



Whitepaper

The State of Corporate Investigations in 2022

Table of contents

Introduction	03
Types of Investigations and common triggers	03
Modern Digital Investigations	06
Internal reports	06
Data security incidents	07
Due diligence & second requests	09
The Challenges of Effective Investigations	10
How Technology Mitigates Challenges	14
Practical Tips	17
Early Case Assessment (ECA)	17
Internal investigations	18
Regulatory investigations	19
Conclusion	20

Overcoming investigative challenges

While the coronavirus pandemic changed much, workplace misconduct itself hasn't gone anywhere.

Theft of customer funds. Workplace harassment and discrimination. A data breach. An employee's violation of corporate leave policies. A potential acquisition target's incomplete books. A proposed executive hire with a history of inappropriate social media comments.

There's no shortage of situations that organizations need to investigate. While the coronavirus pandemic sent many employees home to work, shifting some of the subjects of investigations and some of the means of reporting concerns, workplace misconduct itself hasn't gone anywhere.

Investigations are incredibly diverse in their subject matter, but they pose a common set of pressures and challenges, such as short timelines, secrecy regarding an investigation's subjects, and an overwhelming abundance of potentially relevant data, to name just a few.

Fortunately, the tools created to manage electronic discovery—including technology-assisted review, entity search, and relationship analysis—are equally adept at managing the challenges of investigations.

This report summarizes the current state of internal investigations and lays out the key challenges that organizations face when it comes to managing their data during an investigation. It then reports how organizations are currently using eDiscovery technology to overcome those challenges and proposes additional ways that organizations could leverage eDiscovery tools and techniques to complete investigations quickly and efficiently across several use-case examples.

Types of investigations & common triggers


Investigations can cover a lot of ground. If someone can think of a way to do wrong, eventually, a company is going to need to investigate that activity. In the modern digitized world, any investigation will be primarily digital. Digital investigations may be proactive or reactive, and a company's involvement with an investigation may occur shortly after a pattern of activity has begun, or months or years later.

Investigations can take a variety of forms and begin with a range of triggers:

- **Internal investigations** into specific allegations such as employee fraud, theft, or misappropriation of company property; theft of trade secrets or intellectual property; or harassment, discrimination, or the creation of a hostile workplace are a sampling of conduct that could lead to an internal investigation.

organizations that fall victim to data breaches must act quickly after such an incident.

- **Regulatory investigations** into an organization's legal and regulatory compliance may begin with a whistleblower allegation or a regulatory agency's detection of an irregularity in financial statements or other required reporting.
- **Due diligence** in anticipation of a merger or acquisition may be part of the company's internal processes or conducted in response



In the modern digitized world, any corporate investigation will be primarily conducted into digital material.

These investigations can begin with specific employee complaints, anonymous hotline reports, anomalies observed during regular audits or other oversight, or through internal web-reporting mechanisms. In the wake of the coronavirus pandemic, internal web-reporting has been a growing source of internal investigation triggers.

- **Data security incidents** such as data/security breaches or insider threats may be first detected by a loss of services, a third-party demand, a user complaint, or an internal alert or notification. Due to the requirements of GDPR,

to a second request from the Federal Trade Commission (FTC).

- **Proactive investigations** may include vetting of C-suite candidates, board members, or other high-level or high-profile employees; audits or other internal assessments of employees' and officers' compliance with corporate policies and applicable regulations such as data privacy requirements; and early case assessment (ECA) processes to test the strength of a potential case before deciding on a course of action.

