Cellebrite
ENTERPRISE SOLUTIONS

2026 Industry Trends in the Private Sector

Building Resilience through Intelligence, Prevention and Response

Executive Summary

Digital evidence is now an essential part of how private-sector organizations manage risk, ensure compliance and maintain business continuity. In nearly every investigation—whether it involves data theft, insider misconduct or eDiscovery—digital information forms the backbone of fact-finding and decision-making.

This shift reflects the reality that modern business happens across multiple apps. Communications, transactions and processes are recorded across mobile devices, cloud platforms and enterprise systems. As this digital footprint grows, so does the complexity of managing, protecting and analyzing it.

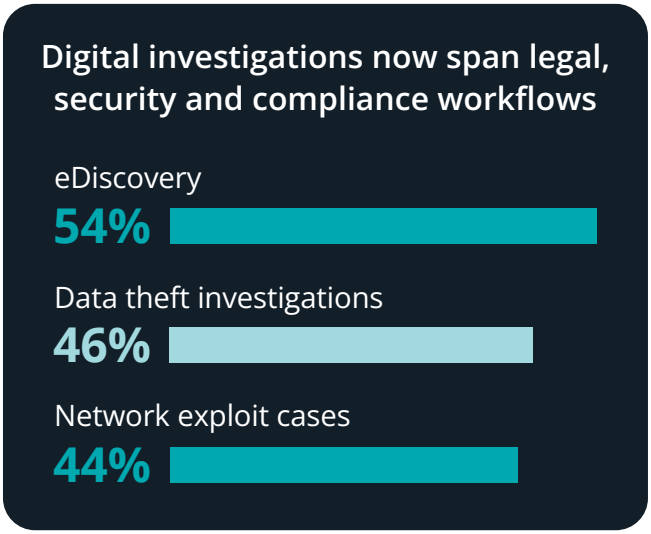
Cellebrite's 2026 Industry Trends in the Private Sector report examines how companies, law firms and forensic service providers are adapting to these demands. Based on input from 276 professionals across 52 countries, it explores how organizations are using digital investigations to strengthen prevention, improve responsiveness and build long-term resilience.

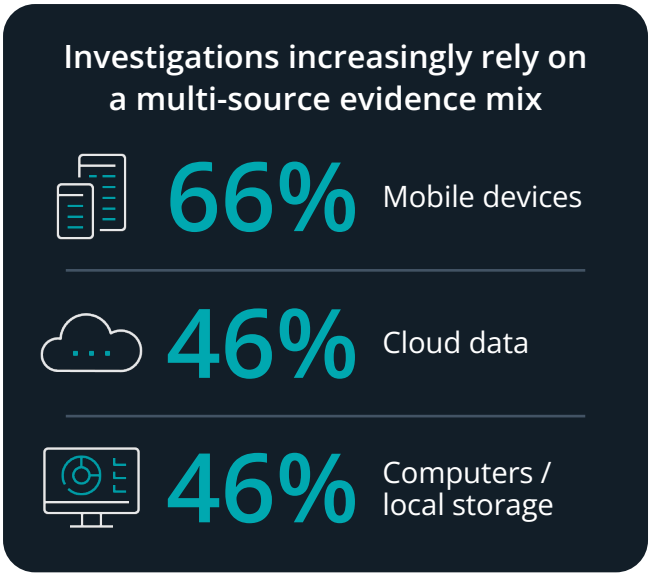
The results paint a clear picture: the private sector is entering a new phase of digital maturity—where intelligence, collaboration and readiness define operational strength.

This report shares insights from professionals in the private sector, including small businesses, large corporations, service providers and law firms. Together, their answers show how digital investigations are changing and how using data smarter can help organizations prevent problems, recover faster and stay more resilient.

