Cellebrite

Service Organization Controls 3 Report

For the period November 01, 2024 to September 30, 2025

REPORT ON CONTROLS PLACED IN OPERATION AT CELLEBRITE LTD.
RELEVANT TO SECURITY AND CONFIDENTIALITY
FOR THE PREMIUM AS A SERVICE

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations ™

Management’s Report of its Assertions on the Effectiveness of Its Controls over the Cellebrite Premium as a Service Based on the Trust Services Criteria for Security, and Confidentiality

March 4, 2026

We, as management of Cellebrite Ltd. are responsible for:

- Identifying the Cellebrite Premium as a Service (System) and describing the boundaries of the System, which are presented in Attachment A.
- Identifying our service commitments and system requirements.
- Identifying the risks that would threaten the achievement of our service commitments and system requirements that are the objectives of our System, which are presented in Attachment B.
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirement.
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

Cellebrite Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Cellebrite Ltd.to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Cellebrite Ltd.’s controls. It does not disclose the actual controls at AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period November 1, 2024 to September 30, 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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.*

Very truly yours,

Signed by:
Sigalit Shavit
97250DDA0D4C491...

Sigalit Shavit, CIO

Signed by:
Ronen Armon
7EBEACB58277463...

Ronen Armon, Chief Product & Technology Officer

EY
Shape the future
with confidence

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Independent Service Auditor's Report

To the management of Cellebrite Ltd.

Scope:
We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the Cellebrite Premium as a Service Based on the Trust Services Criteria for Security and Confidentiality (Assertion), that Cellebrite Ltd.'s controls over the Cellebrite Premium as a Service (System) were effective throughout the period November 01, 2024 to September 30, 2025, to provide reasonable assurance that Cellebrite Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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*.

Cellebrite Ltd. uses Amazon Web Services ('AWS') (subservice organization) to provide infrastructure management services. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Cellebrite Ltd., to provide reasonable assurance that Cellebrite Ltd.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 01, 2024 to September 30, 2025.

Management's responsibilities
Cellebrite Ltd.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Cellebrite Ltd.'s service commitments and system requirements were achieved. Cellebrite Ltd. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our responsibilities
Our responsibility is to express an opinion on the controls over the System, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether the controls over the System operated effectively, in all material respects. An examination involves performing procedures to obtain evidence about the controls over the System, which includes: (1) obtaining an understanding of Cellebrite Ltd.'s relevant Security and Confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Cellebrite Ltd.’s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Cellebrite Ltd.’s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Cellebrite Ltd.’s AI services.

We are required to be independent of Cellebrite Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Cellebrite Ltd.’s service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion
In our opinion, Cellebrite Ltd.’s controls over the System were effective throughout the period November 1, 2024 to September 30, 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use
This report is intended solely for the information and use of Cellebrite Ltd. And user entities of Cellebrite Ltd.'s Cellebrite Premium as a Service, and is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global Limited

March 4, 2026
Tel-Aviv, Israel

Attachment A: Description of the Premium as a Service

Company & System Overview and Background

Cellebrite, the creator of Premium as a Service is the global leader in partnering with public and private organizations to transform how they manage Digital Intelligence in investigations to protect and save lives, accelerate justice, and ensure data privacy.

Cellebrite aid organizations with the complexities of legally sanctioned digital investigations with a Digital Intelligence Investigative Platform and services to unify the investigative lifecycle and manage digital evidence.

Products and Services Offered by Cellebrite Premium as a Service's

Premium as a Service helps maximize data access and boost productivity by providing ad-hoc exclusive Premium capabilities to every UFED connected.

Cellebrite's Premium as a Service provides benefits for lab technicians and examiners by giving lawful unlock and extract capabilities for the widest range of iOS and Android devices – and giving access to more evidence.

