carahsoft

Cellebrite

2026 Industry Trends

The State of Digital Investigations in Public Safety

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, NASPO ValuePoint and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Cellebrite, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/CellebriteResources

Join Events & Webinars:
carah.io/CellebriteEvents

Discover Technology Solutions:
carah.io/CellebriteOverview

Learn About Procurement:
carah.io/CellebriteContracts

Connect With Our Team:
Cellebrite@carahsoft.com
(888) 823-5278

Cellebrite

2026 Industry Trends

From Access to Insight:
Modernizing Digital Investigations

Executive Summary

Digital evidence lies at the heart of modern investigations and intelligence gathering. Data from devices helps power the investigative and judicial lifecycle, from initial investigation to charging, plea negotiations and court.

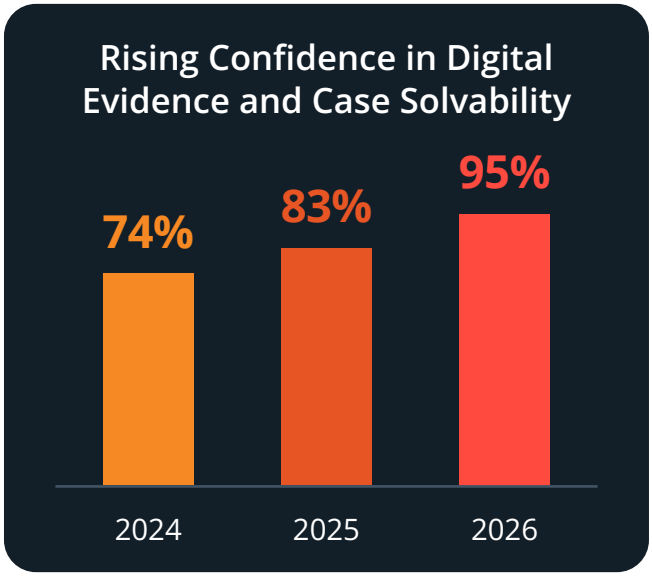
In today's cases, digital evidence is common and often essential. It helps establish facts, timelines and sometimes, intent, in ways traditional evidence cannot. As a result, the public, judges and juries expect public safety agencies to use digital evidence and to do so responsibly and transparently. Agencies are increasingly responding by shifting resources and updating how they work to strengthen their digital investigation capabilities.

As agencies increasingly rely on data, they also wrestle with ballooning data volumes and vastly increased complexity. Cases increasingly involve multiple devices and additional digital sources. This is creating overload for investigators, examiners and analysts as they strive to connect data across sources and deliver accurate and defensible evidence that supports timely and fair judicial outcomes.

Cellebrite's 7th Annual Industry Trends Survey (2026) explores the challenges agencies face in managing digital evidence and the factors shaping their investigative priorities. It captures diverse insights across the global public safety and judicial ecosystem, reflecting the experiences of examiners, investigators, analysts, lab managers, prosecutors and agency leaders. The results provide meaningful and practical information that deliver a clear message: we are firmly in the era of digital evidence, but significant modernization is needed to rise to the challenges of a digital-first landscape.

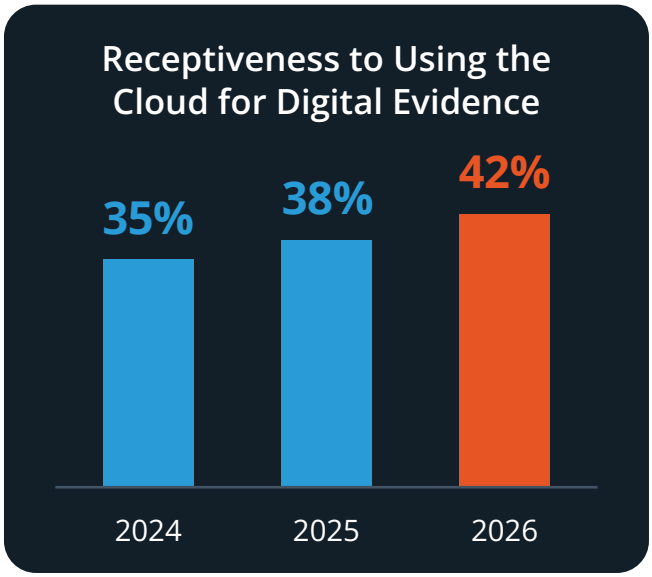
Key Findings

Digital evidence is now central to nearly every case.
Its impact on case outcomes is at an all-time high with 95% of survey respondents agreeing it significantly increases case solvability — up from 74% in 2024 and 83% in 2025.



Agencies are actively shifting their focus to digital investigations.
62% are reallocating resources to bolster digital investigations, and half of agency managers describe digital investigations as a strong or strategic budget priority.

Agencies are becoming more open to using the cloud for digital evidence.
Receptiveness increased from 38% in 2025 to 42% in 2026, showing a steady shift toward cloud-based management, sharing, and storage of digital evidence.



Key Findings

Public confidence depends on agencies' digital investigative capabilities.
97% of respondents say their community expects digital evidence to be used in nearly every case.

Increasing workloads and complexity are seriously straining investigative capacity.
94% of respondents say digital evidence has become more complex, adding pressure to already heavy caseloads. Examiners most often cite accessing locked iOS devices as a challenge, while 68% of investigators say the time required to review digital data is the biggest barrier to moving cases forward.

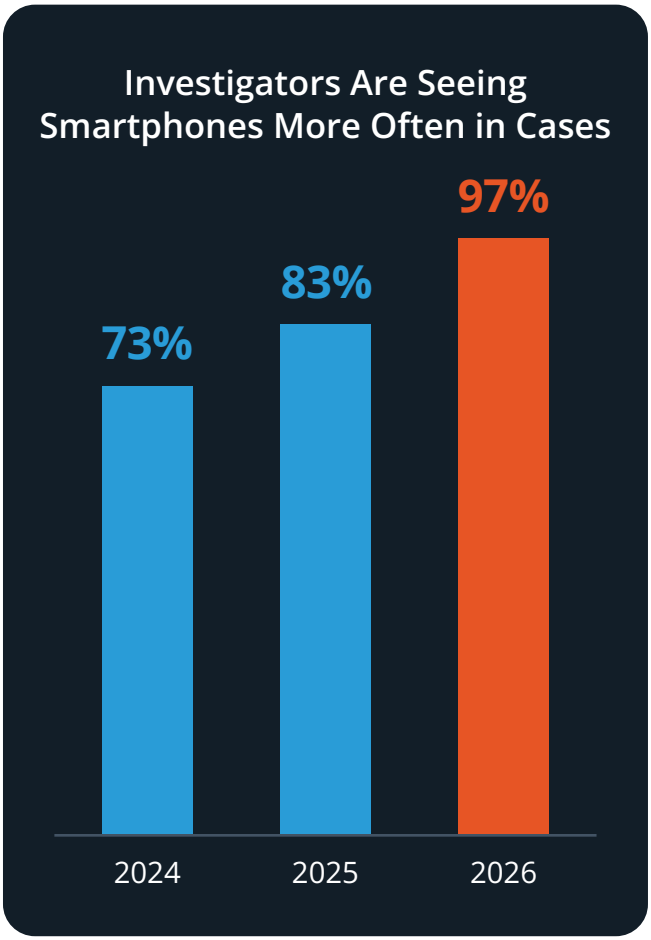
Smartphones are involved in nearly every investigation.
97% of Investigators say that smartphones are a frequent source of evidence, up from 73% in 2024. A typical investigation involves 2 to 5 devices, making them ubiquitous digital witnesses to potential criminal behavior.