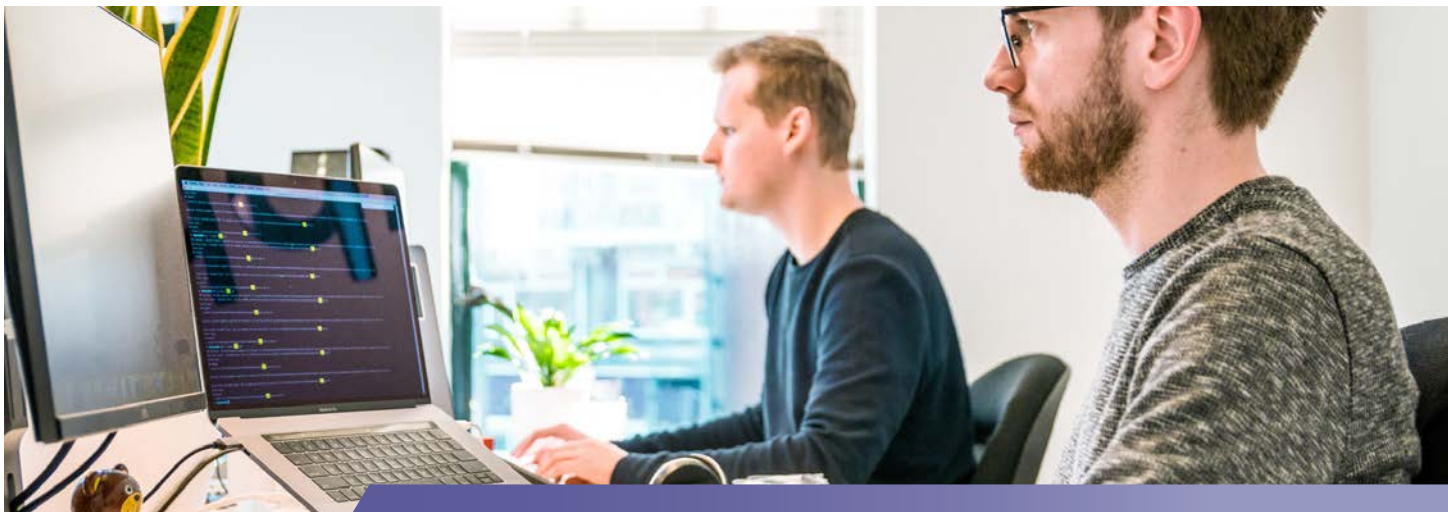
Whatever the trigger and whatever the substance of the allegation, investigations follow a relatively consistent path that includes:

- Detection of a trigger event and identification of the nature of an allegation;
- Planning an investigation, including a determination of what the organization needs to prove or disprove and who should lead that investigation;
- An identification of the actors involved and any potential data custodians;
- Identification, preservation, and collection of potentially relevant information;

- Iterative searching of the organization's electronically stored information (ESI); and
- Preparation of a report with findings, conclusions, and next steps;
- All while maintaining a chain of custody for data in case the results of the investigation need to be produced for a third party.

With that in mind, let's take a closer look at trends in corporate investigations.





Modern digital Investigations

Corporate investigations in a post-pandemic world

Reports and investigations seem poised for a banner year as more employees return to in-person work.

The coronavirus pandemic has upended much of the business world for the last two years, and investigations have not been exempt from those and other changes.

Internal reports in some industries have dropped off in favor of direct whistleblowing to regulatory authorities or governmental institutions.

The widespread shift to remote working may have dampened some reporting—although a decrease in reports does not necessarily reflect a change in the level of misconduct. Overall, however, reports and investigations seem poised for a banner year as more employees return to in-person work.

Internal Reports

According to the [NAVEX Global 2021](#) Risk and Compliance Incident Management Benchmark Report, the median number of internal misconduct reports declined slightly for the first time in years. On average, there were 1.3 reports per 100 employees in 2021; in other words, a 1,000-person company would face about 13 events per year.

Reports through traditional hotline services decreased, with more incidents brought to the company's attention through web-reporting systems, perhaps reflecting the increase in remote work and online communication.

There was also a decrease in retaliation, harassment, and discrimination reports, which may have become less visible or easier to tune out while employees have been working remotely. These reports could rise substantially with the widespread return to in-person work.

In a troubling trend, the benchmark report also noted that “the gap between incident occurrence and incident reporting dates (...) widened dramatically.”

For accounting, auditing, and financial reporting, the delay from incident to report more than doubled, from an average of 16 days to 36 days. With every day that passes, investigations become more difficult, so this delay in reporting could be crucial.

33%

The number of data breaches with significant data losses increased 33% between 2020 and 2021, climbing from 3,950 to 5,258.

