A-LIGN

Everbridge, Inc.

Type 2 SOC 3

2023

everbridge™

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF EVERBRIDGE, INC. MANAGEMENT

ASSERTION OF EVERBRIDGE, INC. MANAGEMENT

May 18, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Everbridge, Inc.'s ('Everbridge' or 'the Company') Critical Event Management (CEM) Platform throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Everbridge'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* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Everbridge, Inc.'s Description of Its Critical Event Management Platform throughout the period April 1, 2022 to March 31, 2023" 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 April 1, 2022 to March 31, 2023, to provide reasonable assurance that Everbridge's service commitments and system requirements were achieved based on the trust services criteria. Everbridge'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 "Everbridge, Inc.'s Description of Its Critical Event Management Platform throughout the period April 1, 2022 to March 31, 2023".

Everbridge uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Everbridge, to achieve Everbridge's service commitments and system requirements based on the applicable trust services criteria. The description presents Everbridge's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Everbridge'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 to achieve Everbridge's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Everbridge's controls.

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 April 1, 2022 to March 31, 2023 to provide reasonable assurance that Everbridge'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 Everbridge's controls operated effectively throughout that period.

Karen Meohas

Karen Meohas
Senior Director of Global Compliance
Everbridge, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Everbridge, Inc.

Scope

We have examined Everbridge's accompanying assertion titled "Assertion of Everbridge, Inc. Management" (assertion) that the controls within Everbridge's CEM Platform were effective throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Everbridge'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* in AICPA *Trust Services Criteria*.

Everbridge uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Everbridge, to achieve Everbridge's service commitments and system requirements based on the applicable trust services criteria. The description presents Everbridge's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Everbridge's controls. The description does not disclose the actual controls at the subservice organization. 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.

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

Service Organization's Responsibilities

Everbridge 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 Everbridge's service commitments and system requirements were achieved. Everbridge has also provided the accompanying assertion (Everbridge assertion) about the effectiveness of controls within the system. When preparing its assertion, Everbridge 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 effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

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 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 the policies or procedures may deteriorate.

Opinion

In our opinion, management’s assertion that the controls within Everbridge’s CEM Platform were suitably designed and operating effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Everbridge’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Everbridge’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on Everbridge’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Everbridge, user entities of Everbridge’s CEM Platform during some or all of the period April 1, 2022 to March 31, 2023, business partners of Everbridge subject to risks arising from interactions with the CEM Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
May 18, 2023

SECTION 3

EVERBRIDGE, INC.’S DESCRIPTION OF ITS CRITICAL EVENT MANAGEMENT PLATFORM THROUGHOUT THE PERIOD APRIL 1, 2022 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

Everbridge, Inc. (Everbridge) is a global software company who provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running.

Everbridge was founded in 2002 in the aftermath of the September 11 terrorist attacks, with the mission of empowering organizational resilience at scale. Everbridge began by building a notification engine to ensure that communications are received without fail when life and organizational safety is at risk.

Since inception, the software-as-a-service (SaaS) based CEM (Critical Event Management) Platform was architected to deliver multi-tenant capability and the speed, scale, and resilience necessary to communicate globally when a critical event occurs. The CEM Platform is designed to address both the emergency and operational components of a critical event and communications program.

Description of Services Provided

The CEM Platform delivers reliable enterprise-ready applications that support the visualization, orchestration, communication, and collaboration capabilities required to ensure operational resiliency to keep people safe and businesses running.

The CEM Platform applications include:

- Mass Notification - a secure, scalable, and reliable mass notification platform application that enables enterprises and governmental entities to send contextually aware notifications to individuals or groups to keep them informed before, during, and after critical events. This application provides analytics, map-based targeting, flexible group management, distributed contact data, language localization, multiple options for contact data management, and a globally optimized approach to voice and SMS routing.
- Crisis Management - optimizes customers' critical event response by orchestrating all crisis activities, teams, resources, and communications in one application. With all stakeholders - from responders in the field to executives in the boardroom - working from a common operating picture, customers can be assured that their plans are executed.
- Incident Management - an incident management platform application that enables organizations to automate workflows and make their communications contextually relevant using drag and drop business rules to determine who should be contacted, how they should be contacted, and what information is required. This application also supports cross-account collaboration and situational intelligence sharing during crises for corporations and communities.
- Information Technology (IT) Alerting - an IT alerting application that enables IT professionals to alert and communicate with key members of their teams during an IT incident or outage, including during a cybersecurity breach. The application integrates with IT service management platforms and uses automatic escalation of alerts, on-call scheduling, and mobile alerting to automate manual tasks and keep IT teams collaborating during an incident. This application also provides shift calendars with integrated on-call notifications to help users better manage employee resources in order to get the right message to the right person at the right time through automated staffing.
- Safety Connection - with an increasingly mobile workforce, distributed teams, and large campuses, this platform application helps businesses and organizations quickly locate and communicate with their people. Safety Connection aggregates geo-location data from multiple systems so that organizations can reach out to those who are potentially at risk (employees, contractors, visitors).
- Visual Command Center - this visualization and orchestration application of the CEM Platform helps organizations aggregate risk data and drive a coordinated response. The application serves as the backbone for the command centers of some of the largest organizations in the world, dynamically displaying threat intelligence and data related to business operations, continuity, security, and the supply chain.