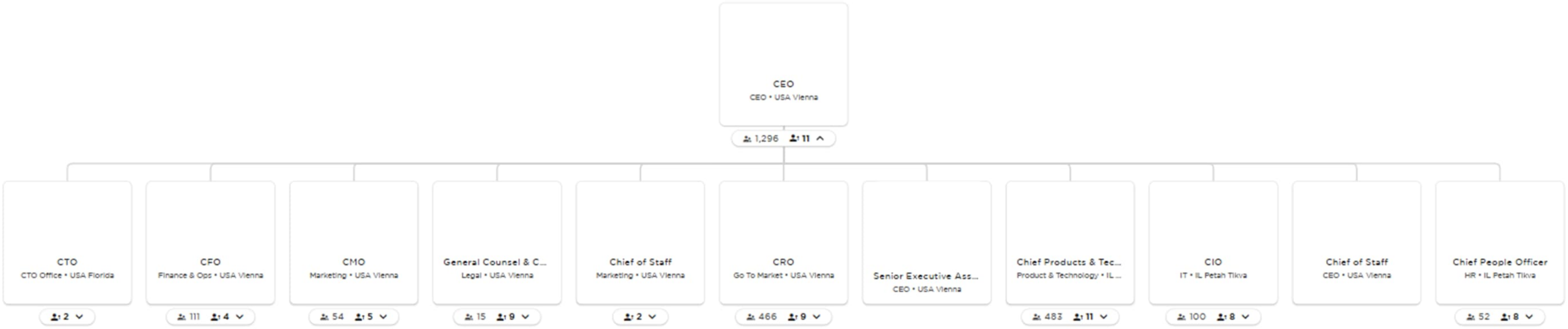
Premium as a Service enables agencies of all sizes to receive a flexible and cost-effective solution that overcomes budget and technology barriers and accelerates time to justice by moving investigations along swiftly with easier and expanded access to advanced data.

Investigations that require advanced mobile device access can now use Premium as a Service packaged to fit agencies' precise needs, and taking advantage of their deployed UFED fleet to create a multiplier network effect. This SaaS offering also frees agency personnel from the time-consuming task and complexities of hardware maintenance.

Premium as a Service introduces new possibilities for eliminating the barriers related to resource and technology constraints that prohibit lawful mobile device access. The technology to unlock many of the most popular iOS and Android devices along with the training needed to do it, is now available in convenient packages that deliver the necessary capabilities when, where, and how examiners need it.

Organizational Structure

Formal policies and procedures are documented, reviewed, and approved on an annual basis by the management and are available to the company's employees. The organization maintains defined roles and responsibilities for managing security and operations:



Overview of the company’s Internal Controls

A company’s internal control is a process – effected by Cellebrite (Premium as a Service)'s Boards of Directors, management, and other personnel – designed to enable the achievement of objectives in the following categories:

- Adherence to the organization policies and procedures
- Effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

The company maintains policies, processes, and governance structures that support the Security and Confidentiality commitments.

Risk Assessment

Cellebrite (Premium as a Service) is committed to managing and minimizing risk by identifying, analyzing, assessing, mitigating, and treating exposures that may hinder, prevent or otherwise impact the company from achieving its goals and serving its clients. Cellebrite (Premium as a Service) recognizes risk management as a strong consideration in strategic and operational planning, daily management, and decision-making at all levels of the company.

Risk identification: The process of identifying, assessing, and managing risks is a critical component of Cellebrite's system of internal controls. The purpose of Cellebrite's risk assessment process is to identify, assess and manage risks that affect the organization’s ability to achieve its objectives. Risk analysis identifies key business processes in which potential exposures of some consequence exist. Exposures consider both internal and external influences that may harm Cellebrite's ability to provide reliable services. The risk identification process addresses the following at minimum:

- Identifying information assets, including physical devices and systems, virtual devices, software, data, and data flows, external information systems, and organizational roles
- Assessing the criticality of information assets
- Identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events
- Identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, business partners, customers, and others with access to Cellebrite's information systems.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks. Cellebrite (Premium as a Service)’s operating and functional units are required to implement control activities that help achieve business objectives associated with the following:

- Adherence to the organization's policies and procedures
- The effectiveness and efficiency of operations
- Compliance with applicable laws and regulations

The control activities are designed to address specific risks associated with Cellebrite (Premium as a Service) operations and are reviewed as part of the risk assessment process. Cellebrite (Premium as a Service) has developed formal policies and procedures covering various operational matters to document the requirements for the performance of many control activities.