Key Findings

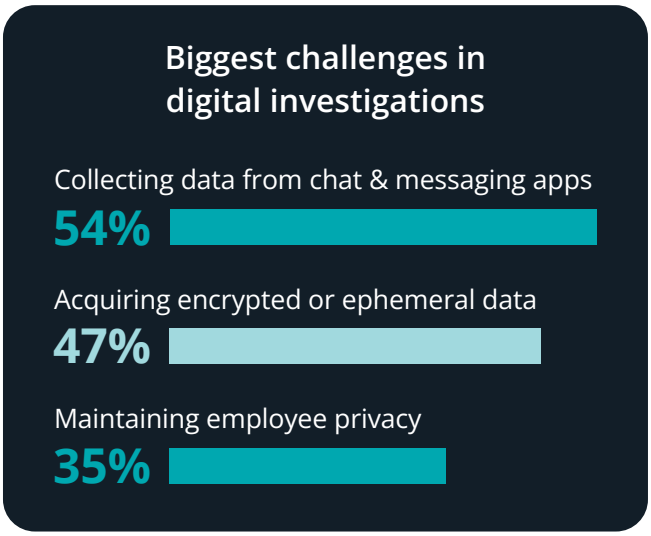
Digital investigations now support multiple areas of business.
eDiscovery remains the most important use case (54%), followed again by data theft investigations (46%) and network exploit cases (44%), reflecting how organizations integrate digital evidence across compliance, cybersecurity and legal workflows.





Mobile, cloud and local data form the core of modern investigations.
Digital evidence comes from a broad mix of sources, with mobile devices contributing an average of 66% of cases (6-point increase from 2024), and both cloud-based and computer or local storage sources each appearing in 46% of investigations.

Persistent challenges center on data collection and privacy.
The top obstacles include collecting from chat and messaging apps (54%), acquiring encrypted data (47%) and protecting employee privacy during mobile data collection (35%).



Key Findings

AI Moves from Vision to Investigative Impact.
In 2025, enterprises expressed strong intent to use AI to enhance data analysis and uncover patterns more efficiently (69%), signaling broad expectations for AI-powered investigative acceleration. By 2026, respondents identified specific, high-impact use cases, led by analyzing communications to find links between people (57%), demonstrating a shift from aspirational AI adoption to practical, investigator-centric capabilities that deliver immediate operational value.

Organizations are becoming proactive about digital resilience.
By turning investigative insights into preventive measures—testing systems, validating controls and monitoring risks—companies are embedding resilience into everyday operations.

Methodology

This survey includes responses from 276 enterprise professionals across 52 countries working in digital forensics, IT, compliance, legal and related roles within the private sector. Respondents represent a wide range of organization types and sizes, including service providers as well as small, medium and large enterprises.

Participants support enterprise-focused use cases such as internal investigations, eDiscovery, data theft response and compliance-driven inquiries. The survey questions capture shared challenges, priorities and practices across teams responsible for managing and analyzing digital evidence in corporate environments.

