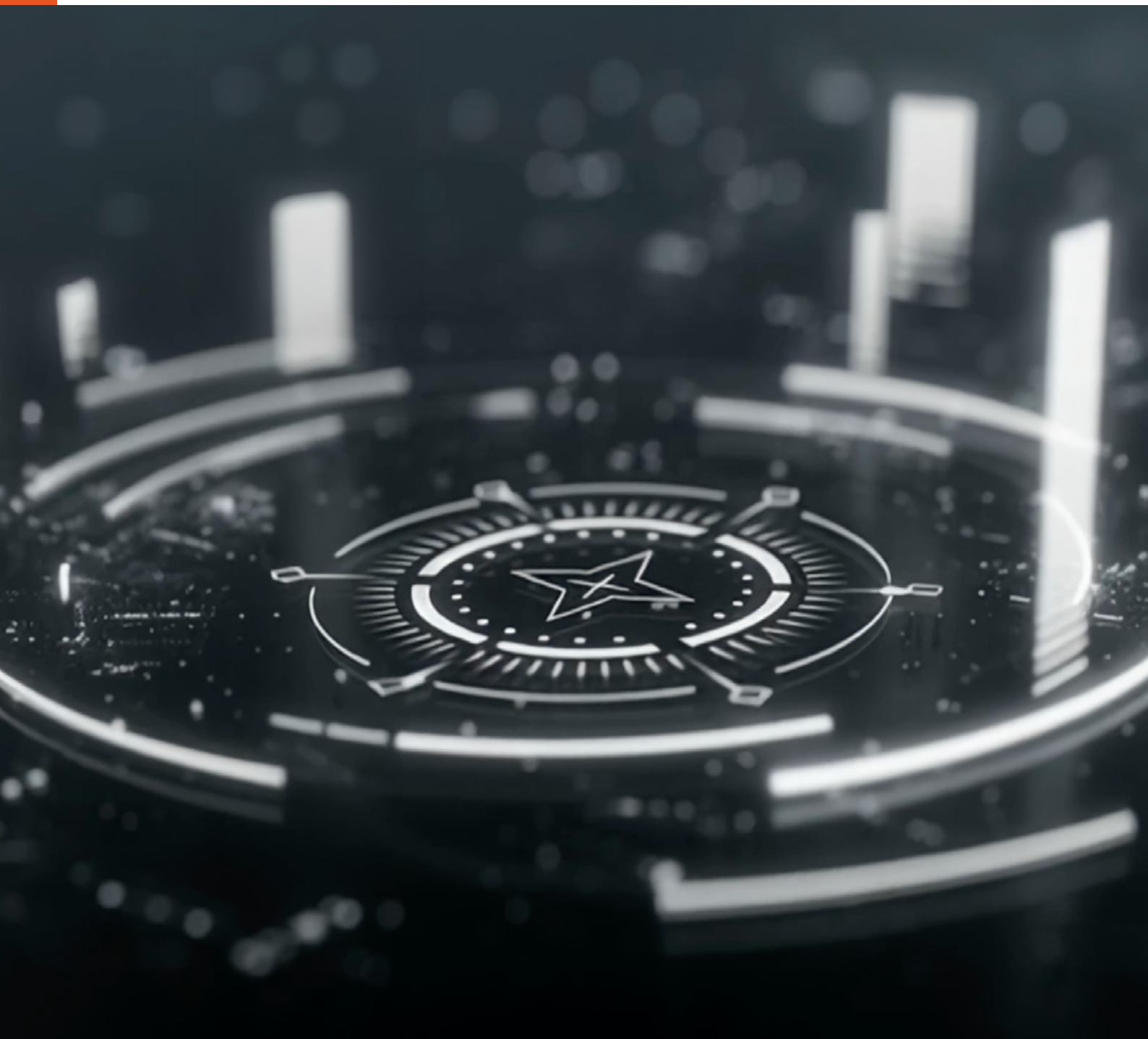
Cellebrite

The Ultimate Buyer's Guide for Law Enforcement Leaders

Navigating The AI Technology Landscape



How to Use This Guide

This guide is designed for leaders and decision-makers across law enforcement and government agencies. It provides a practical framework for evaluating digital investigation technologies, including AI-enabled capabilities, with a focus on security, transparency, human oversight and regulatory awareness.

AI-related capabilities described in this guide are intended to assist law enforcement and government agencies by accelerating review, prioritization and organization of digital evidence. All outputs generated by AI systems must be reviewed, validated and interpreted by qualified users before any investigative or evidentiary reliance.