- Risk Center - this risk intelligence and situational awareness application of the Platform combines thousands of the most trustworthy data sources with an experienced team of analysts to empower organizations to proactively monitor and mitigate risk. Built on the Visual Command Center platform, the solution leverages powerful visualization tools and hyper-local risk intelligence from the Risk Intelligence Monitoring Center (RIMC) to provide situational awareness and help organizational functions such as security, business continuity, supply chain, and operations mitigate or eliminate the impact of risk.
- Care Converge - a comprehensive clinical communications platform application that helps healthcare organizations coordinate with clinical staff in seconds for all-hands clinical emergencies, as well as day-to-day communications such as shift coverage and patient transitions.
- Community Engagement - a community engagement application that integrates emergency management and community outreach by providing local governments with a unified solution to connect residents to both their public safety department, public information resources, and neighbors via social media and mobile applications. This platform application improves the communication reach for emergency personnel, while providing residents with real-time emergency and community information, and allows residents to anonymously opt-in and provide tips.
- Mobile Applications - two separate mobile applications - one for residents and employees, and one for critical event managers - enables customers to ensure they can initiate critical communications while mobile, and their recipients can also be reached no matter their location.

Principal Service Commitments and System Requirements

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

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

The principal service commitments and system requirements related to CEM Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Everbridge 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 “material security incident”) • Everbridge 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 • Configuration Standards • Secure Development Life Cycle

Trust Services Category	Service Commitments	System Requirements
Availability	• Everbridge will ensure 24/7/365 technical support availability • Everbridge 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 • Contingency Plan and Exercise
Confidentiality	• Everbridge will not disclose any confidential information to any person or entity other than the representatives of Everbridge who have a need to know such information in the course of the performance of their duties • Upon any termination of services, Everbridge 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 • Everbridge will notify the customer if Everbridge becomes aware of a breach of confidentiality • Everbridge 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 • Data Processing Agreements • Privacy by Design

Components of the System

Infrastructure

Primary infrastructure used to provide Everbridge's CEM Platform includes the following:

Primary Infrastructure	
Production Service	**Business Function**
AWS Networking: VPC, Subnets, NAT/Internet Gateway, ELB/ALB/NLB Load Balancers	Implement Virtual Private Datacenter with isolated network
AWS Route 53	DNS Service
AWS Elastic Computer Cloud (EC2) and Elastic Block Storage (EBS)	Virtual hosting service including storage

Primary Infrastructure	
Production Service	**Business Function**
AWS EKS	Kubernetes based container orchestration
AWS S3	Cloud storage
AWS SQS	Queueing service
AWS SNS	Pub/Sub Queueing service
AWS SES	E-mail delivery service (MTA)
AWS EFS	Shared network file server
AWS Open Search Service	Elasticsearch Database
AWS RDS	PostgresSQL database
AWS Elasticache	Redis and Memcache caching service

Software

Primary software used to provide Everbridge's CEM Platform includes the following:

Primary Software	
Production Service	**Business Function**
Datadog, Alert Site, CloudHealth	Infrastructure Monitoring, availability and performance
Pendo	User and Page Telemetry
Sumo Logic	Log Monitoring
Sophos	Antivirus - Endpoint Protection
Qualys & Veracode	Vulnerability Scanning
Mongodb	Database/Backup/Replication Software
Amazon GuardDuty	Intrusion Detection
Cloudflare	External web application network traffic data
Honeycomb	Application Performance Monitoring
Snowflake	Data Lake and Analytics platform
Postgres SQL	Database
AWS Services: EC2, EKS, S3, VPC, SQS, SNS, SES, OSS	Basic IaaS and related services for computer, network and storage
Gitlab	Source code management and deployment pipelines
Terraform	Infrastructure as Code automation
SaltStack and salt-cloud	Configuration management