97%

say digital evidence is expected to be used in nearly every case

94%

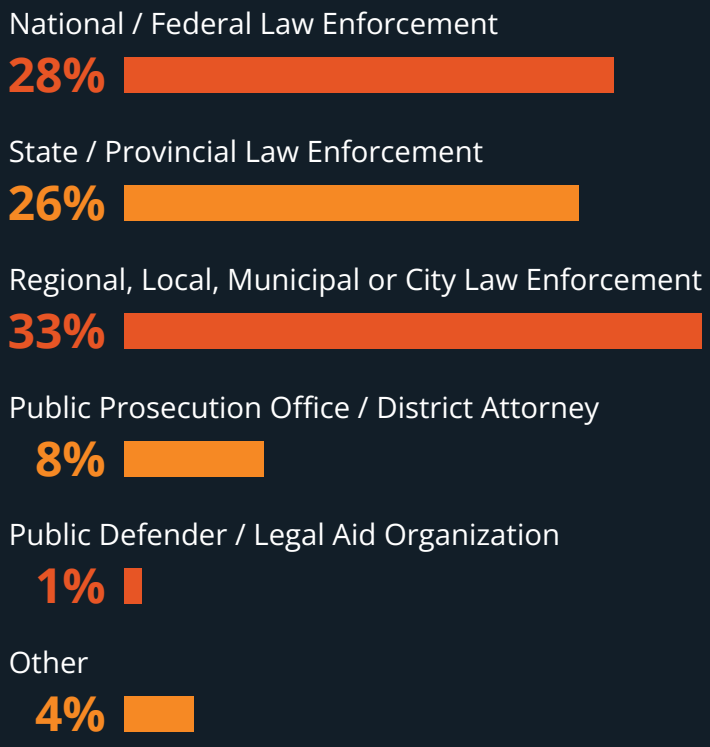
of respondents say that the complexity of digital evidence has increased



Respondents by Region

38%	17%	27%	19%
North America	Latin America	Europe, Middle East, Africa	Asia-Pacific

Respondents by Current Professional Role



Methodology

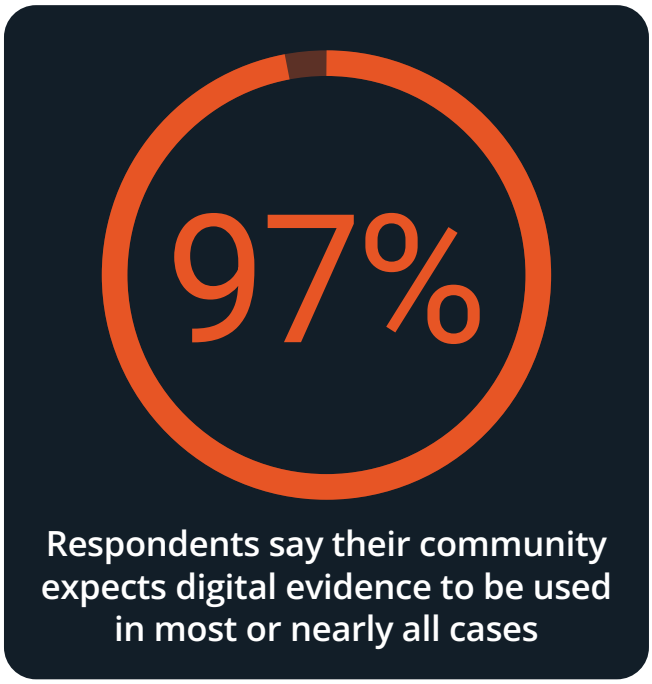
This survey includes responses from more than 900 public safety professionals from 63 countries. Participants represent a broad range of regions and agency types, including local, state, national and federal law enforcement, as well as prosecutors' offices, public defenders and related public safety organizations.

Respondents span key roles involved in digital investigations, including examiners, investigators, analysts, lab managers, prosecutors and agency leaders. The survey combined general questions with role-specific questions to ensure the findings reflect both shared challenges and the realities of day-to-day work across the investigative and judicial process.

Digital Evidence is the Backbone of Criminal Justice

Digital evidence is now a central component of the criminal justice system. Traditional types of evidence, such as eyewitness testimony and physical exhibits, still play a crucial role, yet the ubiquitous nature of digital evidence means the justice system has come to rely on it. In our survey, 93% of respondents say digital evidence is critical in key justice system decisions, including arrests, charging, pleas and trials.

This mirrors the central role digital technology plays in everyday life. It records where we are, with whom we communicate, our actions, our views and opinions, our financial transactions and much more. It isn't merely convenient—it's virtually inescapable. That's why digital evidence is so valuable in investigations: it shows a pattern of life and reveals connections between individuals that may be otherwise unseen. Because it is a uniquely unbiased witness, it has become the primary factor in how cases are built, decisions are made and justice is delivered.



Today's Investigations Demand Digital Evidence

Public safety agencies are reshaping how they conduct criminal investigations. This isn't simply a shift in preference—the overriding assumption is that digital evidence will be used, with 97% of survey respondents saying their community expects it to be used in most or nearly all cases.

Driving Structural Change in Investigations

Many public safety agencies are now turning this expectation into practice. **More than 60% are reallocating resources to bolster digital investigations**, placing increasing emphasis on acquiring and analyzing digital evidence. This shifting focus is echoed in funding priorities, with at least half of agency managers describing digital investigations as a strong or strategic budget priority. We expect this trend to continue growing, as agencies work to close the gap between expectations and practice by making digital investigation the default operational model.

The Expanding Evidence Landscape

The smartphone is at the center of the digital evidence universe, **with 97% of investigators** reporting that smartphones appear frequently in their cases. That's up significantly, from 73% in 2024, demonstrating the important role these devices play in the evidence landscape.

It's No Longer About a Single Device or Source

Investigations today rarely depend on a single source of digital evidence. Our survey reveals agencies continue to encounter **2 to 5 devices per case** and include other sources such as call detail records, video surveillance systems and more.

Diverse Evidence Sources Multiply Challenges

This expansion increases the amount of data to review and the need to connect information across sources. In fact, the survey reveals the **single biggest challenge (68%) investigators face is the time it takes to review digital data**. In part, this is about increased data volumes, but it's also about correlating evidence from multiple devices and sources.

To create a holistic view of evidence, it's critical to connect the dots across sources, but when done manually, this can be an extremely time-consuming activity. These connections can extend across multiple devices, communications channels, data platforms and agencies, making correlation difficult. Working against the clock also increases the risk of missing critical connections, leading to weaker investigations.

Key Challenges That Slow Down Investigations

Our survey identified several other key issues and bottlenecks that make digital investigations both challenging and time-consuming. These include:

Locked devices

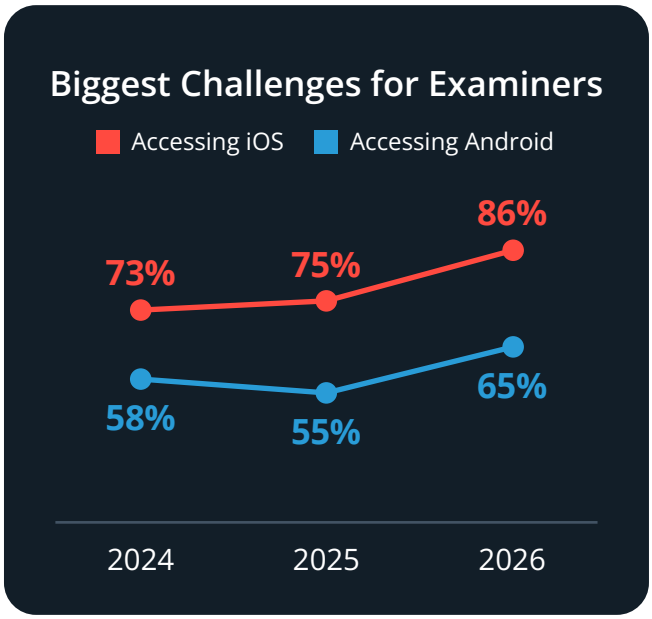
56% of devices arrive locked, creating barriers for examiners and investigators. 86% of respondents report difficulty unlocking iOS devices, while 65% report difficulty with Android. This is a perennial challenge with constant updates to operating systems, typically requiring specialized third-party tools and/or services to unlock devices.

Inability to correlate across sources

This type of correlation is critical for unlocking investigative insights, but it requires analytical tools. Unfortunately, only 28% of respondents report using dedicated analytical tools, leading to low levels of correlation. Finding links between cases is also a significant challenge, with only 44% of respondents saying they are able to do this.

Reporting and translation complexity

57% of analysts struggle to explain technical data to non-technical stakeholders, creating a communication gap that slows down the end-to-end investigative process. For example, 58% of legal teams say that forensic reports are difficult to interpret.