CHAPTER 1

SaaS / Cloud Deployment Options

Public safety and law enforcement agencies face unprecedented challenges due to the rapid growth of digital evidence. Mobile devices, cloud applications, encrypted communications, social media and IoT data generate terabytes of evidence in nearly every case. Managing this digital overload while maintaining evidence integrity and compliance with data protection standards is a top concern for public sector leaders. Traditional manual review of digital evidence on USBs or portable hard drives is no longer sufficient.

AI-powered investigation technology addresses these challenges by accelerating insight discovery, automating repetitive review tasks and helping investigators identify critical connections more quickly and accurately.

You need to consider a provider with infrastructure supports cloud-native, hybrid and air-gapped deployments, enabling secure delivery of digital investigation tools across diverse environments with tenant data segregation, isolated processing environments and real-time platform status reporting.

For decision makers, the choice between deployment models must balance scalability, security and compliance. Cloud deployments accelerate onboarding and expansion but require strict governance and transparency. Hybrid and air-gapped options may be necessary for sensitive data or regulatory requirements.

SaaS / Cloud Deployment

- Built-in Infrastructure: No need for local servers; hosting and maintenance handled by the provider.
- Scalability: Easily scale up or down to meet demand without hardware limitations.
- Always Current: All users stay on the latest version with automatic updates and premium capabilities.
- High Availability: Typically offers 99.95% uptime and robust disaster recovery.

On-Premise

- Air-Gapped Security: Ideal for agencies requiring complete isolation from external networks.
- Full Control: Direct oversight of hardware, data and security configurations.
- Custom Integrations: Easier to tailor systems to unique workflows without vendor constraints.
- Predictable Costs: One-time capital expenditure vs. ongoing subscription fees

TIP

Choose platforms that support secure, compliant and flexible deployment models to meet operational and regulatory needs.

CHAPTER 2

Security Protocols

Security and privacy are foundational to digital investigations. Cellebrite implements industry-recognized security measures, including encryption at rest and in transit, access controls, audit logging and continuous monitoring.

Security certifications (such as SOC 2 Type II) and alignment with recognized frameworks (e.g., ISO 27001 and 27017, GDPR compliance, UK Cloud Security Principles) support organizational risk management efforts.

Agencies are responsible for conducting their own security assessments and ensuring compliance with internal and external requirements.

AI-enabled processing occurs within the Cellebrite environment configured by the customer and is subject to the same security controls as other platform functionality.

CHAPTER 3

AI in Law Enforcement – Responsible Use

Key AI Terms Explained

The following terms are commonly used in discussions about modern investigative technologies. Understanding their scope and limitations is essential for informed evaluation and responsible use.

→ Artificial Intelligence (AI)

A broad term referring to computer systems designed to perform tasks that typically require human intelligence, such as pattern recognition, language processing and data analysis. In investigative tools, AI is used to assist with organizing, searching and prioritizing information, not to make legal or investigative decisions.

→ Machine Learning (ML)

A subset of AI in which systems learn statistical patterns from data to improve performance on specific tasks, such as classification or prediction. ML-based tools support investigators by identifying patterns or similarities in large datasets, while outputs must always be reviewed and validated by users.

→ Generative AI (GenAI)

AI systems capable of generating new contents such as text summaries or responses, based on patterns learned during training. In law enforcement tools, generative AI may assist with summarization or information retrieval, yet it may omit details or introduce inaccuracies. GenAI cannot replace the human review of original source materials.

→ Deep Learning (DL)

An advanced form of machine learning that uses multi-layered neural networks to process complex data such as images, audio or text. In investigative contexts, deep learning may support tasks like image grouping or speech-to-text conversion, without determining meaning, intent, or legality.

→ Large Language Models (LLMs)

A category of generative AI models trained on large volumes of text to understand and produce human-like language. LLMs can support functions such as search, summarization or question-and-answer interfaces within investigative platforms, while requiring careful oversight due to their probabilistic nature.

→ Agentic AI

A term used to describe AI systems designed to act autonomously toward predefined goals, including planning or executing multi-step actions.

AI Use in Investigations

AI-enabled features may assist with tasks such as content grouping, summarization, timeline organization and search prioritization. These capabilities are designed to improve efficiency and investigator well-being while preserving transparency and control.