People

Everbridge is comprised and supported by the following teams responsible for the delivery and management of the Everbridge SaaS:

- Engineering: Responsible for the development, testing, deployment, and maintenance of new code for Everbridge. Also monitoring the infrastructure and maintaining the security of the production environment.
- Operations: Responsible for managing access control.
- Product Management: Responsible for overseeing the product life cycle, including adding new product functionality.
- Compliance and Legal 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.
- Information Security Team: Supports Everbridge platform by monitoring Internal and external security threats and maintaining security systems including malware and antivirus as required.
- People and Culture Department: Defines policies and procedures for recruitment and termination of employment including initiating the instruction to remove access.
- Corporate IT: Responsible for implementing and maintaining internal network security and access control requirements.

Data

Everbridge customers can use the CEM Platform to visualize, orchestrate events, and send notifications to recipients where the content of the notification or message is completely determined by the customer.

For message recipients, the CEM Platform stores and processes the contact data for each recipient. The recipient contact data may be classified as personally identifiable information (PII). This information may include first name, last name, address, phone numbers (home, work, mobile, etc.), e-mail addresses, fax, and pager numbers, as well as contact attributes associated with communication preferences, language spoken, technical certifications, on-call status, etc.

Everbridge has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

Processes, Policies and Procedures

Policies and procedures are in place and include the automated and manual procedures involved in the operation and maintenance of CEM Platform. These include those relating to product management, engineering, technical operations, security, and IT. These procedures are drafted in alignment with the overall information security policies and include Business Continuity, Vulnerability Management, Vendor Management, Physical Security, Operations Security, Asset Management, Cryptography, Access Control, and Acceptable Use. All policies are updated and approved as necessary for changes in the business, but no less than annually. All teams are expected to adhere to the Everbridge policies and procedures that define how services should be delivered. These are located on Everbridge’s shared drive and can be accessed by any Everbridge team member.

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

Procedure	Description
Access Control	How Everbridge restricts logical access, provides and removes that access, and prevents unauthorized access
Operating Procedures for Information and Communication Technology (ICT)	How Everbridge manages the operation of the system and detects and mitigates processing deviations, including logical security deviations

Procedure	Description
Change Management	How Everbridge identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made
Risk Mitigation	How Everbridge identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners
Secure Development	How Everbridge 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 Everbridge ensures the proper and effective use of cryptographic controls in order to protect the confidentiality, authenticity, and integrity of information
Business Continuity	How Everbridge establishes the steps necessary to implement business continuity management for the Everbridge product

Physical Security

Everbridge Head Office (Burlington, MA) and its satellite offices have physical security measures that are designed to deny unauthorized access to equipment, resources, and to protect personnel and property from damage or harm.

The organization’s sensitive areas are secured via door locks, keycard access controls, physical intrusion detection systems, visitor access control procedures, employee ID badges, and video surveillance systems. Everbridge uses keycard access control systems and badge readers to restrict access to its facilities, and these employee badges and key cards are assigned to personnel using the principle of least privilege.

The company manages its surveillance systems, access controls systems, and alarms. The organization’s facilities are monitored by security surveillance camera systems, with cameras monitoring all ingress and egress points and sensitive areas. Visitors to the facilities are required to complete an entry in its visitor logs, which document all relevant details regarding the visitor.

Logical Access

The CEM Platform is entirely separate from the Company’s corporate infrastructure. Approved operations personnel utilize a Federal Information Processing Standards (FIPS)-validated virtual private network (VPN) solution to connect to the CEM Platform production environment. The VPN solution itself requires the use of two-factor authentication and is integrated into a centralized Identity Provider (IdP) service. This allows the Company to quickly grant, audit, and revoke access as needed.

Identification and authorization within the IdP are designed to meet stringent Federation Assurance Level 2 (FAL2) user identity, password, and multi-factor requirements as stipulated by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3.

Once successfully authenticated and connected via the VPN, in order to access EC2 and data instances, administrators connect to a farm of bastion hosts, which also authenticate against the centralized IdP. These bastion hosts enforce Data Loss Prevention (DLP) as well as malware protection mechanisms to protect the CEM Platform.

Access to the CEM Platform is granted only to staff with an appropriate business need and relevant job function. Furthermore, access is further restricted based on a least privileged principle, where increasingly fewer individuals have higher levels of access.

