Report on SnapComms, Inc. an Everbridge Company's SnapComms Platform Relevant to Security, Availability, and Confidentiality Throughout the Period December 1, 2020 to March 31, 2022

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: SnapComms, Inc. an Everbridge Company ("SnapComms")

Scope

We have examined SnapComms' accompanying assertion titled "Assertion of SnapComms, Inc. an Everbridge Company Management" (assertion) that the controls within the SnapComms Platform (system) were effective throughout the period December 1, 2020 to March 31, 2022, to provide reasonable assurance that SnapComms' 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*).

The description of the boundaries of the system indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at SnapComms, to achieve SnapComms' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of SnapComms' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

SnapComms uses a subservice organization to provide Platform-as-a-Service (PaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SnapComms, to achieve SnapComms' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of SnapComms' controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

SnapComms 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 SnapComms' service commitments and system requirements were achieved. SnapComms has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SnapComms is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness 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 SnapComms' 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 SnapComms' 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 were 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 the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the SnapComms Platform were effective throughout the period December 1, 2020 to March 31, 2022, to provide reasonable assurance that SnapComms' 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 SnapComms' controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
June 9, 2022

Section 2

Assertion of SnapComms, Inc. an Everbridge Company Management

SnapComms
AN EVERBRIDGE COMPANY

Assertion of SnapComms, Inc. an Everbridge Company ("SnapComms") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the SnapComms Platform (system) throughout the period December 1, 2020 to March 31, 2022, to provide reasonable assurance that SnapComms' 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.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at SnapComms, to achieve SnapComms' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of SnapComms' controls.

SnapComms uses a subservice organization for Platform-as-a-Service services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SnapComms, to achieve SnapComms' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of SnapComms' controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2020 to March 31, 2022, to provide reasonable assurance that SnapComms' 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*) if complementary subservice organization controls and complementary user entity controls assumed in the design of SnapComms' controls operated effectively throughout that period. SnapComms' 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 December 1, 2020 to March 31, 2022, to provide reasonable assurance that SnapComms' service commitments and system requirements were achieved based on the applicable trust services criteria.

SnapComms, Inc. an Everbridge Company

Elliot Mark
Vice President

Attachment A

SnapComms, Inc. an Everbridge Company's Description of the Boundaries of Its SnapComms Platform

Type of Services Provided

SnapComms, Inc. an Everbridge Company's ("the Company") SnapComms Platform ("SnapComms") is a multi-channel, multidevice internal communications platform. Messages are created using the secure, cloud-based SnapComms Content Manager and sent to employees who have the SnapComms App installed on their computer, tablet, or smartphone. These messages can be in the form of Desktop Alerts, Tickers, Surveys and Quizzes, Screensavers, Wallpapers and Lock Screens, or Newsletters.

In August 2020, SnapComms was acquired by Everbridge Inc., a global software company that provides enterprise software applications across the critical events space. This acquisition has not only strengthened SnapComms and Everbridge's position in the mass notification arena but also provided a platform for a stronger and more robust security, privacy and compliance posture for our combined customers.

Since the acquisition SnapComms has been in the process of integrating all security policies and procedures to align with Everbridge and provide a consolidated Information Security Management System. The transition to bring these two companies together from a compliance standpoint will result in providing our customers with assurance that they are protected.

The boundaries of the system in this section of the report details SnapComms. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of SnapComms are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of SnapComms.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Microsoft Azure ("Azure") to provide the resources to host SnapComms' infrastructure. The Company leverages the experience and resources of Azure to support the scalability, availability, and durability of the SnapComms platform. Depending on the geographic location and specific security requirements, customer data is stored and processed in the following regions: North America (Canada and USA), Europe (UK and EU), and Australia.

The in-scope hosted infrastructure consists of Azure's services, as shown in the table below:

Infrastructure	
Production Service	**Business Function**
Azure SQL Database	Data storage
Azure Virtual Network	Networking and distributed denial-of-service (DDoS) protection

Infrastructure	
Production Service	**Business Function**
Azure App Service	Application hosting
Azure Functions	Task execution
Azure Service Bus	Queueing services
Azure Key Vault	Management of cryptographic keys

Software

Software consists of the programs and software that support SnapComms. The list of software and ancillary software used to build, support, secure, maintain, and monitor SnapComms include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
StackPath Content Delivery Network	Content delivery services
Azure DevOps	Code repository and continuous integration/continuous delivery (CI/CD) services
Jira	Bug and feature tracking
Salesforce	Help desk, ticketing system
Site24x7	Monitoring and alerting
DNS Made Easy	Domain Name System (DNS) services
Elastic	Application logging

People

The Company develops, manages, and secures SnapComms via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
SnapComms Engineering	Responsible for the development, testing, deployment, and maintenance of new code for SnapComms.
SnapComms SRE	Responsible for managing access controls, monitoring the infrastructure, and maintaining the security of the production environment.
SnapComms Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.