Respondents by Region

42% North America

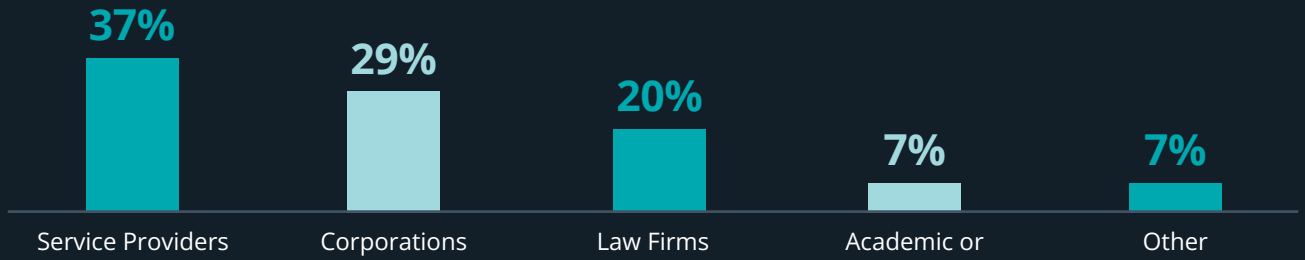
15% Latin America

28% Europe, Middle East, Africa

15% Asia-Pacific

Respondents by Company Size

Respondents by Organization Type



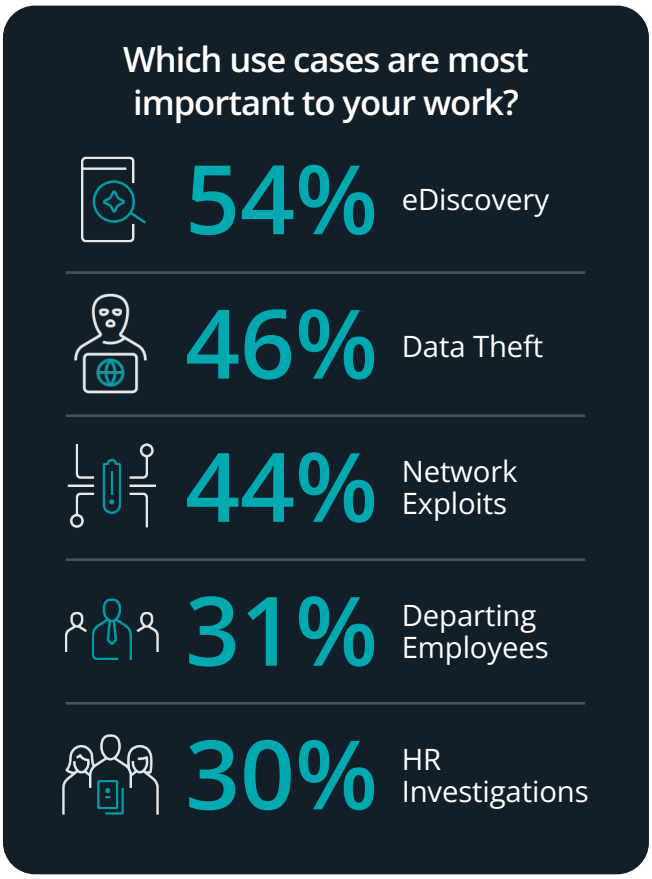
The Expanding Role of Digital Investigations

Digital investigations now support a wide range of business functions—from compliance and cybersecurity to legal discovery and internal reviews.

These figures reflect the diverse ways organizations are applying digital forensics to protect information, manage risk and ensure compliance. When asked which investigations are **most important to their own work**, respondents cited:

- **eDiscovery for preservation, collection and recovery (54%)**
- **Investigating potential data theft (46%)**
- **Identifying, mitigating and investigating network exploits (44%)**

Together, these findings show how digital forensics has evolved from a specialized technical practice into a shared discipline. Data collected from devices and systems now supports legal, security, IT and business teams alike, helping organizations make informed decisions that strengthen overall resilience.



Managing Evidence at Scale

On average, respondents report conducting about **four to six mobile device examinations per month**, along with a similar number of computer and local storage examinations. The challenge isn't only the growing volume of data—it's the increasing complexity of sources and the need to ensure every step remains defensible and compliant.

Collaboration among **legal, IT and forensic** functions helps mitigate this strain, as does strategic outsourcing to **forensic service providers**, who extend capacity and support specialized or high-volume cases.

This collaborative model allows organizations to maintain speed without compromising the integrity of evidence or the security of sensitive data.

Prevention and Readiness

The private sector continues to demonstrate a strong, proactive approach to risk management. Investigations focused on **data theft (46%)** and **network exploit cases (44%)** show that companies are responding to incidents while also identifying and fixing vulnerabilities before they cause damage.

This approach turns lessons learned from past incidents into prevention strategies. By testing systems, validating access controls and monitoring potential points of failure, organizations are making digital resilience part of their daily operations.