At the network access tier, the CEM Platform is protected inside a tightly managed set of virtual networks. Based on a default-deny principle, only network traffic required for proper functioning of the CEM Platform is allowed to flow in and out of these virtual networks. Inside each virtual network, all systems are protected by systems-specific, software-defined firewalls that further extend the default-deny principle and only allow explicitly allowed traffic to flow to and from each system.

Furthermore, the CEM Platform is protected by a state-of-the-art web application firewall (WAF) that detects and prevents suspicious or malicious access from reaching the platform.

User Account Revocation

Upon termination of employment or an external party contract, the People and Culture Department immediately initiates the removal of all access rights granted to the party in question to avoid unauthorized access by ex-employees or ex-contractors. The following is performed when revoking user access:

- Collecting physical assets allocated to the user (e.g., laptop, office key).
- Removing access to the password management system.
- Removing application user accounts by their asset owners.
- Removing or suspending the user’s user ID (e.g., email address).
- Updating access right records to reflect the changes.
- Changing passwords to accounts that will remain active and are known by the departing party.

User Access Review

The Company reviews user access rights during employee onboarding, when an employee changes their role, and during exit of employment events. When these events are triggered, the employee account is checked for any irregularities in access rights, and access rights are amended or removed, as necessary.

When reviewing the access rights of an asset, the asset owner should consider:

- Whether the current users’ access rights match their current role and access profile
- If redundant user access is removed
- Whether privileged access that is no longer needed is removed

Computer Operations - Backups

Geographic replication is enabled and occurs daily to support continuity efforts.

Two-form factor authentications are required to access the hosting administration consoles and all access is monitored and logged.

Computer Operations - Availability

The availability category refers to the accessibility of the system or services as committed by the Company’s MSA. The availability of the CEM Platform is dependent on many aspects of the Company’s operations. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

Controls have been designed to address the following availability risks:

- Insufficient processing capacity
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Availability risks are addressed through the use and testing of various monitoring tools, replication setup, and backup and disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

Change Control

All changes to production systems and infrastructure must follow the Company's ITIL-based change management process, which requires varying degrees of review and approval based on different change categories.

This approach also ensures that critical tools such as infrastructure monitoring, log monitoring, malware scanning, file integrity monitoring, and vulnerability scanning are all embedded onto each system without exception. The centralized log aggregation and security information and event management (SIEM) solution ensures that all events are correlated to identify anomalous and/or suspicious activities quickly.

The Company's has a Change Advisory Board that meets weekly to review, discuss and approve (or reject) all Major change requests. GOCs and Security Operations Center (SOC) treat all alerts generated by the SIEM and other tools pursuant to the Company's incident response plan and high priority incident process. Any incidents classified as disaster recovery are covered by CEM Platform's contingency plan. The plan is tested at least annually to ensure applicability and accuracy.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Datacenter redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure. In the event that a primary system fails, the redundant systems are configured to take its place.

In-scope workstations are protected by virus protection software. The software is configured to perform updates to the list of known threats and to protect data from infection by malicious code or viruses in real time.

Qualys scans are performed daily. ECR scans are updated hourly. Veracode scans are automatically performed. New artifacts are submitted for ECR scans upon publishing and to Veracode on at least a monthly basis. Findings are identified and addressed.

Boundaries of the System

The scope of this report includes the CEM Platform developed and maintained by Everbridge, Inc. from its Head Office (Burlington, MA) and satellite facilities.

The scope of this report does not include the cloud hosting services provided by AWS at multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common / Security, Availability, and Confidentiality criteria were applicable to Everbridge's CEM Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing physical security controls for the housed in-scope system.

Complementary Subservice Organization Controls

Everbridge's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Everbridge's services to be solely achieved by Everbridge control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Everbridge.

The following subservice organization controls have been implemented by AWS included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4 CC7.2	Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team documentation.
		Physical access to data centers is approved by an authorized Individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Availability	A1.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Everbridge management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Everbridge performs monitoring of the subservice organization controls, including the following procedures:

- Communicating with the subservice organization to monitor compliance with the service agreement and stay informed of changes planned at the hosting facility and relay any issues or concerns to AWS management.
- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring the services performed by vendors and subservice organization(s) to determine whether operations and controls expected to be implemented are functioning effectively.

COMPLEMENTARY USER ENTITY CONTROLS

Everbridge's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Everbridge's services to be solely achieved by Everbridge control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Everbridge's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls:

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
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