Important:

- AI outputs may be incomplete or contain errors
- Original source material must always be reviewed
- Investigative conclusions remain the responsibility of the user

Sensitive Content

AI-assisted classification tools may help prioritize review of large datasets and reduce unnecessary exposure to harmful material. These tools do not confirm the legality, context or evidentiary value of content and must be used in accordance with applicable law and agency policy.

AI-powered solutions in digital investigations use machine learning, pattern recognition and natural language understanding to assist human decision-making. These tools do not replace investigators but strengthen and accelerate their work through assisted review, prioritization and context discovery. Key applications include entity extraction, assisted review, content recognition, relationship mapping and automated summarization.

Cellebrite integrates AI and advanced analytics across its portfolio to accelerate investigations, improve accuracy and boost efficiency, while ensuring human judgment and evidentiary integrity remain central. Products like Inseyets, Pathfinder, Guardian, Inspector and Autonomy offer capabilities such as visual intelligence, relationship mapping, evidence organization and workflow orchestration.

Cellebrite + AI to Accelerate Evidence Review

Detecting and Prioritizing CSAM (Child Sexual Abuse Material)

Cellebrite leverages AI-powered image and language classification to help investigators sift through thousands of hours of digital content—including photos, videos and chat logs—to identify potential CSAM quickly.

- AI automates categorization and flags high-risk content, reducing manual review time and investigator exposure to harmful material.
- This approach accelerates case resolution and supports trauma-informed workflows for law enforcement.

TIP

Implement AI responsibly with transparency, bias mitigation and human oversight.

CHAPTER 4

Value Drivers

Why Agencies Are Turning to AI-Powered Investigation Tools Managing Growing Data Volumes

The amount of digital evidence per case continues to increase. AI helps agencies process and analyze vast datasets quickly without sacrificing accuracy.

Uncovering Hidden Connections

AI-powered analytics identify links, behaviors and relationships across devices and information that may otherwise remain undiscovered. manual workload, allowing investigators to focus on interpretation, judgment and reporting.

Accelerating Case Resolution

Automated triage and assisted review reduce manual workload, allowing investigators to focus on interpretation, judgment and reporting.

Strengthening Evidence Integrity

Automated processes minimize human error and maintain consistent documentation, ensuring findings remain defensible in court.

Supporting Investigator Wellbeing

AI helps protect investigators from repeated exposure to distressing material by flagging and categorizing sensitive content.

Before AI:
Cellebrite leverages AI-powered image and language classification to help investigators sift through thousands of hours of digital content—including photos, videos and chat logs—to identify potential CSAM quickly.

With AI:
Automated normalization and correlation reduce this process to minutes or a few hours, enabling investigators to quickly integrate CDR data into timelines and link analysis. Results can be validated through full transparency—investigators can review the normalized records, see original source fields and verify how each data point was standardized and linked. This visibility ensures confidence in the process and supports defensible outcomes.

Impact:

What once delayed case progression for nearly a week now happens almost instantly, accelerating lead generation and case resolution.

CHAPTER 5

10 Questions to Ask Your Vendor

Decision makers must ask critical questions about transparency, compliance, interoperability and governance. Key areas include bias mitigation, certifications, integration capabilities and incident response.

Essential questions include:

1. How do you ensure transparency and explainability in your AI models?
2. How are your AI models trained and what steps do you take to mitigate bias?
3. What models do you use and do they learn on customer data?
4. Do you share any data with external or open AI providers?
5. Are your AI models developed in-house, based on open-source, or through third-party vendors?
6. Can your AI system ingest and integrate data from platforms like RMS and CAD?
7. What governance structures and oversight processes are in place for responsible AI use?
8. What governance structures and oversight processes are in place for responsible AI use?
9. What is your roadmap for integrating AI responsibly into investigative workflows?
10. How do you support training and adoption for law enforcement users to maximize AI benefits?

CHAPTER 6

Procurement Considerations

AI regulation is evolving worldwide and each jurisdiction defines AI differently. Agencies should focus on capabilities, accountability and transparency rather than labels. Key recommendations include understanding local frameworks, evaluating transparency and oversight, engaging compliance teams early and applying principles of fairness, reliability and human oversight.

Procurement best practices involve defining operational outcomes and measurable goals, setting evaluation metrics, requesting benchmark results, ensuring transparency and oversight, piloting solutions before deployment and assessing usability. An evaluation checklist should cover transparency, accuracy, security, privacy and compliance, oversight and support and training.

