Cellebrite

Guardian

Cellebrite Guardian
Security Overview

Reviewed September 2026

Cellebrite Guardian

CELLEBRITE GUARDIAN SECURITY OVERVIEW

Security is our highest priority at Cellebrite. This document provides a detailed overview of the security framework, system design, and operational best practices that power the Cellebrite Guardian Suite.

Guardian was built according to the principles of **Security by Design**, the principle that Security is built into the product from day one and not as an addition, and **Zero Trust**, the principle assumes that every interaction is "untrusted" and should be secure and verified.

In addition, we're providing details on infrastructure security, procedures, policies, and the data center security standards our infrastructure providers share.

Security By Design

Cellebrite implements the **Secure Software Development Lifecycle** (SDLC) that ensures security is embedded in our development and deployment processes and establishes the implementation of the security deliverables in alignment with the software development lifecycle:

1. At the Planning phase, security requirements are collected and added to the system requirements.
2. At the Design phase, our security architect performs a Threat Modeling Assessment (TMA) and designs the security controls required for the security risk mitigation.
3. At the Development phase, we utilize the best-in-class security scanning tools that perform Static Application Security Testing (SAST), Software Composition Analysis (SCA) and Image Scanning to identify vulnerabilities in the code developed by our engineers and in the open-source components.
    - Vulnerabilities are prioritized using advanced tools, industry methodology and manual assessments.
    - Mitigation of vulnerabilities is handled in accordance with the company policy.
4. At the Validation phase, we perform security validation, API fuzzing and Dynamic Application Security Testing (DAST).
5. Penetration Testing based on the Open Web Application Security Project (OWASP)
    - Conducted by a 3rd party assessor for major product releases.
    - Mitigation plan is defined according to the Business Impact Assessment.

Cellebrite
Guardian

Defense in Depth

Security solutions have been put in place as part of our multi-layer protection approach for web and API traffic protection as well as the application runtimes.

- Network Firewall Providing anti-DDoS protection, advanced rate limiting solutions, and bot protection.
- Web Application Firewalls and additional cloud-native solutions protect the integrity of the web and API traffic processed by Guardian and prevent availability attacks on the system.
- Endpoint Protection platform monitors and protects the workloads running on the virtual machines (EDR) and Kubernetes clusters (CWPP).
- Cloud Security Posture Management solution is used to detect the vulnerabilities and security misconfigurations in the production environment.

Secure Coding Training

Cellebrite Research and Development employees, including software engineers, DevOps and QA undergo specialized training in Secure Coding with a focus on the software languages and development tools they use in their day-to-day work. Additionally, our security mindset program includes R&D security champions to implement security practices within the R&D teams.

Data Protection

- The Guardian Suite is hosted within the AWS cloud that provides high availability and security infrastructure. Hosting region is local to the customer, currently: US, Mexico, UK, Brazil, Australia, and Ireland.
- Each customer's data is kept segregated from any other tenant.
- Customer data at rest is encrypted using industry-standard AES-256 encryption.
- Tenant data is processed within isolated instances.
- Data in transit is encrypted using Transport Layer Security (TLS) 1.2 or above.

Data Center Security

Amazon Web Services (AWS) is a best-in-class cloud computing provider that delivers an infrastructure that is at least 99.99% available. Guardian is hosted in AWS Standard Cloud in the United States, Mexico, United Kingdom, Ireland, Australia, and Brazil, providing data residency and low latency. Other regions throughout the world will become available as demand dictates. Leveraging a provider like AWS ensures that Guardian is using a highly available and highly secure underpinning infrastructure capable of meeting data sovereignty requirements.

Guardian also adheres to the DOJ's Criminal Justice Information Systems (CJIS) Security Policy and further information can be provided for customers who need to be CJIS-compliant.

When necessary for specific compliance requirements, AWS GovCloud provides secure cloud hosting services designed for FedRAMP High baseline; U.S. International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4, and 5; FIPS 140-2; IRS-1075; and other compliance standards. Refer to AWS for more information on AWS GovCloud (US).

AWS Europe provides a secure cloud hosting environment conforming to ISO 27001, PCI DSS Level 1, Cloud Security Alliance (CSA), GDPR, System and Organization Controls (SOC), the NCSC UK's Cloud Security Principles, and more compliance standards. Refer to the AWS Compliance Center for resources on the AWS Great Britain environment.

Identity and Authentication

Guardian applications leverage the modern authentication protocol OIDC (OpenID Connect) together with the authorization code flow.

All Guardian users access the application using unique per-user credentials and multi-factor authentication. Additional authorization layers prevent users from accessing data without proper explicit permissions from organizational administrators. In addition, access control mechanisms are implemented to verify each web request's session validity and authenticity.

Sessions are established between the browser and Guardian. All sessions have an inactive timeout, which forces the user to log in / reauthenticate if no activity is detected for that session.