Information and Communication

Information and communication are integral components of Cellebrite (Premium as a Service)'s internal control system. They involve the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization’s operations. At Cellebrite (Premium as a Service), information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees. A description of the Cellebrite system and its boundaries is documented and communicated to Cellebrite employees and to external users through the Cellebrite website.

Logical and Physical Access

A security policy is documented by Cellebrite (Premium as a Service) management and is reviewed and approved on an annual basis.

Cellebrite (Premium as a Service) has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. The assets inventory is managed using automated tools and any non-compliant or problematic devices are then flagged and a notification is generated and the device is blocked until resolved.

Access Control, User, and Permissions Management

Access to Cellebrite (Premium as a Service) information assets is restricted using strong password settings. Cellebrite (Premium as a Service) employees and contractors will not be granted access to any information asset that is not directly needed for their work in Cellebrite (Premium as a Service).

Access to system resources is protected by means of the following security measures:

1. Access to alter and delete backups is restricted to authorized users and uses strong authentication methods.
2. Endpoint protection platform is installed on employees' devices (i.e., workstations and laptops), centrally managed, and configured to receive updates regularly.

Additionally, Cellebrite (Premium as a Service) access to the identity management tool is performed using two-factor authentication and is restricted to authorized personnel. User access and permissions in Cellebrite environments are provisioned using a centralized tool. There is a dedicated team that is responsible for reviewing and actioning any exceptions flagged.

Revocation Process

User accounts are disabled or deleted on the production and other organizational information assets timely upon notification of job termination. Organizational devices are returned upon leaving the organization.

System Access

Access to the production environment console is restricted to authorized personnel and performed using a two-factor authentication method. Privileged access rights are defined as any access authorizations created for the employee for their work, temporarily or permanently, beyond those specified in respect of their position in the user permissions table. Access to the source control tool is performed using two-factor authentication and is restricted to authorized personnel.

Physical Access and Visitors

Physical access to Cellebrite's office is restricted to authorized personnel using secure authentication methods and visitors to the Cellebrite office are accompanied while on premises. Employees encountering an unfamiliar or suspicious person wandering around the office are expected to ask them politely about the nature of their business and if necessary, accompany them to their host. Visitors are not allowed to access or connect to Cellebrite (Premium as a Service) company’s network or equipment.

Software Development Lifecycle (SDLC) Overview

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the change management application. Each change goes through a life cycle. Infrastructure changes are reviewed, approved, and implemented through a change management process. All changes are logged, assessed for risk, and tested prior to deployment. Code changes must be reviewed and approved in order to progress through the SDLC and deploy a version to production.

Software Testing and QA Process: A successful test result is mandatory in order to continue with the SDLC process and deploy a version to the production environment. Procedures are in place to ensure automated testing is performed on approved data and test plans in order to ensure the overall security status of the production environment.

Software Release: The company enforced segregation between development, staging, and production environments to enforce confidentiality and privacy on customers' data.

Description of the Production Environment

Production Environment

The processes described below are executed within Cellebrite (Premium as a Service)'s production environment, which is hosted through AWS Virtual Private Cloud - located globally.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between Cellebrite (Premium as a Service)'s cloud service components.

To provide sufficient capacity, Cellebrite (Premium as a Service)'s network infrastructure relies on platforms provided by AWS. To ensure appropriate network security levels, Cellebrite (Premium as a Service) security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality and availability.

Production Monitoring

Cellebrite (Premium as a Service) has an established internal audit function that evaluates management's compliance with Cellebrite (Premium as a Service)'s identity management, source code management, and infrastructure controls. Audit trail (security logs) is deployed on the production environment 24/7 to capture actions made directly by the user or a cloud service. Actions performed in the production environment, including OS, DB, and application are monitored, logged, and reviewed.