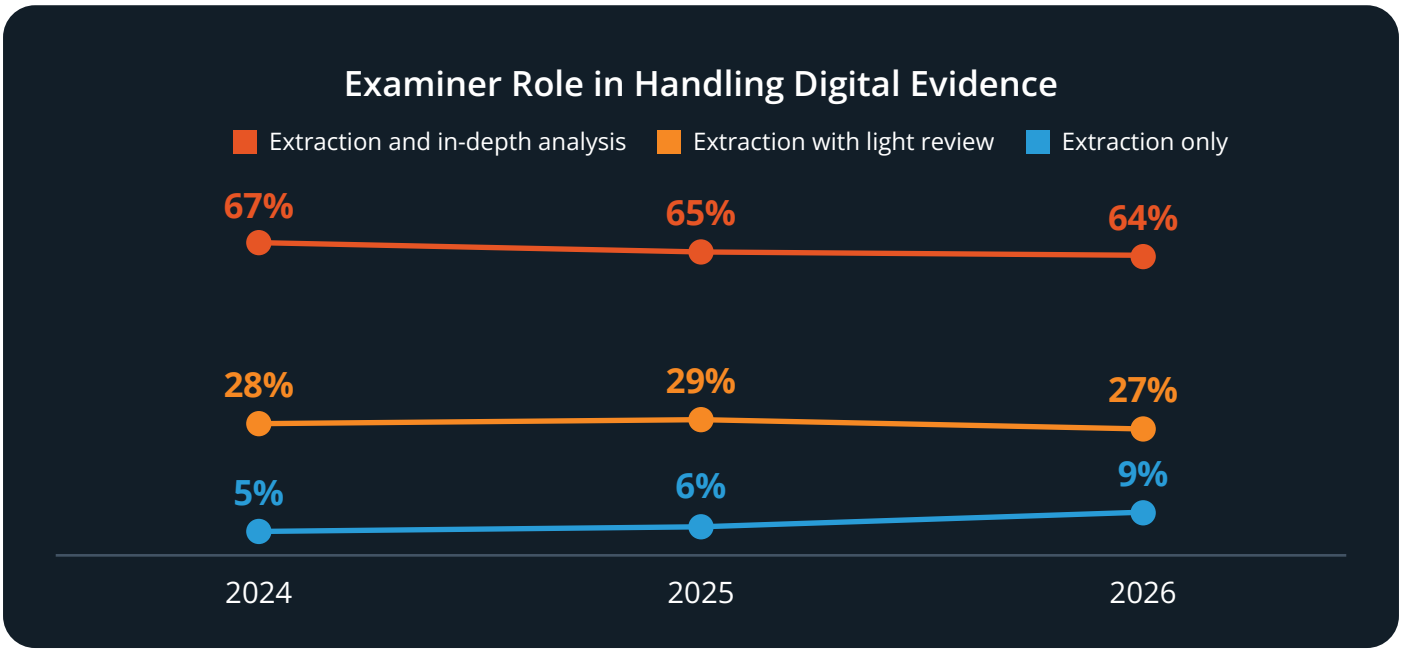


Training gaps

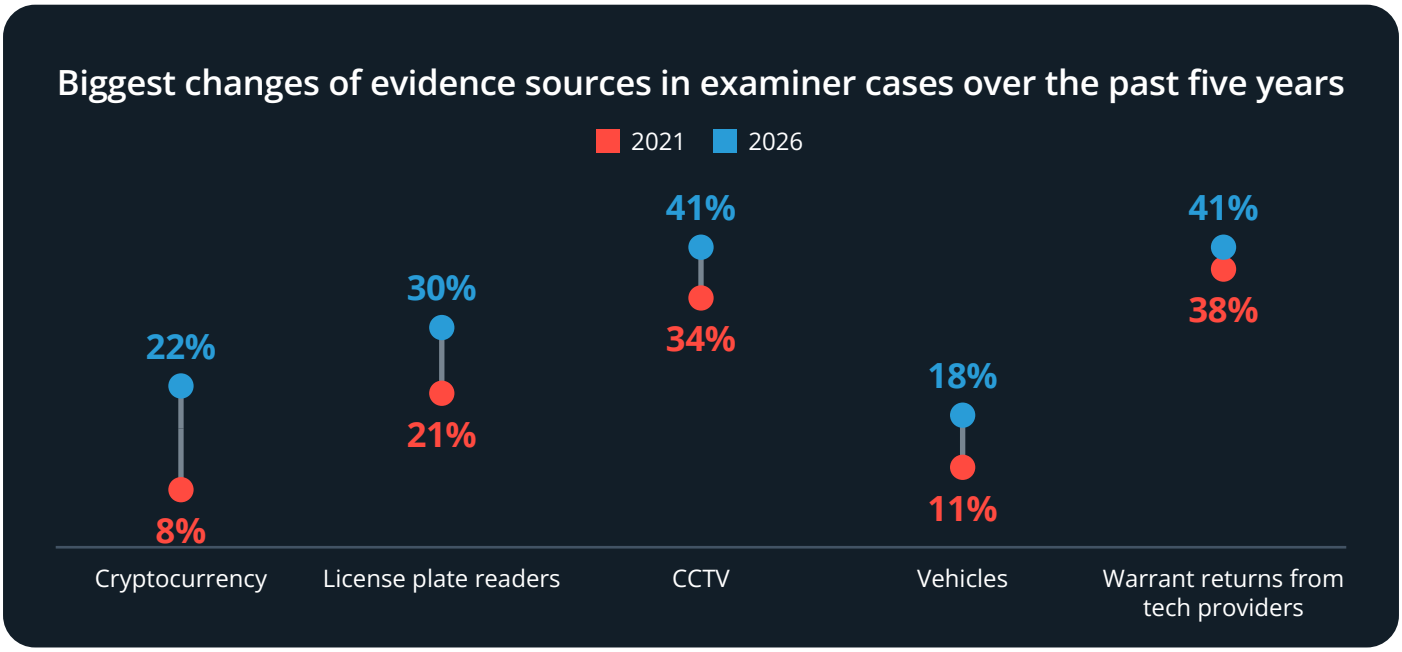
Agency leaders face a scaling problem: more personnel need digital evidence competency, and gaps can slow investigations and extend turnaround times. With technology changing and turnover continuing, maintaining a trained workforce across roles remains difficult. 71% of agency managers report inadequate training as a major challenge.

Digital Forensics: Examiner Workloads

Digital forensic examiners remain central to turning device data into usable, defensible evidence. In 2026, nearly two-thirds report handling both data extraction and in-depth analysis, which is a slight decrease from years prior.



What's changed more noticeably is the shape of the evidence examiners encounter. Smartphones are still nearly universal (97%), but supporting digital sources appear more often than they did five years ago.