External Interface Protection

Guardian protects our interfaces by leveraging web security best practices, including secure headers that protect the web sessions and data security. The application uses public and private subnets with enforcing Network Access Controls to manage the traffic. Additionally, sensitive web cookies are protected with relevant security flags such as HttpOnly, Secure, and SameSite.

Secure User Management

Guardian employs robust measures to ensure the uncompromising separation of user pools per tenant, thus effectively mitigating any risk of unauthorized access or interference between disparate tenant environments and upholding the utmost confidentiality, availability, and integrity of each tenant's data and resources.

A Guardian Administrator configures user Roles and Permissions within the application at the workspace level. Guardian Investigate Administrator users can add users to the system, add additional Administrator users, reset passwords, and manage group permissions for the workspace.

Security Operations

Separation of Duties

Cellebrite Maintains strict separation between the Engineering and Production environments.

- Access to the production environment is limited to the team of Site Reliability Engineers (SREs) that perform the software upgrades and maintenance.
- SaaS platform operation and specifically access to the customers data repositories is monitored and scrutinized by the Cellebrite Threat Ops team.
- SRE access to the production environment is limited to company-approved assets that are running company-controlled endpoint protection services and are managed by Cellebrite IT.
- All the system actions are logged in alignment with the industry standards.
- Cloud infrastructure security logs are collected and processed by the Cellebrite Security Defense Center team.

Personnel Security

All employees working on Guardian are required to complete and comply with mandatory security training, have undergone background checks and are educated on supporting Guardian and working with underpinning contract providers such as AWS.

User Audit Logs

Guardian Administrators have access to the transactional event log that records system events—such as logins, uploads, downloads, and file views—but it does not track ongoing or behavioral user activity.

For example, Guardian tracks when a user or authorized reviewer logs into the solution, when they view a case file that has been assigned to them, when they upload an evidence file, or when they download an evidence file to view it locally. This supports the Activity Report and Chain of Custody Report that are available for purposes of understanding who has been given access to evidence and whether they viewed it, which is often information that must be disclosed in court.

But there is no tracking, monitoring, or screen recording of user activity, including how long a user spent viewing a particular page or which specific artifacts a user views inside a case file, such as emails, chat messages, photos, videos or map locations. That is behavioral user activity information and is not viewable or reportable data that be reviewed or exported by the host agency's Guardian administrator, nor can it be accessed by Cellebrite or any of its employees.

Since Guardian is only tracking user access and does not monitor user activity, we have ensured investigative and judicial integrity.

Supply Chain Security

Cellebrite conducts vendor risk assessments to ensure that the solution providers that are part of the Guardian solution/supply chain are secure and follow best practices wherever possible. Our assessments include questionnaires, a review of their certifications and reports, and, if appropriate, independent assessments.

Certification and Compliance

Cellebrite is compliant with the following standards:

ISO 27001

The global standard for IT security management.

ISO 27017

The global security standard for cloud service providers.

Cellebrite Guardian

European Union General Data Protection Regulation (GDPR)

Cellebrite maintains compliance with the EU GDPR and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the EU and Switzerland.

SOC2

Guardian completed a SOC 2 Type 2 assessment. SOC 2 is the de facto standard attestation of security control design for Software as a Service (SaaS) applications. You can rest assured that strict controls are in place to keep your data safe. Contact your Cellebrite sales representative for more information.

FedRAMP® High Authorized

Cellebrite is committed to meeting the highest levels of security compliance required by US government customers. **Guardian has achieved FedRAMP High authorization**, enabling federal agencies to securely host, share, and review digital evidence in a cloud environment assessed and authorized for federal use. It is currently listed in the FedRAMP Marketplace as Cellebrite Government Cloud.

IRAP

Cellebrite Guardian was independently assessed under the Infosec Registered Assessors Program (IRAP) at the PROTECTED tier, providing assurance that its security controls align with the requirements of the Australian Government Information Security Manual (ISM).

UK Cloud Security Principles

Guardian adheres to the Cloud Security Guidance and the 14 Cloud Service Principles defined by the National Cyber Security Centre.

Guardian Terms of Service

Guardian is governed by the SaaS Terms of Service. See the Terms of Service at:
https://legal.cellebrite.com/SaaS.htm

Privacy Statement

Cellebrite has a defined Privacy Policy. Read the policy at:
https://cellebrite.com/en/privacy-statement/

Cellebrite Guardian

Application and Data Security

Perimeter Security

Guardian is a Cellebrite solution that is deployed in the Cellebrite AWS environment. Cellebrite employs a multi-layered security approach to safeguard its AWS environments comprised of four defense layers. This solution is part of Cellebrite's defense-in-depth strategy.

The initial layer utilizes a distributed cloud service that routes all application traffic through robust external scrubbing services that provide advanced security controls, including DDoS protection, anti-bot services, and advanced web application protection.