People	
Group/Role Name	**Function**
Compliance and Information Security Team	Responsible for ensuring the integrity, availability, and confidentiality of customer data is protected at every stage of the product life cycle and across all Company processes.
People and Culture Department	Defines policies and procedures for recruitment and termination of employment including initiating the instruction to remove access.

Procedures

Procedures are in place and include the automated and manual procedures involved in the operation and maintenance of SnapComms. These include those relating to product management, engineering, technical operations, security, and information technology (IT). These procedures are drafted in alignment with the overall information security policies and include Business Continuity, Security Vulnerability Management, IT Suppliers, Physical Security, Operations Security, Asset Management, Cryptography, Access Control, and IT Acceptable Use. All policies are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of SnapComms:

Procedures	
Procedure	**Description**
Access Control	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
Operating Procedures for ICT	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Secure Development	How the Company defines rules to ensure that information security is taken into account throughout the entire development life cycle, resulting in secure software and systems.
Cryptographic Controls	How the Company ensures the proper and effective use of cryptographic controls in order to protect the confidentiality, authenticity, and integrity of information.
Business Continuity	How the Company establishes the steps necessary to implement business continuity management for the SnapComms product.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the SnapComms production network. Once stored in the environment, the data is accessed remotely from customer systems via the internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

The following table details the types of data contained in the production application for SnapComms:

Data		
Production Application	**Description**	**Data Store**
SnapComms	Customer-created content is stored ready for assembly.	Azure SQL databases
SnapComms	Published customer content encrypted ready for delivery to SnapComms' applications.	Azure Storage
SnapComms	Consumer applications generate events that are sent back to the system for processing (e.g., click-through events, questionnaire events).	Azure Data Lake
Azure	Information about scheduled infrastructure changes, scaling events, and system events are immutably stored for audit trail purposes.	Azure Monitor

Complementary User Entity Controls (CUECs)

The Company's controls related to SnapComms cover only a portion of overall internal control for each user entity of SnapComms. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list

Criteria	Complementary User Entity Controls
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses Azure as a subservice organization for Platform-as-a-Service (PaaS) provider. The Company's controls related to SnapComms cover only a portion of the overall internal control for each user entity of SnapComms. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Azure's physical security controls mitigate the risk of unauthorized access to the hosting facilities. Azure's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management reviews the Azure SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by Azure to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to Azure management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to SnapComms to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls taking into account the related CSOCs expected to be implemented at Azure as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• Azure is responsible for ensuring data stores are encrypted at rest.
CC6.4	• Azure is responsible for restricting data center access to authorized personnel. • Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.

Criteria	Complementary Subservice Organization Controls
CC6.5 CC6.7	• Azure is responsible for securely decommissioning and physically destroying production assets in its control.
CC6.6 CC6.7	• Azure is responsible for restricting the transmission of data to authorized users and processes.
CC6.8 CC7.2 CC7.3 CC8.1	• Azure is responsible for patching infrastructure supporting the service as a result of identified vulnerabilities.
CC7.2 A1.2	• Azure is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • Azure is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.
CC9.1 A1.2	• Azure is responsible for employing a multi-location strategy for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.
A1.2	• Azure is responsible for configuring daily differential and weekly full backups for data stores housing sensitive customer data. • Azure is responsible for database replication to secondary data centers in real time and for alerting administrators of replication failures.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of SnapComms. Commitments are communicated in the Company's Master Service Agreement (MSA).

System requirements are specifications regarding how SnapComms should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to SnapComms include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will implement appropriate technical and organizational measures to protect client data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data (a "security incident"). • The Company will implement measures to remedy or mitigate the effects of a security incident and to keep the client informed of all developments of such an event.	• Access controls for access to all systems and data. • Risk assessments • Change management controls • Encryption standards
Availability	• The Company will ensure 24/7/365 technical support availability. • The Company will implement measures to remedy or mitigate the effects of an availability incident and to keep the client informed of all developments of such an event.	• Monitoring controls • Backup and recovery standards • Disaster recovery plan
Confidentiality	• The Company will not disclose any confidential information to any person or entity other than the representatives of the Company who have a need to know such information in the course of the performance of their duties. • Upon any termination of services, the Company will continue to maintain the confidentiality of the customer's confidential information and, upon request and to the extent practicable, destroy all materials containing such confidential information. • The Company will notify the customer if the Company becomes aware of a breach of confidentiality. • The Company will protect the customer's confidential information in the same manner that it protects its own confidential information, but in no event using less than reasonable care.	• Data classification • Retention and destruction policy • Non-disclosure agreements (NDAs) • Employee training • Employment agreements