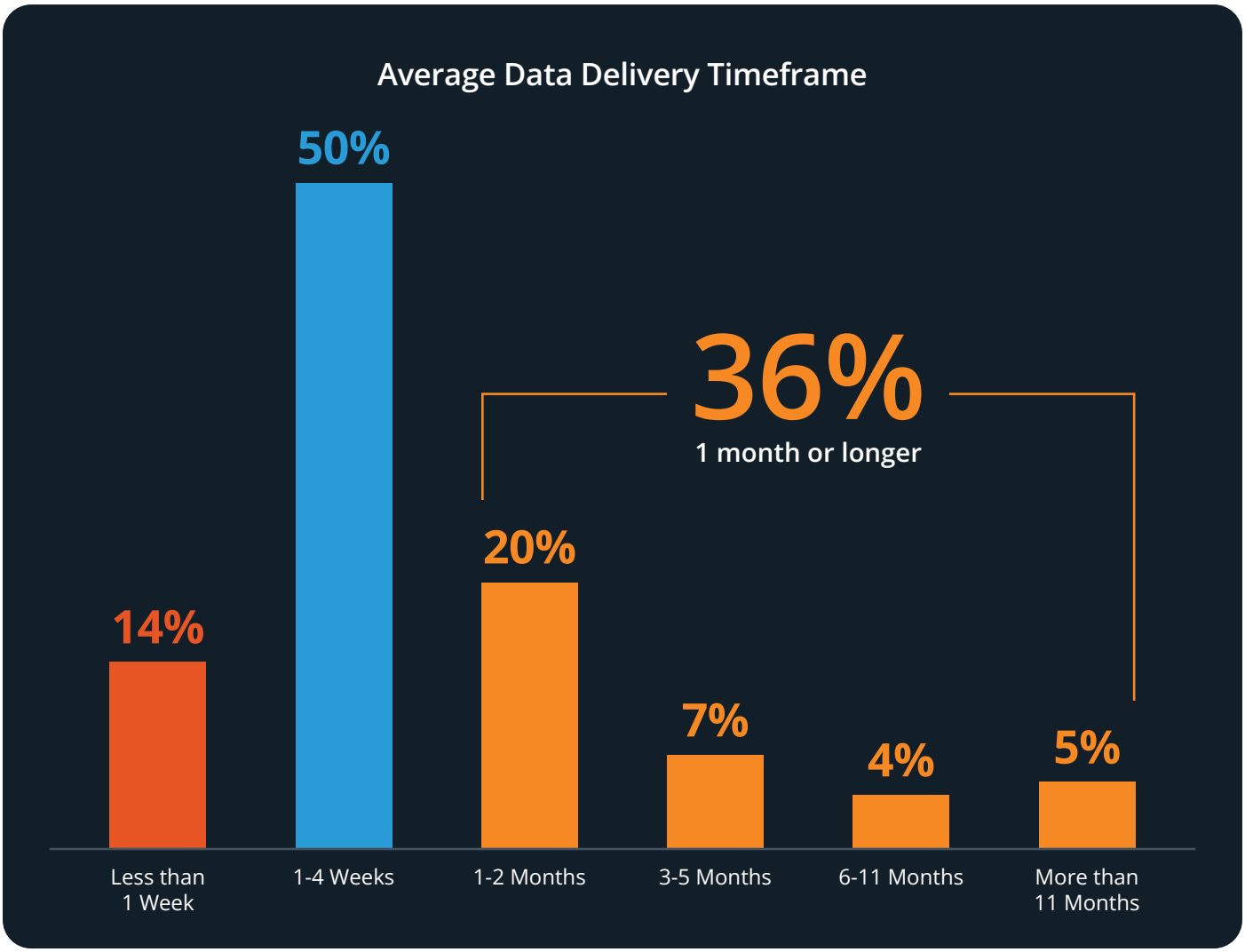
Digital Forensics: Examiner Workloads

More cases now involve multiple digital sources. Single-device cases fell from 17% (2024) to 5% (2025), while two to five devices per case rose from 52% to 74% over the same period.

Work volume is also higher. The median number of extractions in the past month increased from 9 (2024) to 13 (2025 and 2026). Most respondents rely primarily on full file system extractions (86%), with physical (6%) and advanced logical (6%) used far less often.

Access remains part of day-to-day operations. More examiners responded their lab can access locked devices in-house (57% to 70% from 2024 to 2026), though some still rely on nearby agencies (15%) or specialty labs (5%). 10% report excluding locked devices from cases in 2026.

Finally, delivery timelines remain extended: 50% report 1–4 weeks to provide mobile device data or a report, while 36% report one month or longer.



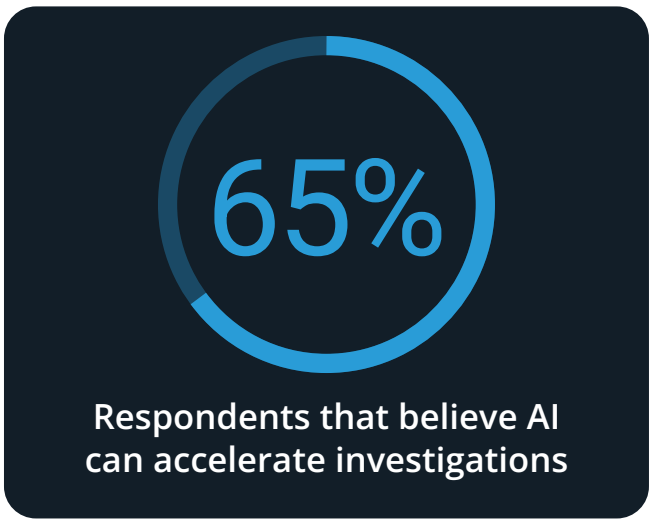
The Investigator Reality

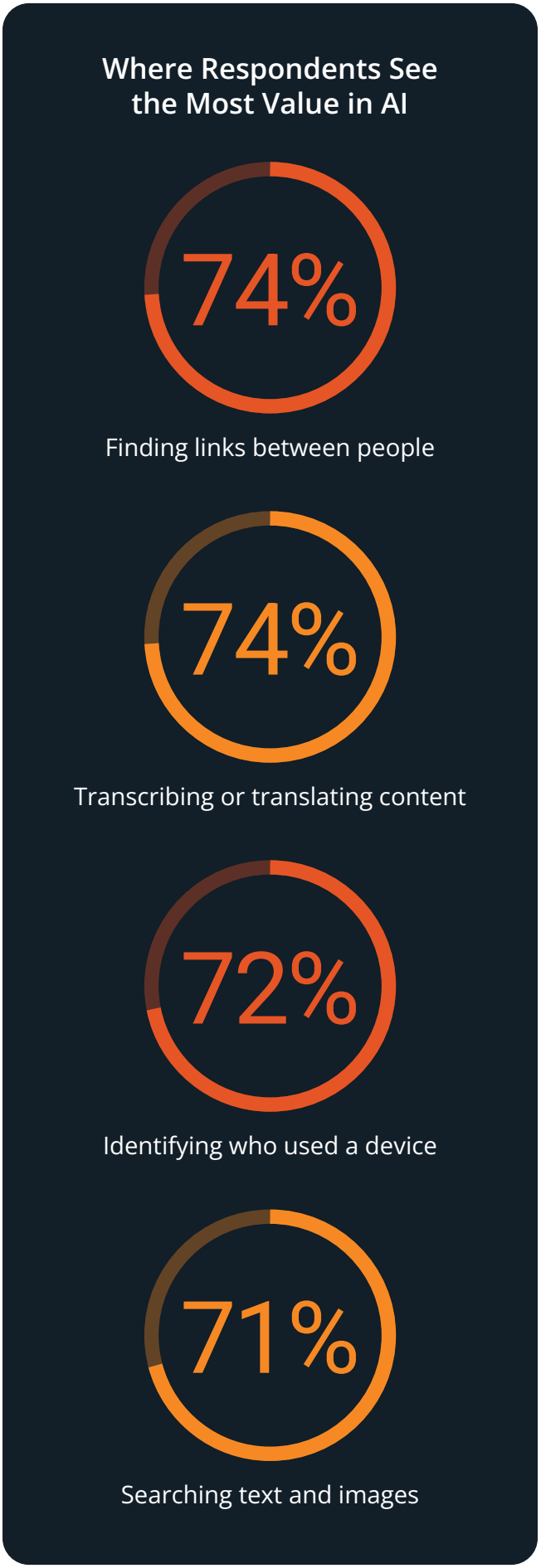
The biggest challenge for investigators once they receive the report is the time needed to review data. Let's break this down by taking a closer look at the modern investigative process and how this is putting enormous pressure on investigators. It's not only about the time needed for an investigation, which is typically **up to 35 hours**. Investigators are also carrying an average **caseload of 6 to 10 active investigations**. Simply put: investigators are juggling approximately 10 weeks of investigative work at any given time.

That puts investigators in a significant dilemma. On one hand, they are under enormous pressure to complete investigations quickly despite their overwhelming caseload. On the other hand, it's essential for them to maintain accuracy and defensibility in court. Even small delays or inefficiencies can lead to backlogs that slow case progress and eventually contribute to eroding public trust. Review and analysis account for most investigative effort, taking up to 20 hours, or nearly 60% of a case's total time.

The problem is that the review and analysis process is highly manual. **More than 70% of respondents say they review evidence manually**, including using spreadsheets (28%), manual file-by-file reviews (30%), and other manual means (14%). **Only 28% use purpose-built investigative analytic tools.** In fact, most teams still look at digital evidence one screen at a time, even when cases span multiple devices.

Unless investigative teams start to automate these time-consuming manual processes, they will continue to struggle with overwhelming caseloads, backlogs and delays.





Artificial Intelligence Can Reduce Bottlenecks

There is a strong belief among respondents that AI can play a significant role in clearing a path for faster investigations. Nearly two-thirds, 65% believe that AI can accelerate investigations, and 78% say that better investigative tools would alleviate caseload pressure.