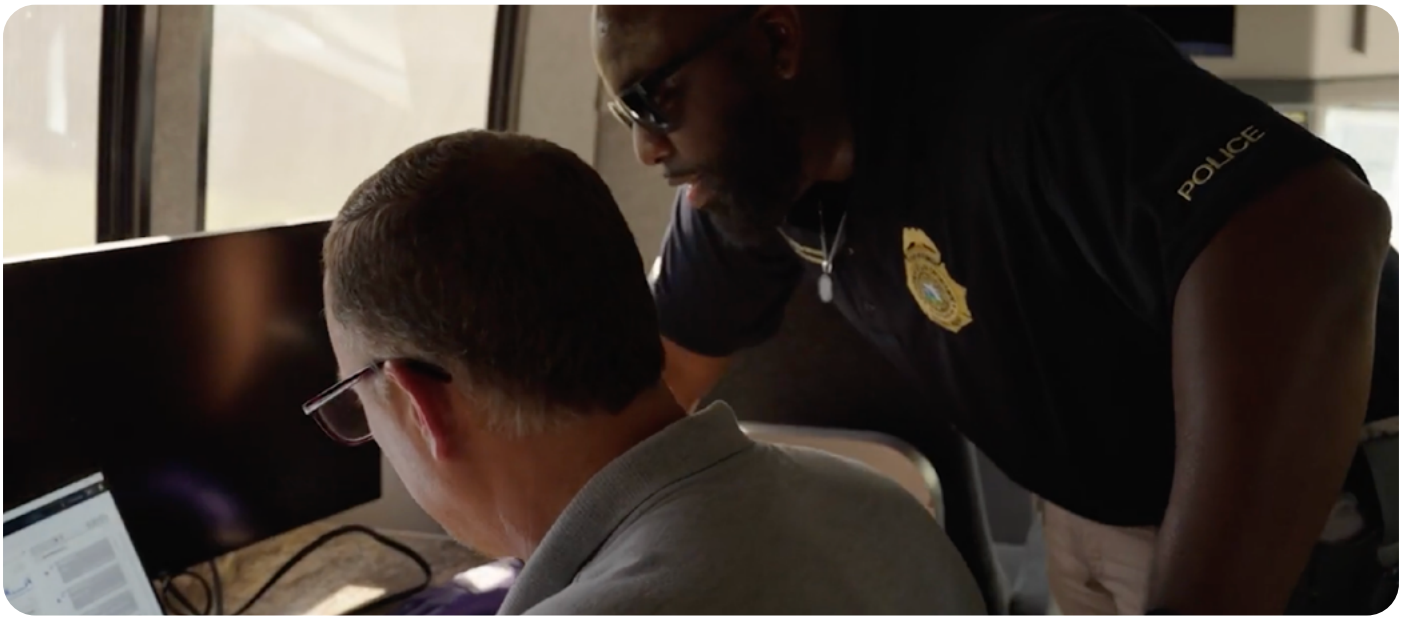
Decision makers must ensure technology investments deliver secure and ethical outcomes, align with global standards and adapt to diverse regulatory environments.

TIP

Apply best practices to ensure technology investments deliver secure and ethical outcomes.

Conclusion

AI-enabled investigative tools can deliver significant efficiency gains when implemented responsibly. Success depends on clear governance, transparency, training and human oversight. Agencies should evaluate technologies carefully and deploy them in a manner consistent with applicable laws, policies and operational requirements.



Legal & Compliance Notice

This document is provided for informational purposes only and is not intended to constitute legal advice, regulatory guidance, or representations regarding legal compliance. Decisions regarding the use, configuration, and reliance on AI-enabled tools remain the sole responsibility of the Customer and must be made in accordance with applicable laws, internal policies, and operational requirements. Cellebrite products incorporate AI-enabled features solely as investigative support and efficiency tools. They are not designed to make investigative determinations, legal conclusions, or evidentiary findings, and they do not replace professional judgment or human review.

About Cellebrite

Cellebrite's (Nasdaq: CLBT) mission is to enable its customers to protect and save lives, accelerate justice and preserve privacy in communities around the world. We are a global leader in Digital Investigative solutions for the public and private sectors, empowering organizations in mastering the complexities of legally sanctioned digital investigations by streamlining intelligence and investigative processes. Trusted by thousands of leading agencies and companies worldwide, Cellebrite's Digital Investigative platform and solutions transform how customers collect, review, analyze and manage data in legally sanctioned investigations.

LEARN MORE:

WWW.CELLEBRITE.COM | WWW.CELLEBRITE.COM/EN/BLOG | WWW.CELLEBRITE.COM/EN/NEWSROOM