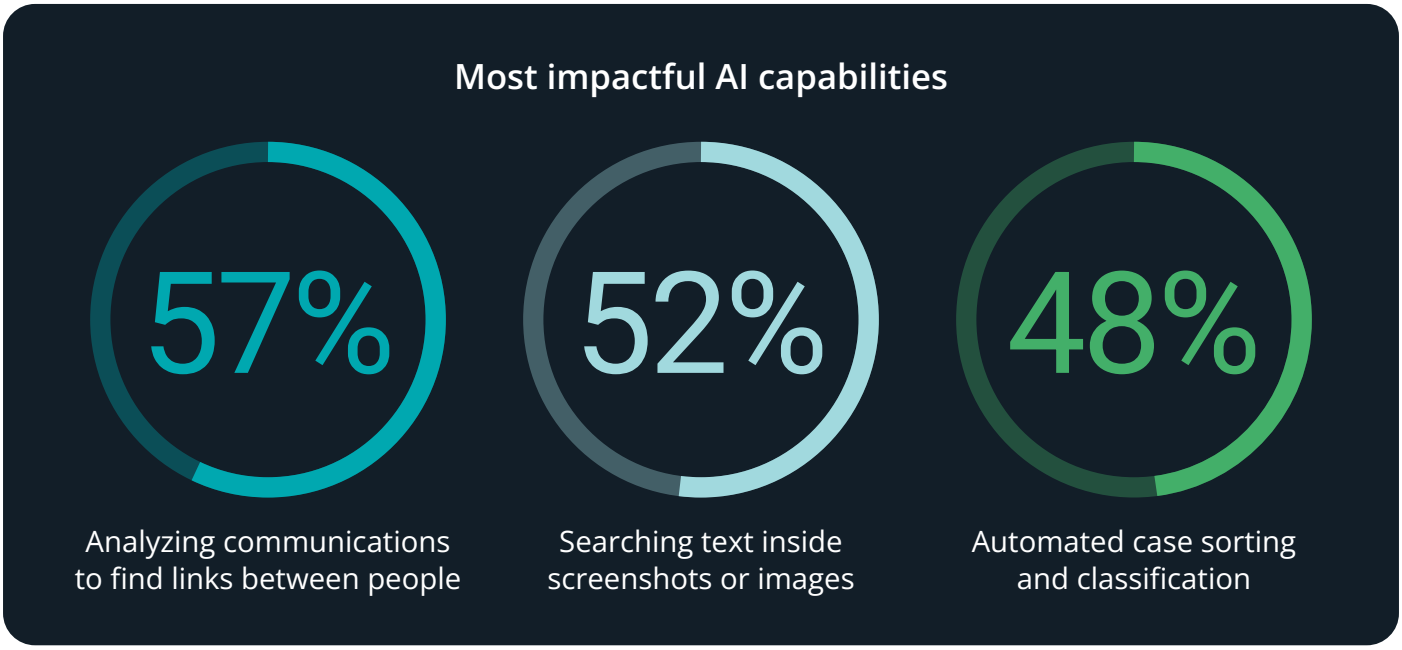
AI in Everyday Investigations

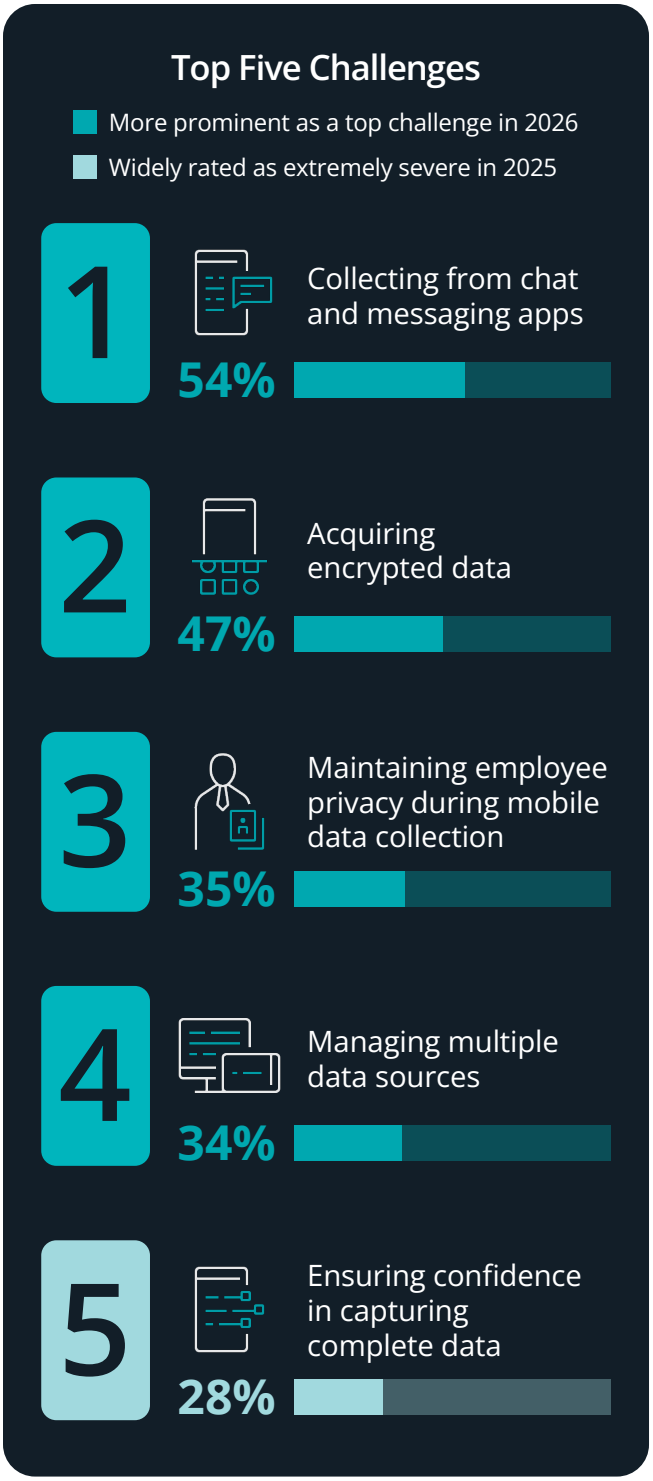
Artificial intelligence (AI) is now part of the investigative toolkit. It is viewed as a practical way to speed up analysis and help teams manage large amounts of data.

Respondents ranked the following AI capabilities as the most impactful:

- **Analyzing communications to find links between people (57%)**
- **Searching text inside screenshots or images (52%)**
- **Automated case sorting and classification (48%)**

AI helps investigators find relevant information faster and improve consistency across reviews. It supports efficiency, yet human expertise continues to drive interpretation and final decision-making. The data shows that AI is a helpful partner, not a replacement for professionals.





Ongoing Challenges

As organizations expand their use of digital evidence and integrate AI into investigative workflows, several obstacles continue to slow progress.