However, investigators looking to meet these challenges are using AI as an assistant that amplifies human capabilities, but never as a replacement for human judgment and experience. They want AI to take care of the busy work, freeing up their brain capacity to focus on high-value activities such as evaluating the relevance of uncovered evidence, constructing evidence-backed narratives and clearly and accurately communicating investigative outcomes.

Despite the growing value public safety professionals see in AI, adoption remains uneven. About **one-third of respondents say their agency's policies do not allow the use of AI**, limiting access to capabilities that could reduce manual effort and speed analysis.

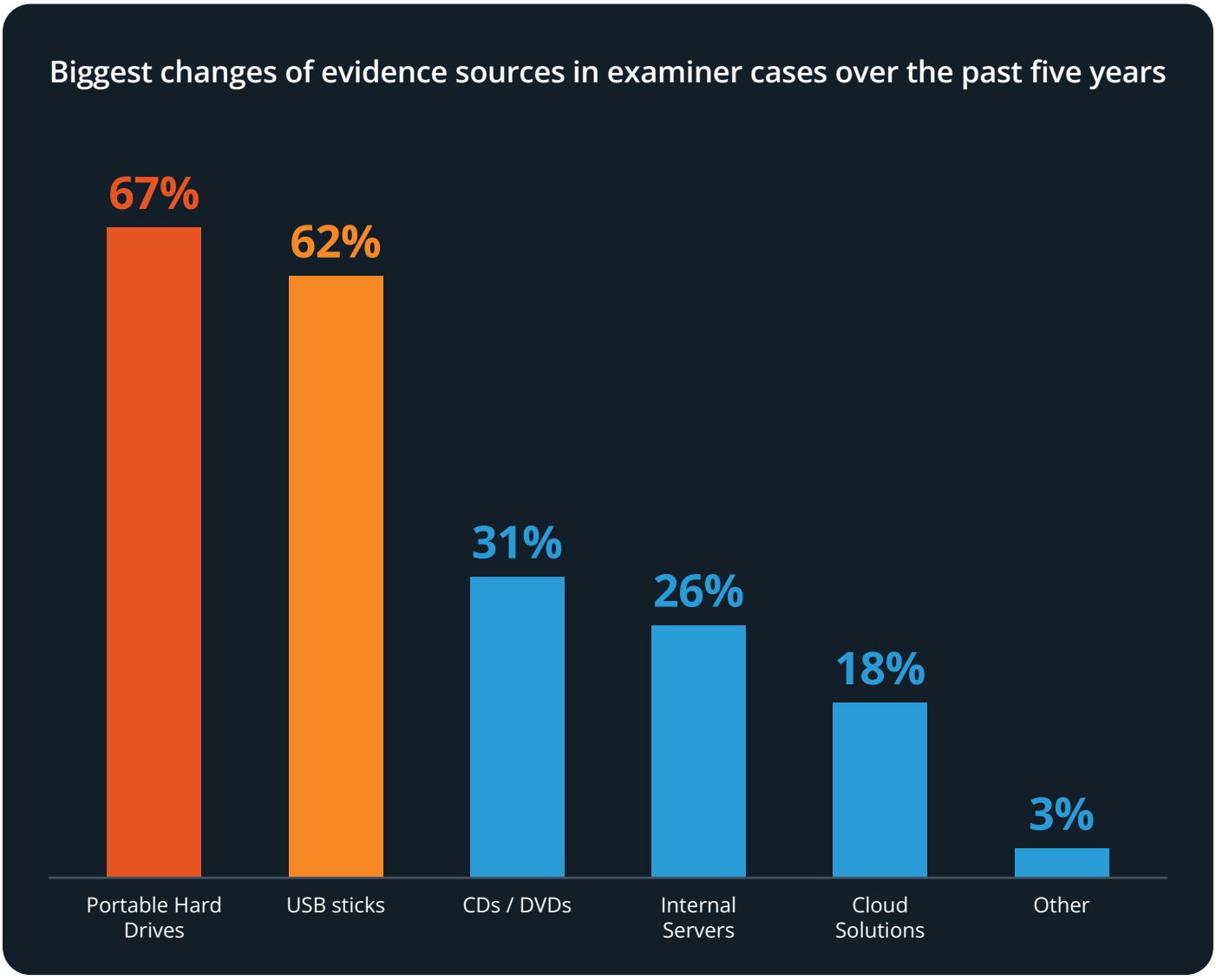
This gap has real consequences. At a time when investigators and examiners face heavy caseloads, rising data volumes and cases that span multiple devices, restrictions on AI use risk reinforcing existing bottlenecks. Without tools that help prioritize, connect and review digital evidence at scale, agencies may struggle to keep pace with investigative demands, contributing to backlogs and longer case timelines.

Collaboration, Cloud and Chain of Custody

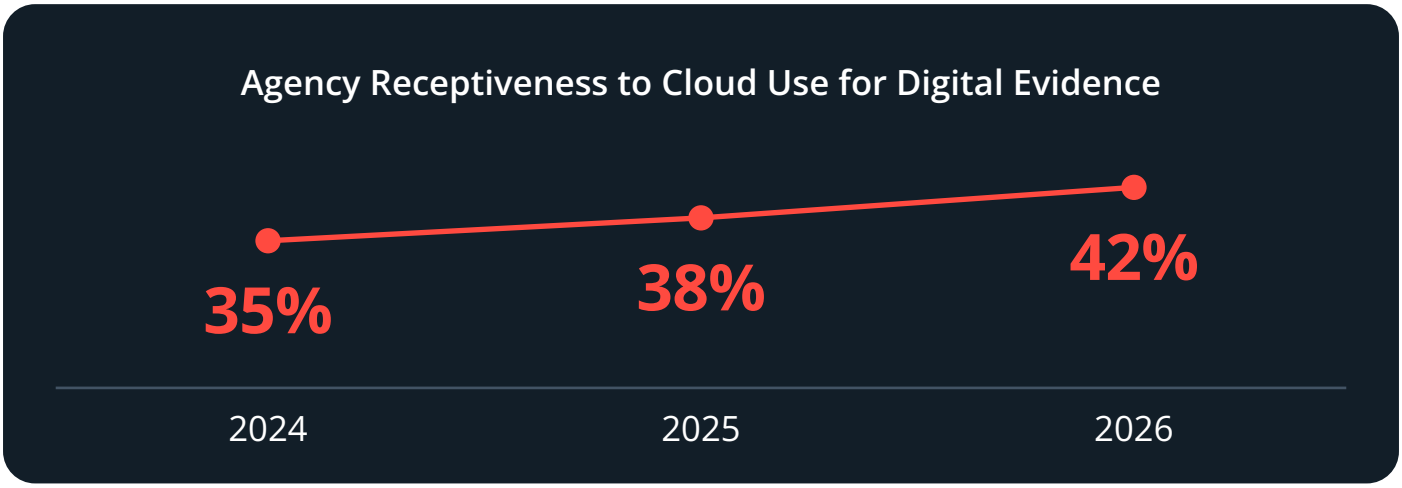
Investigations often involve multiple stakeholders, including prosecutors, defense teams, courts and agencies from other jurisdictions. Because of this, extracted evidence needs to be shared across organizational and geographic boundaries.

However, our survey shows that sharing is a significant issue. More than half of respondents say that sharing digital evidence externally is moderately to extremely difficult.

Why? Because sharing still largely depends on physical media. For example, **67% say they share evidence on portable hard drives, and 62% also use USB sticks.** This makes evidence hard to track, slows down investigations, prevents effective collaboration and puts the chain of custody at risk. The impact is particularly significant for multi-jurisdictional investigations, compromising prosecutorial readiness and public safety partnerships.



