Cellebrite

OCTOBER 2026

Autumn Release
Fact Sheet

Cellebrite's Autumn 2026 Release helps public safety, national security and business teams access more digital evidence, uncover deeper insights and turn findings into informed action. With expanded device access, new agentic AI capabilities and advances in mobile research and evidence management, the release helps teams reduce manual work and apply their expertise across increasingly complex investigations and operations.

WHAT'S NEW

Inseyets

Next-Generation Access: Expanded Access to More iPhones and iOS Support

Advanced AFU (After First Unlock) access to new iOS, including iOS 26.6, and the latest iPhones, including iPhone 15-17, ensures investigative and intelligence teams can gain access to critical evidence. Users gain access to a broader range of Apple devices, including more ways than ever to deploy with online, on-prem and air-gapped offerings. The latest access capabilities reduce reliance on limited acquisition options with Cellebrite's next generation of advanced access. By extending access to more devices and operating system versions, through new access and deployment methods, teams can get to the truth faster.

Advanced Unlocks for iOS: Available Now
Inseyets: Available Now

Expanded Android Access: Access the Widest Range of Devices with Greater Confidence

The latest advancements for Android expand support across the widest range of devices in the industry, including new support for widely used Nokia feature phones and expanded Samsung models. Not only do teams have access to the widest range of Android devices, but next-generation Samsung AFU capabilities provide a competitive edge when accessing mission-critical mobile devices. These enhancements enable data access from a larger portion of the Android ecosystem while improving coverage for modern Samsung devices. With broader device support available directly within existing workflows, agencies can bring specialized mobile forensic expertise to more investigations and intelligence-led operations.

Inseyets: Available Now
Advanced Unlocks for Samsung: Q4 2026

Offline Brute Force: Recover Information from Previously Inaccessible Devices

Offline Brute Force pairs UFED with Autonomy's offline processing capabilities, to enable accelerated dictionary attacks and custom rules-based analysis without relying solely on on-device processing. This allows for GPU acceleration reaching speeds of more than 49,000 hashes per second and removes size limitations of dictionaries. This capability expands access to evidence and intelligence that remain out of reach, allowing agencies to apply forensic expertise to a wider range of locked devices.

Available December 2026

UFED to PA Automated Streamline Flow

Users can now run and configure Streamline within automated workflows, enabling consistent and scalable processing with minimal manual intervention. This allows for seamless, efficient workflows within the Cellebrite ecosystem, cutting down extraction and decoding workflow times.

Available Now

Digital Collector: Expanded Support for the Latest Operating Systems

Digital Collector continues to keep pace with evolving technology environments, with planned support for the latest macOS and Windows releases. This helps investigators and enterprise teams maintain reliable access to digital evidence across modern computer systems while minimizing disruption to existing workflows.

Available November 2026

Tactical Extraction Kit (C-TEK): Bring Digital Intelligence to the Edge

The Cellebrite Tactical Extraction Kit is a complete hardware and software bundle designed for triage, extraction and analysis in any environment. With ruggedized computing, power independence, Faraday protection and support for multiple device types, operators can collect and analyze digital devices wherever an operation takes place. By putting digital forensics tools directly into the hands of field personnel, agencies can extend intelligence-gathering closer to the point of collection.

Available Now

CFID Drone Data Support in Physical Analyzer: Expand Investigations beyond Traditional Devices

New drone support enables Physical Analyzer users to visualize, analyze and interpret data collected from unmanned aerial systems (UAS). Drone data collected using CFID, the only product supported for upload to Physical Analyzer, can now be incorporated into existing workflows alongside data from mobile devices, computers and other digital sources, helping investigative and intelligence teams build a more complete picture. By expanding the range of information that can be examined, agencies can uncover additional insights while leveraging familiar Cellebrite workflows across emerging technologies.

Available Now

The Next Generation of the CFID: More Power in Your Hands. More Insights Within Reach.