Data security incidents

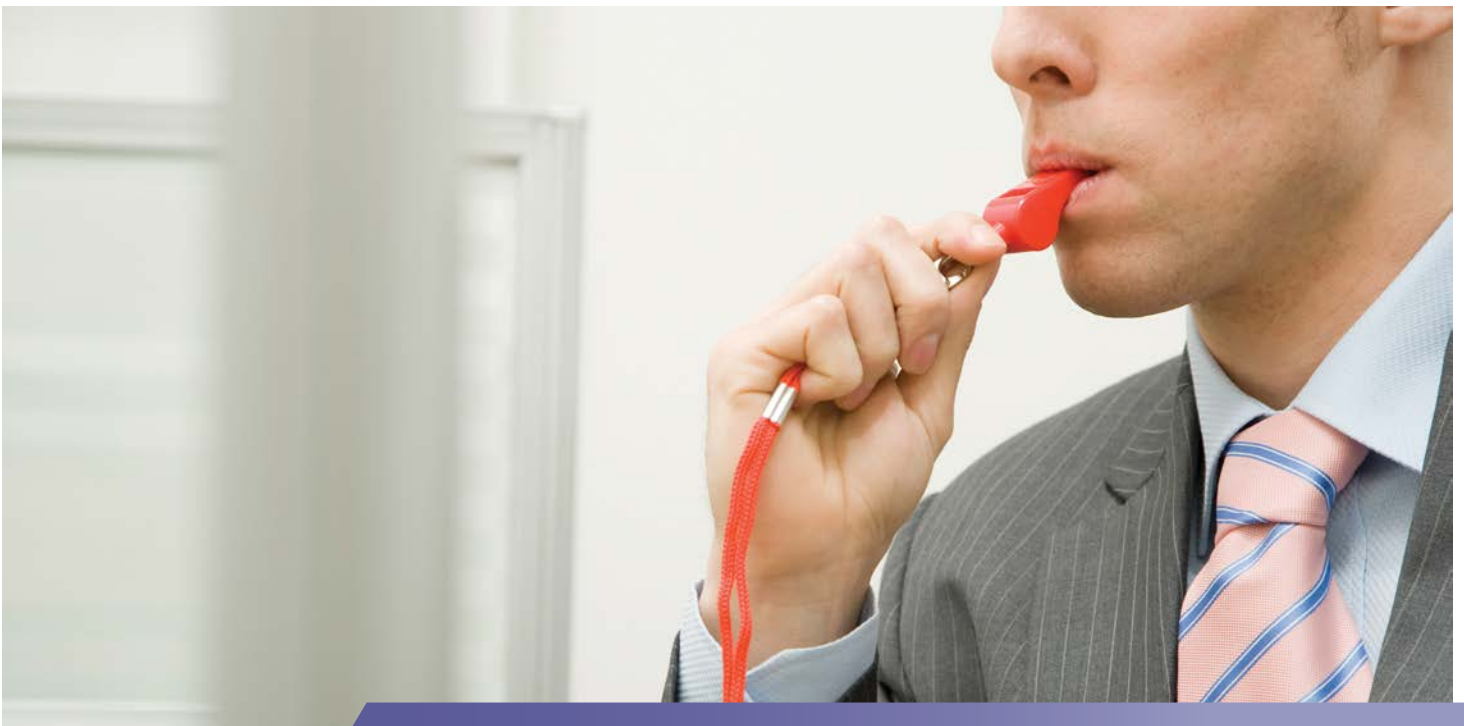
With the move to online working and online services, it's no surprise that data security incidents have increased substantially over the last few years. Based on data sourced from over 88 different countries, the Verizon 2021 [Data Breach Investigations Report](#) found 5,258 confirmed data breaches where data was lost. This was up from 3,950 in [2020](#). That's over 20 breaches per workday—and a whole lot of data security investigations.



Government Investigations

One of the reasons that there may be fewer internal reports of misconduct is the increase in financial incentives for federal whistleblowers. In its 2021 Annual Whistleblower Program Report to Congress, the U.S. Securities and Exchange Commission (SEC) summarized its record-breaking year, with 108 individuals who received approximately \$564 million in awards. That represents, in the SEC's words, "more whistleblower awards in FY 2021 than in all prior years combined." With huge financial incentives at play, the SEC received more than 12,200 tips, up 76% from the prior year.

"The Commission made more whistleblower awards in FY 2021 than in all prior years combined."



Due diligence & second requests

Another major source for digital investigations are due diligence and second requests associated with Mergers & Acquisitions (M&A). Whenever companies are involved in an M&A process, large digital investigations are held on both ends.

In the US, the Federal Trade Commission (FTC) received a total of [3,644 merger](#) filings under the Hart-Scott Rodino (HSR) Act in 2021—so many that its own employees struggled to keep up with the agency's timelines. The overall value of mergers and acquisitions in 2021 reached a [record high of \\$5.8 trillion](#), up 64% from the previous year.

Though Europe saw no such an increase, levels did [bounce back](#) to pre-pandemic levels over the course of 2021: M&A deal numbers rose to a total of 2,015 transactions, a higher total than in 2019 (1,958) after a down year in 2020 (1,705). In terms of M&A in the larger countries in Europe, the United Kingdom and France lead the way.