The second layer serves as a central security point, protecting all accounts and preventing unauthorized access to Cellebrite's AWS environment. It enforces policies, access restrictions, and monitoring while offering advanced web application firewall capabilities, such as protection against injection attacks, cross-site scripting, and SQL injection.

The third layer deploys agile, app-centric security components in front of each microservice, utilizing advanced web application firewall capabilities like rate limiting, bot protection, IP reputation services, and schema validation to thwart suspicious activity and unauthorized access. Additionally, this layer ensures that all requests are authenticated and authorized before reaching the microservice, which provides an extra layer of protection.

The fourth and final layer is the zero-trust layer, delivering granular, fine-grained access control to each service. It ensures protection against internal and external attacks, ensuring that each service is fortified against all threats.

By deploying these multiple layers of security, Guardian provides a secure environment for our AWS deployments, guaranteeing the integrity and confidentiality of client data.

Asset Protection and Resilience

With Guardian, you choose the region where your data resides to meet your compliance and jurisdiction needs, which dictates where your data is stored, processed, and managed.

All customer data at rest, such as evidence files, are securely stored in Guardian using tenant-specific S3 storage using 256-bit AES encryption keys. Encryption keys are securely managed and are unique per customer. Access to customer data is restricted by permissions to the specific object storage bucket and the relevant decryption key.

This protects access to customer data and ensures that only authorized clients can access and process the data.

Data resilience ensures that data at rest is stored in multiple availability zones. The availability zones never span across regions, ensuring Guardian Investigate compliance with data governance laws.

Cellebrite regularly conducts back-ups of Guardian customer data to ensure data recovery. Backups are appropriately protected, ensuring only authorized individuals can access the protected data and that backup data is encrypted. Backups are stored in multiple availability zones as an added layer of protection; if a data center fails, your data is still safe.

Cellebrite has sanitization processes that ensure that your data is permanently deleted should you choose to leave the platform.

Cellebrite uses monitoring systems to identify performance issues and detect problems in the Guardian platform. The monitoring tools are integrated with a 24 / 7/ 365 alerting system to ensure the relevant teams are notified of any issues in the platform.

To ensure the secure and reliable management of secrets within our system, we have implemented a multi-faceted approach that combines the use of Kubernetes secrets, AWS Key Management system, AWS Secret Manager, and AWS Parameter Store. Kubernetes secrets provide a secure and reliable way to store and manage sensitive information, such as passwords, API keys, and certificates within our cluster, while AWS Key management system AWS Secret Manager and AWS Parameter Store allow us to store and manage secrets outside of the Kubernetes cluster with additional functionality such as rotation and auditing.

Furthermore, we have implemented a rigorous IAM policy that enforces the principle of least privilege for each service by providing a separate IAM role. For AWS resources, we use a unique IAM role to ensure that each service has access only to the resources it requires, reducing the risk of security breach due to compromised credentials. If we are not using AWS resources, we have implemented a separate database user for each service, which ensures each service has access only to the databases it requires and nothing more. This approach provides a high level of security and protection against potential security threats, ensuring that our secrets are securely managed, and access to them is strictly controlled.

Guardian is backed by a 99.95% uptime SLA which means that it will be there when you need it. Supporting transparency of the platform, Guardian Investigate leverages a status/trust site to reflect the status of the platform and to communicate pending maintenance to our customers. All customers can subscribe to this status page to be notified of maintenance or issues with the platform.

Visit the status page and subscribe today at: https://status.cellebrite.com.

Cellebrite
Guardian

Separation Between Tenants

Guardian is a multi-tenant solution. Traffic & Data isolation and segregation between tenants is designed and enforced from the ground up. Each data object stored in the system is confined to the relevant tenant scope. This allows for strict enforcement of role-based access policies and enforces tenant isolation & segregation. Each tenant's sub-environment is isolated via multiple abstract layers including network, identity, object stores, etc.

Guardian employs Amazon Elastic Kubernetes Service (EKS) to manage the Kubernetes cluster, providing a reliable and scalable platform for deploying containerized applications. To ensure a secure and isolated multi-tenant environment, Cellebrite has implemented a network architecture based on security groups and network policies using Calico, a popular open-source networking and network security solution for Kubernetes. This approach allows tenants to communicate only with authorized resources, providing a high level of security and isolation within the cluster. By leveraging these technologies together, we have created a secure and efficient environment that enables multiple teams or customers to share the same Kubernetes cluster while ensuring the confidentiality and integrity of their resources and data.

Additionally, to ensure the multi-tenant environment provides a high level of data segregation and security, Cellebrite has implemented measures to store each tenant's data in separate and secure resources. Specifically, we have created different resources such as distinct Amazon S3 buckets and databases for each tenant. This approach guarantees that each tenant's data is stored separately and is only accessible by authorized users. We have also enforced strict access controls to these resources by employing IAM policies that restrict access to only the necessary users and resources, thus reducing the likelihood of unauthorized access or data breaches. These measures provide a strong level of data security and privacy to our tenants, ensuring that their data remains confidential and secure.