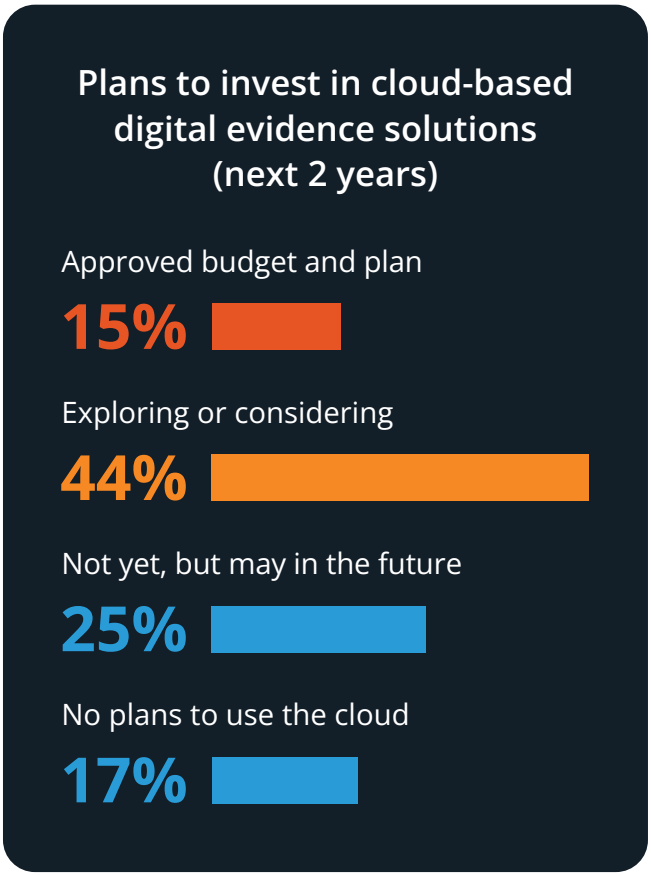
Collaboration, Cloud and Chain of Custody



Cloud Is Gaining Traction

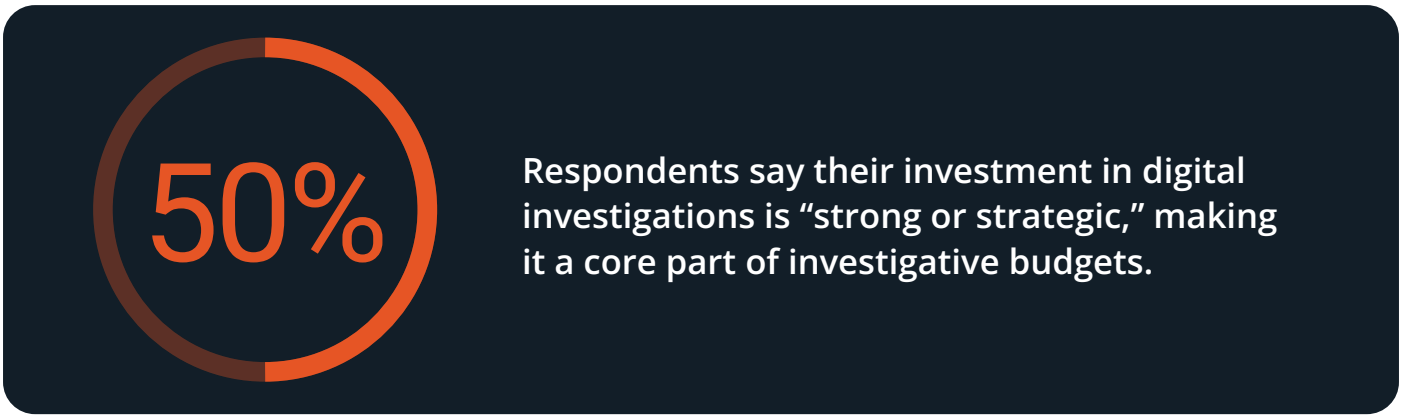
Cloud solutions provide the most efficient, traceable and collaborative way to share digital evidence. While adoption is still limited—only 18% of respondents in the survey use cloud solutions for sharing digital evidence—momentum is growing. Nearly half, 46% of agency managers say they are receptive or very receptive to adopting the cloud, and 44% are actively exploring cloud solutions.

Independent of this survey, it should be noted that several jurisdictions are already embracing the cloud. For instance, the UK National Policing Digital Strategy 2020–2030 recommends adopting a cloud-first approach. Similarly, several US states have adopted cloud-first mandates, including California. The cloud is being mandated in other countries such as New Zealand.



Leaders Are Focusing on Modernization

Public safety leaders are making it clear that modernizing digital investigations is no longer optional. Rising case volumes, more complex evidence and public demand for effective, transparent outcomes have turned modernization into a priority.

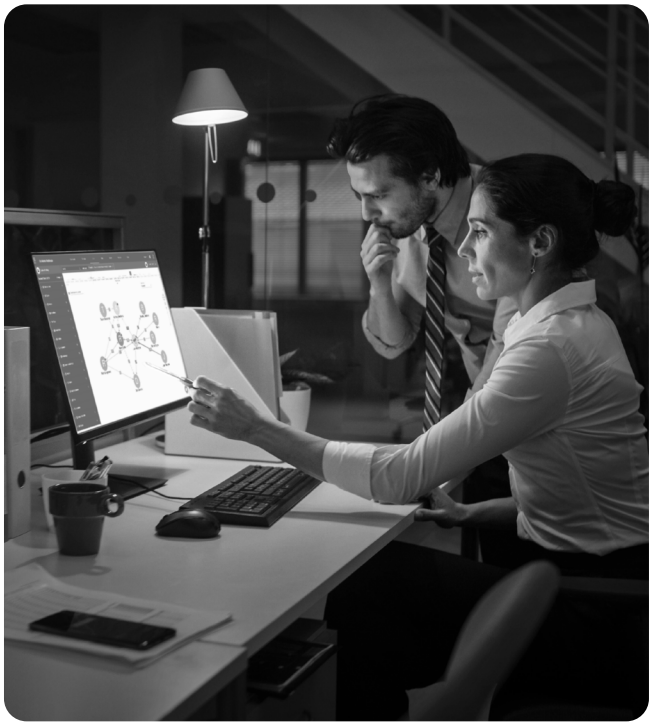


These signals show clear momentum: leaders are committing resources, shifting priorities and embedding modern digital investigation practices into everyday operations.

The Bottom Line

Digital evidence is at the core of modern justice. It runs through every stage of an investigation and helps shape how cases are built. It's not optional—it's a direct and inevitable result of the way we live and communicate in a digital-first world. It also creates challenges for investigations. Survey respondents are telling us they are struggling to cope with the scale and complexity of today's digital evidence landscape. There's too much data, too many connections across multiple devices and sources and too much pressure to deliver under extraordinary caseloads. Traditional, manual approaches have reached the breaking point, leaving the door open for missed or overlooked evidence.

Fortunately, this survey also shows a way forward. Respondents overwhelmingly believe that a combination of automation and AI can accelerate digital investigations, not by replacing human insights and expertise, but by complementing human capabilities and offloading mundane, high-volume work. This has the potential to free up investigators to do what they do best—make informed judgments on the relevancy of evidence, construct compelling and accurate narratives and ensure the transparency and defensibility of their conclusions. At the same time, agency leaders are recognizing that it's critical to modernize digital investigations and are increasingly making the investments needed to drive transformation. This combination of a viable solution and the willingness to adopt it points to a brighter future where digital investigations can scale to support timely, accurate and fair judicial outcomes.

