monitoring and Alerting
- Troubleshooting Tools
- Automation Workflow Orchestration
- Integration Capabilities
- Scalability and Flexibility
- Compliance Management
- Role-Based Access Controls
- API and Integration Support

System Description

Principal Services Provided

Kaseya is an enterprise technology solution catering to managed service providers (MSP's), 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 security, availability, and confidentiality commitments to customers are documented and communicated to customers in the Kaseya Master Services Agreement and the description of service documents published on the customer facing Website. The principal security, availability, and confidentiality commitments include, but are not limited to:

- Maintaining appropriate administrative, physical, and technical safeguards to protect the security and availability of the Kaseya Products platform and the customer data in accordance with Kaseya's security requirements.
- Performing annual third party security and compliance audits of the environment, including, but not limited to, reporting on Service Organization Controls (SOC) relevant to security, availability, and confidentiality.
- Using formal HR (Human Resources) processes, including background checks, code of conduct and company policy acknowledgements, security awareness training, disciplinary processes, and annual performance reviews.
- Accessing management procedures for the request, approval, provisioning, review, and revocation of Kaseya personnel with access to production systems.
- Preventing malware from being introduced to production systems.
- Monitoring the production environment for vulnerabilities and malicious traffic.
- Using industry standard secure encryption methods to protect customer data at rest and in transit.
- Transmitting unique login credentials and customer data via encrypted connections.
- Maintaining a disaster recovery and business continuity plan to ensure availability of information following an interruption or failure of critical business processes.
- Maintaining and adhering to a formal incident management process, including security incident escalation procedures.
- Maintaining confidentiality of customer data and notifying customers in the event of a data breach.
- Identifying, classifying, and properly disposing of confidential data when retention periods are reached and/or upon notification of customer account cancellations.

Kaseya regularly reviews the security, availability, and confidentiality performance metrics to ensure these commitments are met.

Components of the System

Kaseya's control environment (the "System") is comprised of the following components:

- Infrastructure (work from home locations, workstations, and cloud hosting)
- Software (cloud-based solutions and applications)

- People (employees, consultants, and users)
- Policies and Procedures (manual and automated)
- Data (transaction streams, files, databases and tables)

The Company's environment and platform are designed and managed with security, availability, and confidentiality in mind. The following sections provide a brief description of the five 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 in the United States; and 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 (Managed by Product Teams), 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

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.

Corporate Policies and Procedures

Kaseya has formalized policies and procedures which are as follows:

- Asset Management Procedures
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Confidentiality Agreement
- Electronic Data Destruction Policy
- Employee Handbook
- Enterprise Encryption Guidelines in Information Security Policy
- Hiring and Termination Checklist
- Incident Response Plan
- Information Security Policy
- Offboarding Process
- Onboarding Process
- Patch Management Procedures
- Vendor Risk Management Policy
- Vulnerability Disclosure Policy
- Backup & Restore Policy and Procedure
- Kaseya Disaster Recovery Plan
- Data Classification Matrix & Handling Guide
- Laptop Security Policy
- Acceptable Use Policy
- Environmental Protection Policy
- Password Policy
- Physical Access Security Policy
- Records Retention Policy
- Software Development Life Cycle Policy
- Vendor Management Program
- Corporate IT MFA (Multi Factor Authentication) Admin Policy
- Work-From-Home Resource Center

Data

Data management common to multiple products includes:

- Kaseya stores several types of customer and company data in the cloud solution platform. Sensitive data is protected through secure encryption methodologies.

- Kaseya retains confidential information to meet legal and regulatory requirements and confidentiality commitments. Requirements for data retention are specified contractually via the customer-specific Kaseya Terms and Privacy Policy.

- Sensitive data is secured any time it must be transmitted or received via open, public networks. Connectivity to the Kaseya Cloud utilizes OpenSSH with AES-256-bit encryption to protect backed-up data in transit.

- Encryption practices protect information involved in the Kaseya Continuity for Microsoft Azure solution from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, and replay.

Disclosures

A payroll employee sent a payroll document with payroll information to his personal email while he was leaving the Company. This was identified during the offboarding process by the Company's internal security team. The former employee entered into a consent injunction filed in federal court in the United States and the former employee deleted the payroll document from their possession and systems. The former employee signed a certification, pursuant to a court order, stating that they did not transfer the payroll document to any other person or entity. There was no compromise to the Company's systems by a third party.

An Accounts Payable employee sent business confidential information including A/P information to their personal email. The ability to send information to his personal email was turned off and their laptop and phone were wiped. The former employee entered into a consent injunction filed in federal court in the United States and signed a certification, pursuant to a court order, stating that they did not transfer A/P information to any other person or entity. There was no compromise to the Company's systems by a third party.

Information in tickets that customers created in Company's Autotask system were indexed and may have been available in search results on the Internet. This was discovered after a normal operational review by the Company's internal security team. The link keys to the indexed data were changed and search providers removed the indexed information from their search engines. Monitoring for robot.txt files is now in place. There was no compromise to the Company's systems by a third party.