Security and Architecture

Cellebrite (Premium as a Service) provides a secure, reliable, and resilient Software-as-a-Service that has been designed based on industry best practices. The below addresses the network and hardware infrastructure, software, and information security elements that Cellebrite (Premium as a Service) delivers as part of this, database management system security, application controls, and intrusion detection monitoring software. The company has developed a Security Incident Response Policy in order to respond to security incidents and personal data breaches in accordance with applicable laws and regulations.

Data Center Security

Cellebrite relies on the global infrastructure of AWS which can include the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards and regulations.

Infrastructure Security

- *End-to-End Network Isolation* - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud from being intercepted.
- *External & Internal enforcement points* - All servers are protected and restricted. The configuration of the cloud providers' firewall rules is restricted to authorized personnel.
- *Server Hardening* - all servers are hardened according to industry best practices.

Application Security

- *Penetration Testing* – An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner.
- *Vulnerabilities Management* - Internal vulnerability scanning is performed by the relevant teams using sufficient tools. Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated as required by the internal team.
- *Segregation of Customer Data* - During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. Part of Cellebrite (Premium as a Service)'s logical security procedures is to ensure users are segregated from each other.

Operational Security

- *Configuration and Patch Management* – Cellebrite (Premium as a Service) makes use of a centrally managed configuration management system. Patch management is in process for the company's laptops and servers. Security settings are hardened and cannot be changed by users. Alerts and remediation are triggered automatically when deficiencies are discovered.
- *Security Incident Response Management* - The company's contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. Whenever a security incident of a physical or electronic nature is suspected or confirmed, Cellebrite (Premium as a Service)'s engineers are instructed to follow appropriate procedures. Customers and legal authorities are notified as required by Privacy regulations. IT vendors that engage in business with the company are subject to information security, confidentiality, and privacy commitments as part of their agreements with the company. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet Cellebrite (Premium as a Service)'s objectives related to privacy.
- *Endpoint Protection* - The company secures and controls its employees' laptops to enforce its security settings, including hard-disk encryption, auto-patching, password requirement, auto screen-lock, and remote wipe capabilities and deployment of additional policies.

Security Awareness & Training

All Cellebrite (Premium as a Service) employees need to be well aware of their information security responsibilities. Awareness is achieved by communicating Cellebrite (Premium as a Service)'s security policies and guidelines to employees in various ways. The Cellebrite (Premium as a Service) security team works to implement security awareness and responsibilities based on the Cellebrite (Premium as a Service) security awareness program. The company has established a Security Awareness Training program and requires employees to complete this training every year.

Support

Client issues are reported to the company via a dedicated support email address. Support issues are handled by using a ticketing system and according to the support policy. Customers can contact the support team through dedicated support channels. The company maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact the company's business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer.

Attachment B: Principle Service Commitments and System Requirements

Confidentiality Procedures

Customer confidentiality is a key factor in Cellebrite (Premium as a Service). As such, Cellebrite (Premium as a Service) has implemented security measures to ensure the confidentiality of its customers' sensitive personal information. All active devices in the production network are included for tracking and reporting purposes. Upon Customer request at the end of a contract agreement, Cellebrite (Premium as a Service) will dispose of customer confidential information.

Confidentiality considerations are incorporated into contracts with vendors and third parties with restricted access are reviewed by Cellebrite (Premium as a Service) and the third party at the time of contract creation or renewal. The review includes identifying and documenting the controls in place at the company to address the CUECs, noted deviations, and the auditor's opinion.

Data Encryption

Cellebrite (Premium as a Service) uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk. Processes are in place to protect encryption keys during generation, storage, use, and destruction. The company has an established key management process in place to support the organization’s use of cryptographic techniques.

Data at Rest and Data in Transit

Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms; data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key; data encryption keys are stored with the data, and encrypted with key encryption keys that are exclusively stored and used inside the providers' central key management services; which are redundant and globally distributed.

Premium-as-a-Service uses TLS 1.2 and TLS 1.3 with high-grade ciphers to ensure that all traffic is securely encrypted in transit.

****