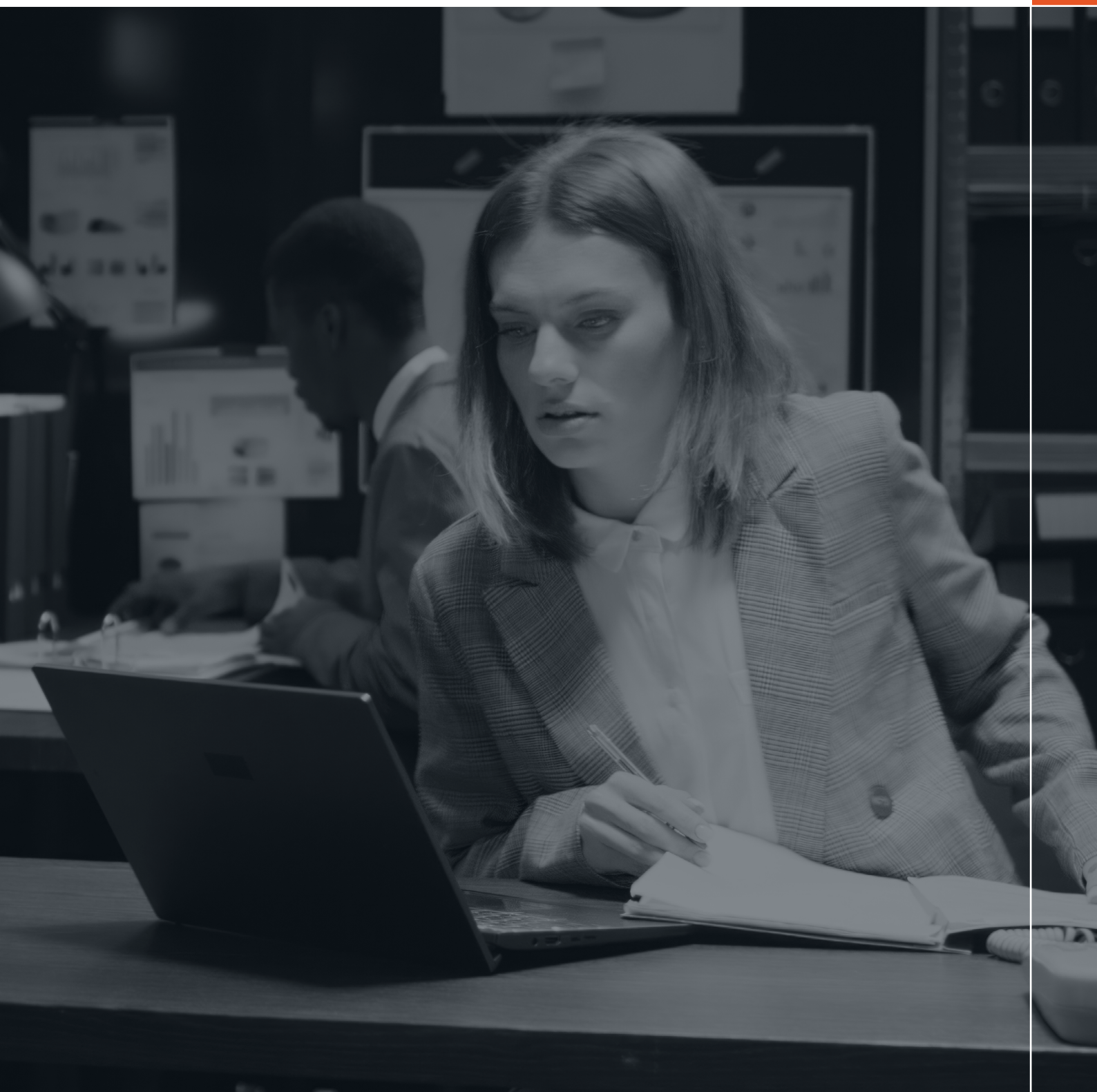


A Final Note About the Survey

Cellebrite wishes to thank our users and practitioners around the globe for taking this survey. Getting the pulse of the industry is critical to decision-making that drives our product innovation roadmap. Cellebrite is proud to be the digital investigative partner of choice around the world, serving more than 7,000+ customers in both the public and private sectors, aiding in more than 1.5 million investigations per year.

Cellebrite

Appendix

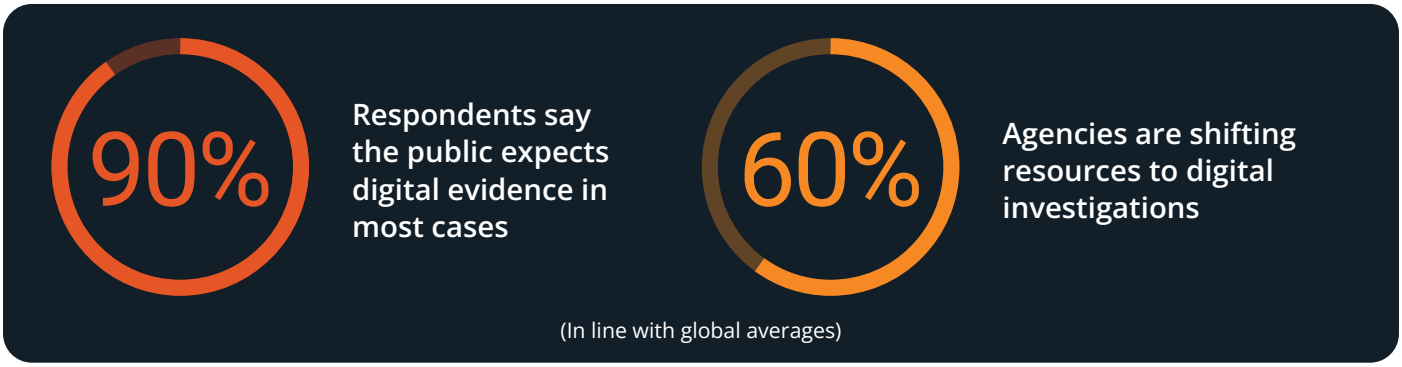


North America

The survey found that North America is broadly aligned with overall global trends, with digital evidence central to case outcomes. Public expectations are high, resources are shifting to digital investigations and caseloads are heavy. However, there are some significant differences. Locked devices are a particular challenge, with North America having the highest rate of locked devices of any region. On the other hand, North American respondents report less difficulty sharing digital evidence, indicating greater cloud readiness.

Digital investigations are the norm

Public expectations and agency priorities remain high



Heavy caseloads persist

Workloads mirror global averages

Locked devices are a major challenge

North America reports the highest lock rates

Manual review still dominates

Limited use of investigative analytics

Respondents use investigative analytics tools

More than half rely on manual review

Respondents say they use Excel or Word

20%

Review extractions one-by-one with digital forensic software

35%

IMPACT: Slower cases and a higher risk of missed connections

Top investigator challenges:

1. Waiting for extractions to finish
2. Time to review data
3. Training gaps in digital evidence review

Greater cloud readiness than global peers

Fewer barriers to sharing digital evidence

Respondents say they are receptive to cloud-based digital evidence management

59%

Respondents say sharing digital evidence is difficult (vs. 57% globally)

43%

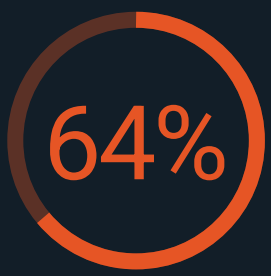
AI seen as high value

Top AI capabilities investigators value

- Analyzing communications to identify links
- Identifying the user of a device
- Transcribing or translating messages and calls

Courtroom clarity remains a challenge

Communicating digital evidence effectively



Respondents say making digital evidence clear and understandable in court is a major challenge

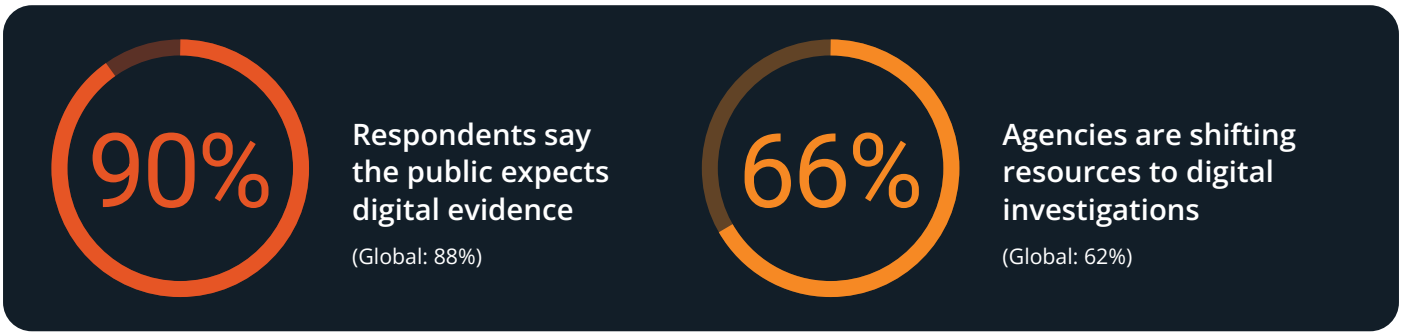
(Global: 68%)

Asia Pacific

In Asia Pacific, digital evidence is central to case outcomes, as it is globally. The public expects law enforcement to use digital evidence, and agencies are shifting their resources to digital investigations. However, Asia Pacific is much more reliant on manual data review processes than its global peers, which slows down investigations and increases the risk of missing connections between evidence items. Cloud adoption is also low. To respond to heavy caseloads and ensure better outcomes, public safety agencies in Asia Pacific must invest in solutions that provide AI-assisted analysis, multi-device correlation and efficient cloud evidence workflows. However, on a positive note, Asia Pacific has a significantly lower rate of locked devices than other regions, making device access easier.