The principle of 'least privilege' and 'separation of duties' dictates access control policies.

Similarly, "least privilege" and "separation of duties" concepts are also enforced within Cellebrite by cloud administrators. The tenant setup is deployed using IaaS (Infrastructure as a Service) technology. The IaaS cannot break the tenant isolation concept, which is enforced and managed by the Cellebrite Landing Zone enterprise administrators. This implementation is based on the AWS Landing Zone solution that establishes and implements the security baseline for our SaaS infrastructure.

The Cellebrite Security Landing Zone covers the following topics:

- AWS Organization and Accounts Structure
- Identity and Access Management
- Logging and Monitoring
- Infrastructure Security
- Data Protection
- Incident Response
- Cost Governance and Control
- Shared Services

Cellebrite Guardian

Third-Party Integration Security

Guardian supports an optional, customer-configured integration with Axon Evidence that lets authorized users export or archive case evidence directly into the customer's own Axon environment. Guardian remains the authoritative system of record for case data, custody, and history at all times.

Connector Authorization and Credential Management

A Guardian administrator connects to Axon using provider-issued API credentials created within the customer's own Axon account. Guardian exchanges these per-tenant credentials for short-lived Bearer tokens via an OAuth 2.0 client-credentials flow, refreshed automatically with no standing session. Credentials are stored in Cellebrite's managed secrets services under least-privilege access, are never exposed to end users, and are validated before use; invalid or disabled connectors are rejected.

Transfer, Access Control, and Entitlement

Every export or archive request is authorized against the user's identity, role, and tenant context, and gated by subscription entitlement and quota before it proceeds. Evidence moves directly from tenant-scoped Guardian storage to Axon over TLS, with integrity verified and transfers handled as idempotent, resumable operations so interruptions cannot create duplicate or partial evidence. Guardian also confirms the user is separately authorized within Axon before allowing them to select a destination case or container.

Export, Archive, and Audit

Export creates a copy of the evidence in Axon while the Guardian original is retained unchanged; Archive transfers a copy and then removes the local evidence data, retaining an artifact record for chain-of-custody traceability. All export and archive actions are logged in Guardian's audit and operational telemetry, feeding the same Activity and Chain of Custody Reports used for other evidence events. Responsibility is shared: Cellebrite secures credentials, enforces authorization, and encrypts data in transit; the customer provisions Axon credentials and governs evidence once it resides in Axon. The integration is inactive unless explicitly configured by the customer.

Operational Security

All changes are logged in our source code repository. We leverage standard deployment tools to provision Guardian ensuring audibility and the use of standard accepted configurations.

Cellebrite has a stringent software release policy. Notifications on pending releases are updated on the public status site (https://status.cellebrite.cloud) before the release, where possible. Urgent or critical releases may bypass this notification if deemed required.

The Cellebrite ThreatOps team continuously monitors product logs, infrastructure operations, and systems audit logs in our internal SIEM (Security Information and Event Management) to promptly detect and react to potential incidents. Cellebrite security has established a comprehensive strategy and policies to respond, notify and remediate security incidents. Cellebrite runs continuous and automated vulnerability scans for the Guardian assets, prioritizes vulnerability fixes, and quickly releases patches.

Our SOC (Security Operations Center) is staffed with highly qualified and experienced Security Analysts who work to keep the environments secure.

Cellebrite has a detailed incident response policy and plan. The approach ensures that security incidents are identified, contained, investigated, and remedied. There are also processes for documentation, reporting security incidents internally and externally, and a root cause analysis to identify and communicate improvements and actions that need to be made after every security incident. Security solutions have been put in place as part of our multi-layer protection approach for web and API traffic protection.

Leveraging the "Defense in Depth" principle, Cellebrite protects Guardian with multiple levels of protection including anti-DDoS protection, advanced rate limiting solutions, and bot protection all supported by next-gen Web Application Firewalls and additional cloud-native solutions for comprehensive overall web protection. These solutions protect the integrity of the web and API traffic processed by Guardian and prevent availability attacks on the system.

Governance Framework

Cellebrite has a security governance framework which coordinates and directs the management of Guardian and the information within it. The Chief Information Security Officer owns the Cellebrite Information Security Program. The Information Security Committee (ISC) governing the Information Security Policy, consists of a cross-functional team representing operational groups across the organization and is led by senior management. All employees are required to understand, agree, and adhere to the Information Security Policy. The Information Security Policy is reviewed and updated annually.

Security Questions

For security questions and inquiries, please get in touch with the Cellebrite Support Team: https://cellebrite.com/en/support/