Several of these challenges were already rated as extremely severe in 2025. These findings reveal that the hardest part of digital investigations is achieving both thoroughness and compliance. The growing layers of data security, privacy regulation and encryption mean teams must navigate carefully—protecting information integrity while preserving trust.

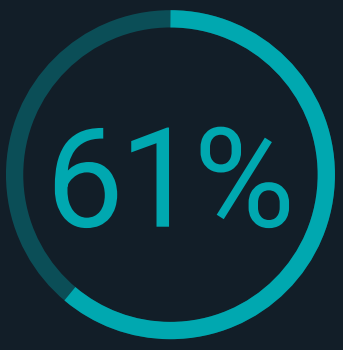
Cloud and Data Storage

While most organizations (61%) store digital evidence on internal servers, 36% said their organizations are receptive or very receptive to using cloud-based solutions.

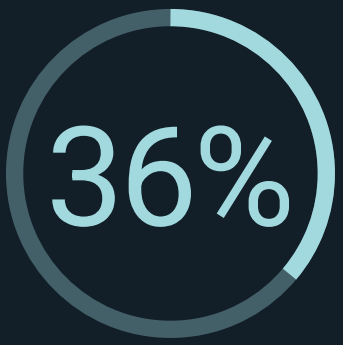
As teams manage growing data volumes from multiple sources and increasingly operate across distributed environments, many see the need for secure, scalable ways to share and access evidence. Respondents indicated that broader adoption will depend on:

- **Data stored within the organization's own country (51%)**
- **Stronger cloud security controls (50%)**

The results suggest that **confidence in vendor security and compliance standards** will shape future decisions about cloud-based evidence management.