The reimagined CFID delivers substantial hardware enhancements designed to improve field-based digital forensics. Increased processing power, expanded storage, live preview and analysis, improved battery capacity and support for simultaneous extractions help teams work more efficiently in time-sensitive environments. By enabling more analysis directly at the edge, CFID now helps organizations get real answers from data wherever it is needed most, without waiting on a lab.

Expected Delivery Q1 2027

VISIT INSEYETS PAGE →

Genesis

Deep Investigator: Find More Investigative Leads from More Application Data

Some of the most important evidence lives in places where standard processing does not fully reach yet, including new applications, niche platforms and databases with limited decoding support. Deep Investigator goes to the source, analyzing the raw SQLite databases behind applications to uncover additional investigative leads that might otherwise be missed. By automatically identifying relevant data sources and linking every finding back to the evidence, investigators can discover more connections, explore emerging applications and validate findings with confidence.

Available Now

Investigate More Evidence: Expand the Digital Evidence You Can Analyze

Genesis now supports additional evidence formats, including computer forensic images, email archives, business documents, calendars, contacts and email files. By bringing more evidence into a single AI-powered workflow, investigators can analyze information across devices, communications and documents, helping uncover connections faster and gain a more complete view of the investigation.

Available Now

Agentic Skills: Accelerate Common Investigative Tasks

Agentic Skills help investigators complete common investigative tasks faster by generating, structuring and executing multi-step workflows. These skills guide investigators through common objectives such as timeline development, communication analysis and case summarization. By reducing prompt engineering and manual effort, Agentic Skills help investigators achieve consistent, high-quality outcomes regardless of experience level.

Available November 2026

Investigate Your Way: Align Genesis to Agency Workflows

Agencies can customize Genesis with local terminology, report formats, investigative playbooks and reference materials. This helps investigators work within familiar processes while generating outputs that align with agency standards and requirements.

Available November 2026

CSAM Investigations Support: Accelerate the Identification of Relevant Evidence

Genesis will help investigators identify and analyze CSAM-related multimedia using AI-powered search, specialized review experiences and natural-language queries. By leveraging agency-provided knowledge files and reference materials, investigators will be able to quickly locate relevant content, uncover potential matches and focus on the evidence most critical to the investigation.

Available December 2026

CJIS Support: Bring AI-Powered Investigations to CJIS Environments

Genesis will help agencies use AI to analyze digital evidence while supporting their CJIS security requirements, bringing faster review and deeper insights to investigations involving sensitive criminal justice information.

Available End of 2026 or beginning of 2027

Analyze Your Data with Genesis, Offline

A planned on-premises deployment option will enable agencies to use Genesis entirely within their own environment. Teams can uncover what matters in complex digital evidence using AI-powered analysis while

maintaining control of their data, infrastructure and security requirements.
Available End of 2026 or beginning of 2027

VISIT GENESIS PAGE →

Corellium

Falcon Mirror: Bring Real-World Mobile Device Context into Your Research

Falcon Mirror Add-On bridges digital investigations and mobile security research by allowing supported Inseyets extractions of iOS devices to be imported into Falcon as a starting point for deeper introspection. Rather than rebuilding apps, configurations, data and user activity from scratch, researchers can begin with realistic device states that reflect actual usage. This expanded access to authentic device context helps security teams accelerate vulnerability research, malware analysis and advanced investigations while making expert workflows more efficient.
Available Now

AI-Powered Mobile Security Research and Pen Testing: Amplify with AI

Falcon and Viper AI-powered research and pen testing introduces a new foundation for applying AI across mobile research and security testing workflows. New releases include a powerful MCP server, Bring-your-own-AI flexibility, an Agentic Chat interface and pre-configured AI workflows that are designed to reduce manual complexity and accelerate your work. By combining physical AI access to virtual iOS and Android devices, research and development teams can create, test and validate software faster and simplify security and compliance processes.
Available November 2026

VISIT CORELLIUM PAGE →

Guardian

Connect the Evidence Ecosystem: Move Evidence across Trusted Systems

Connect Guardian to your existing archive and evidence storage systems, allowing agencies to maximize past investments without changing how they work. Guardian supports third-party evidence storage environments so agencies can archive, export and share evidence without disrupting workflows, while remaining the authoritative system of record for chain of custody and transfer log history. By eliminating manual downloads and re-uploads, investigators can move evidence more efficiently, reduce administrative burden and gain greater flexibility in how digital evidence is stored, managed and shared across partners.
Available Now