Digital investigations are the norm

Public expectations and agency priorities exceed global averages



Caseloads match global norms

Work volume remains high

Fewer locked devices, but access challenges remain

Access is easier, but not friction-free

Manual review dominates investigative work

Heavier reliance on manual tools than global peers

Respondents use Word or Excel for review

(Global: 28%)

Respondents use digital forensic software to review devices one at a time

Top investigator challenges:

1. Waiting for extractions to complete
2. Time required to review data
3. Reviewing data across multiple devices

Lowest cloud readiness globally

Data sharing remains difficult

Respondents are receptive to cloud-based digital evidence management (Global: 54%)

19%

Respondents say sharing digital evidence is difficult (Global: 57%)

75%

INSIGHT: Limited cloud adoption directly constrains evidence sharing.

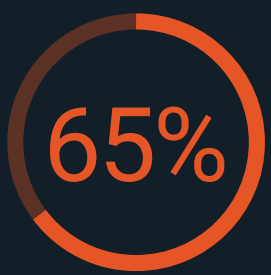
AI seen as high value

Top AI capabilities investigators value

- Identifying the user of a device
- Transcribing or translating messages and calls
- Finding similar or matching images across devices or cases

Courtroom clarity remains a challenge

Explaining digital evidence effectively



Respondents say making digital evidence clear in court is a major challenge

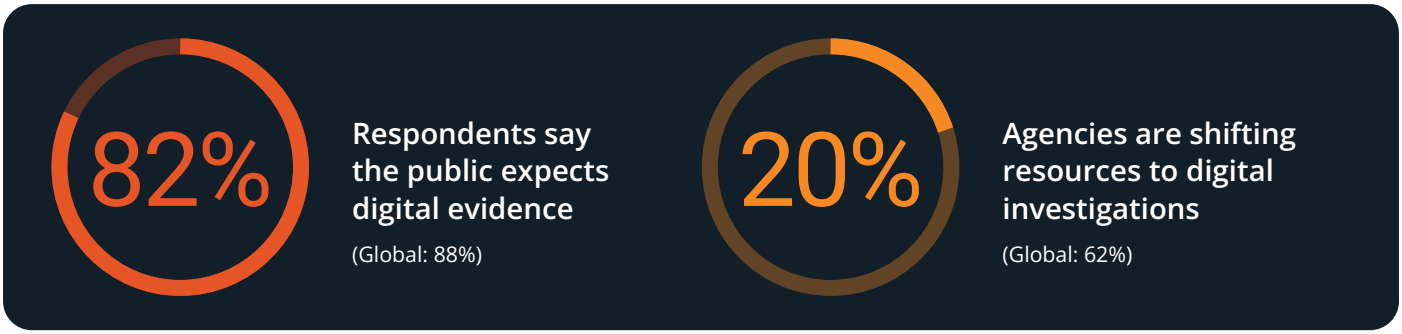
(Global: 68%)

Europe, Middle East and Africa (EMEA)

In EMEA, digital evidence is recognized as critical to investigations, as it is globally. The public expects law enforcement to use digital evidence, yet agencies are reallocating resources to digital investigations at a much lower rate than their global peers. This gap is concerning, as agencies are struggling to scale digital investigation capacity, particularly in the areas of review times and training. Sharing data is also a significant issue, even though there is moderate cloud adoption. This points to other sharing barriers, such as policy, integration or chain of custody constraints. Finally, clearly communicating digital evidence in court is a major challenge, with EMEA struggling more than any other region. To respond, EMEA needs to accelerate modernization, including investing in automated digital analysis, better reporting tools and compliant cloud-based solutions that overcome sharing barriers.

Digital investigations are lagging

Expectation exceeds investment



Caseloads remain high

Workloads mirror global averages

Locked devices still slow examinations

Access challenges persist

Manual review remains widespread

Limited use of investigative analytics

Respondents use investigative analytics tools

Respondents use Word or Excel for data comparison

29%

Review extractions one-by-one with digital forensic software

32%

Top investigator challenges:

1. Time required to review data
2. Waiting for extractions
3. Training gaps

Cloud acceptance is rising, but sharing lags

Structural barriers remain

Respondents are receptive to cloud-based digital evidence management (Global: 54%)

60%

Respondents say sharing digital evidence is difficult (Global: 57%)

60%

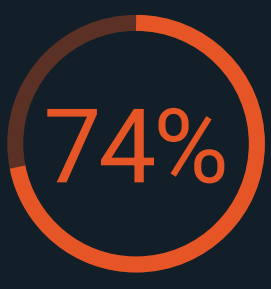
AI seen as high value

Top AI capabilities investigators value

- Transcribing or translating messages, calls and media
- Analyzing communications to identify links between people
- Searching for text within images screenshots.

Court clarity is the highest regional challenge

A critical gap for prosecution



Respondents say making digital evidence clear and understandable in court is a major challenge

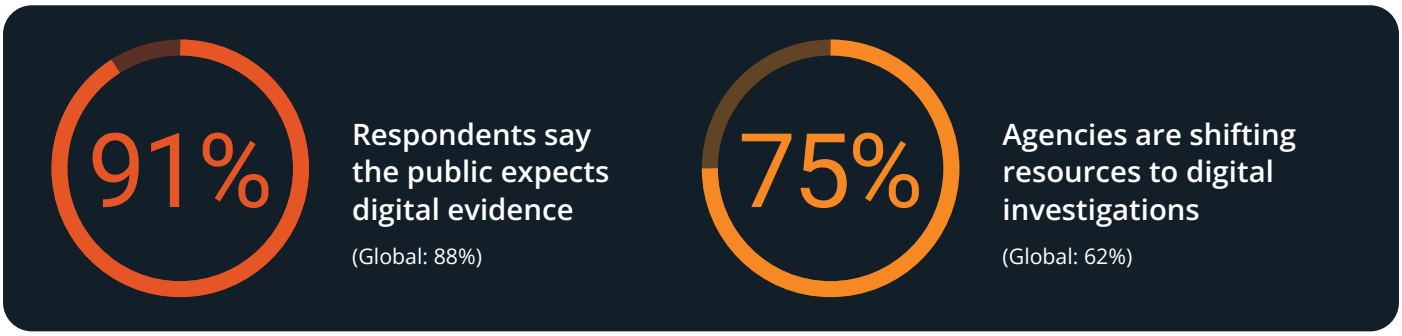
(Global: 68%)

Latin America

In Latin America, digital evidence is central to case outcomes, as it is globally. Public expectations are among the highest worldwide and agencies are reallocating resources to digital investigations faster than in any other region. However, sharing digital evidence remains difficult even though agencies are receptive to using the cloud, reflecting workflow and infrastructure barriers. To respond, agencies in Latin America must invest in AI-based tools that can connect evidence across multiple data sources, as well as compliant, automated cloud workflows.

Agencies are shifting rapidly

Fastest regional move toward digital investigations



Caseloads match global norms

Workloads mirror global averages

Locked devices are a major challenge

North America reports the highest lock rates

Investigator challenges mirror global patterns

Manual work slows progress

Top examiner challenges:

1. Time required to review data
2. Training gaps in digital evidence
3. Difficulty correlating data across devices

More than half of investigators say they review device extractions one by one using Word, Excel or digital forensic software, which increases review time and the risk of missed connections.

Cloud readiness is strong, but sharing remains difficult

Adoption outpaces workflows

Respondents are receptive to cloud-based digital evidence management (Global: 54%)

69%

Respondents say sharing digital evidence is difficult (Global: 57%)

60%

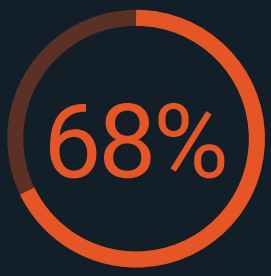
AI is seen as highly valuable

Practical, communications-focused use cases

- Translating or transcribing messages, calls and files
- Analyzing communications to identify links between people
- Searching for text within images or screenshots

Courtroom clarity remains a concern

Clear communication is essential



Respondents say making digital evidence clear and understandable in court is a major challenge

(Global: 68%)