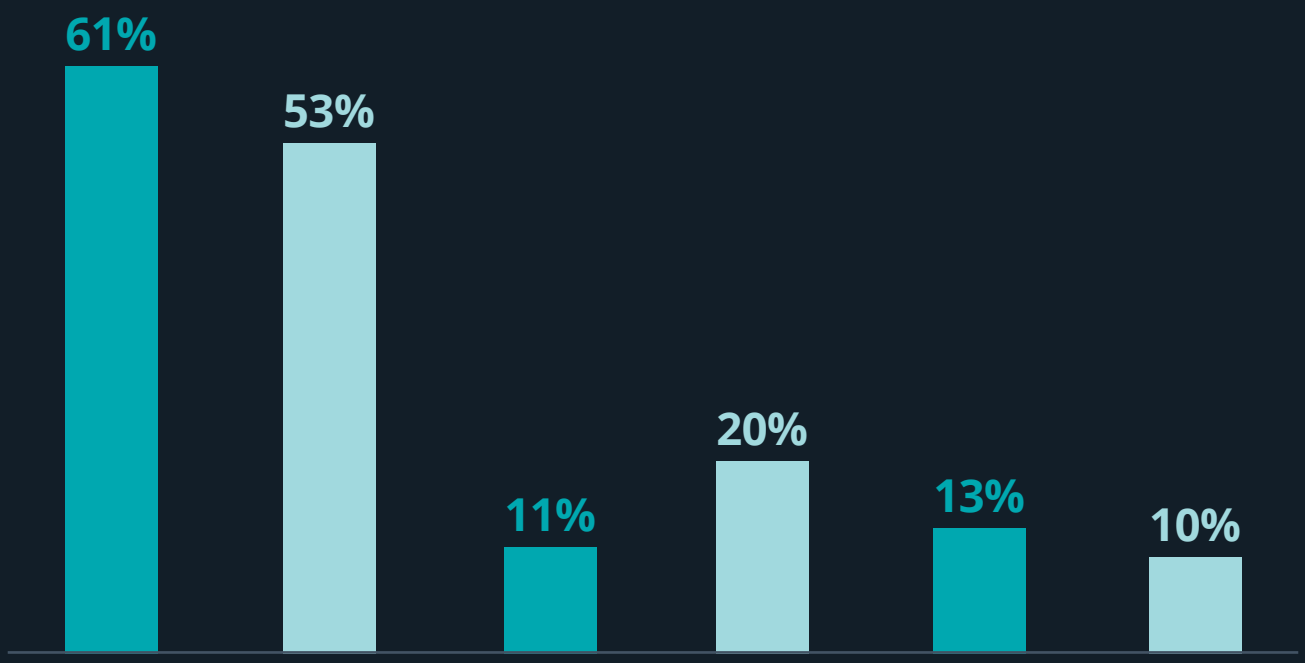


Organizations that store digital evidence on internal servers



Organizations that are receptive or very receptive to using cloud-based solutions

Respondents by Organization Type



Looking Ahead

The private sector is steadily integrating digital investigations into everyday business operations. With devices everywhere and apps introducing new risks, digital data is becoming part of every department's work.

Organizations are increasingly using digital data to:

- **Enable HR and Legal teams to close matters quickly with timely, relevant data**
- **Reduce vulnerabilities and overall risk exposure**
- **Safeguard intellectual property and sensitive data**
- **Improve efficiency and accuracy in incident investigations**
- **Use investigative insights to improve governance and strategic decision-making**

This workflow shift means digital forensics will serve not only to respond to problems, but to prevent them—transforming investigations into intelligence and resilience.

Conclusion

The 2026 Industry Trends in the Private Sector report shows an industry adapting to rising data demands and higher expectations. Across corporations, law firms and forensic providers, one idea stands out: **resilience through intelligence, prevention and response**

Teams that can collect, manage and use digital evidence efficiently will be better equipped to reduce risks, protect their organization and clients and maintain trust. Digital forensics and investigations are no longer only about finding answers after the fact—it is about creating systems that keep businesses secure, responsive and ready for what comes next.

Cellebrite
ENTERPRISE SOLUTIONS

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

CONNECT WITH US:

@CELLEBRITE