File System View: Navigate Evidence in Its Native Structure

Investigators reviewing evidence in Guardian Viewer no longer need to navigate individual views and artifacts to understand the broader context of the data. With the new File System View, users can now browse evidence through its native folder structure, making it easier to understand the full scope of collected evidence, quickly

locate relevant files and gain a more complete picture of the investigation.
Available October 2026

Enhanced Security: Control Every User Session

Enhanced Security introduces configurable session timeout controls that allow administrators to define how long users can remain inactive before being automatically logged out. This added flexibility helps organizations align access controls with internal security requirements and operational policies while reducing the risk of unauthorized access to sensitive evidence. By giving agencies greater control over access and session management, Guardian strengthens platform security without disrupting day-to-day investigative workflows.
Available November 2026

VISIT GUARDIAN PAGE →

Pathfinder

Investigate CDRs: Turn Telecom Records into Investigative Intelligence

AI-based CDR Normalization and Analysis brings telecom data into Pathfinder, eliminating the need to manually configure every provider format. Investigators and analysts can examine calls, messages, network activity and location context through the familiar Timeline, Map, Graph and Communications views, alongside their forensic data. By correlating identifiers such as IMSI, IMEI and MSISDN across sources and cases, Pathfinder broadens access to connected intelligence and helps teams establish relevance earlier.
Available December 2026

Find More Visual Evidence: Surface Critical Media with Greater Confidence

Media Analysis modernization expands Pathfinder's image and video classification with broader detection coverage, greater accuracy and faster, more reliable processing. More granular categories help investigators and analysts distinguish specific types of weapons, drugs and vehicles, while a new classification certainty filter gives users control over the level of trust applied to results. These enhancements make visual evidence more accessible, helping teams reduce missed evidence and focus their expertise on the media most relevant to the investigation.
Available December 2026

View the Whole Investigation: Bring Case Knowledge and Activity into Focus

The new Workspace in Pathfinder allows users to curate investigative knowledge of Case Subjects and their relationships, along with any insights and key evidence found — all to serve as persistent collaborative context for the investigation team. Workspace also showcases a new standard of reporting, with full flexibility of both content and structure. When a fully detailed export is required, Pathfinder now allows a revamped Excel report, suitable for both human readers and processing by downstream integrated third-party solutions.
Available December 2026

VISIT PATHFINDER PAGE →

Training and Services

Cellebrite Advanced Services (CAS) Labs Now Supports Drone Extractions

CAS is an extension of your forensics lab. Our experts work from secure labs worldwide, using the latest technology to access and extract data from locked mobile devices, computers and, now, drones. Our processes are forensically sound and backed by the research team that builds the methods. When a device stops your investigation, it doesn't have to stop your case.

Available Now

Refreshed CCO + CCPA Training for Inseyets

The updated Cellebrite Certified Operator for Inseyets (CCO) and Cellebrite Certified Physical Analyst for Inseyets (CCPA) courses provide hands-on training aligned to the latest version of Cellebrite Inseyets. CCO develops skills in mobile device extraction and Inseyets UFED workflows, while CCPA advances evidence analysis skills using Inseyets Physical Analyzer, helping examiners build proficiency with current Cellebrite capabilities across the digital forensics workflow.

Available November 2026

New Defense and Intelligence Training Courses: CIET D&I, CEDI and CADI

These three purpose-built courses support different roles in the intelligence workflow. Cellebrite Inseyets Essentials for D&I (CIET D&I) establishes foundational Inseyets skills across extraction, analysis and reporting; Cellebrite Extractions for Defense and Intelligence (CEDI) develops operational skills for device collection, extraction and exploitation; and Cellebrite Analysis for Defense and Intelligence (CADI) builds analytical skills

VISIT TRAINING PAGE →

NEXT STEP

Explore the Autumn 2026 Release →