All told, organizations are facing unprecedented challenges in keeping up with investigations. Let's turn to a more in-depth consideration of those challenges.



The pursuit of compliance

Having a robust compliance program and proper investigative tools in place won't guarantee you stay out of trouble - but it'll reduce the amount of trouble you might find yourself in.

Having a solid plan for investigations saves organizations money and reputational damage. What's more, in many jurisdictions having appropriate policies and safeguards in place will put the organization and the leadership in place for (some degree) of clemency.

Referring back to the GDPR [enforcement tracker](#), many of the fines follow instances of "Insufficient technical and organizational measures to ensure information security". However, investigations present a wide array of challenges:

are involved, timelines can grow even shorter and less flexible. The prompt action demanded by investigations does not leave time for legal or compliance teams to sift through data manually.

- **Discretion and secrecy.** Organizations conducting an internal investigation do not know whether the allegation is founded at the outset. It is often in the company's best interest, then, to conduct its initial investigation quietly, without disclosing the claim or its suspicions to other employees or the subject

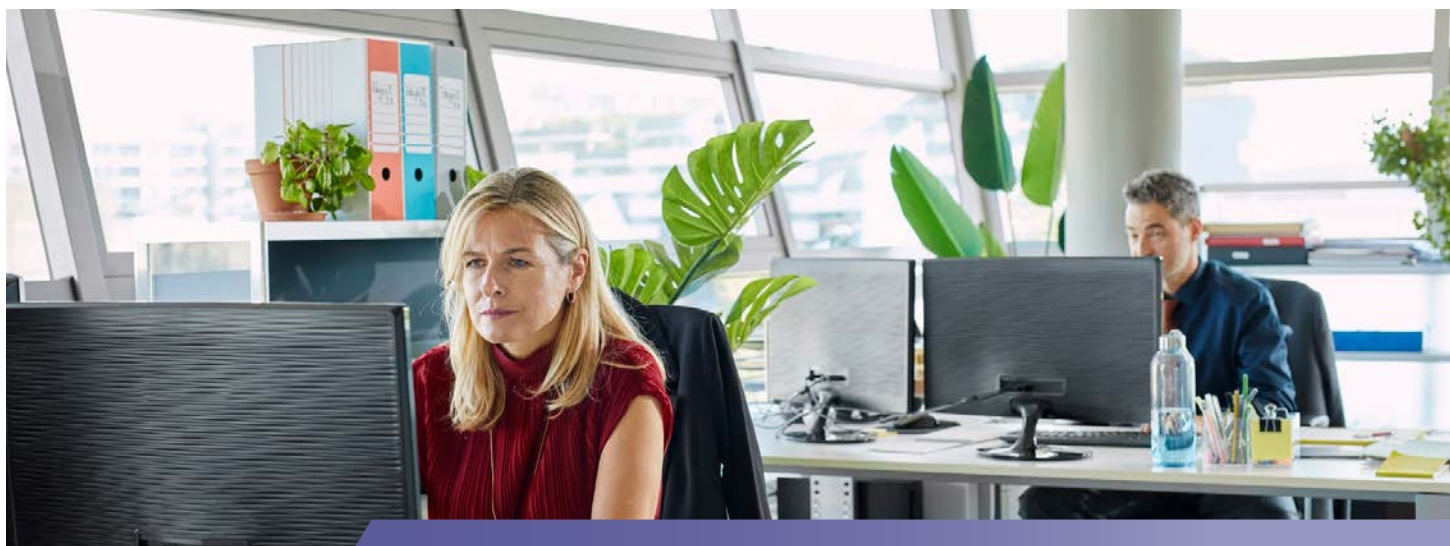


Many fines handed by GDPR enforcement agencies are for lacking organizational and technical security measures.

- **Short timelines.** When an organization learns about a complaint, it must act quickly. Every day that goes by without action is another day during which an employee is stealing funds, mistreating a coworker, or abusing corporate policy. When regulatory agencies

of the investigation. If a governmental agency is involved, that agency may not fully disclose what or who it is investigating, leaving the company to search for records without a complete understanding of the conduct it is investigating.

- **An unclear scope.** An initial allegation is likely to contain only the facts known to the complainant, but those are not necessarily the only important facts. For example, if an employee reports that their supervisor discriminates against them on the basis of race, gender, or other protected characteristic, there may be other employees—current or former—who have experienced the same treatment. The scope of an investigation should be controlled as tightly as possible, but sometimes an investigation must expand to encompass new facts. When regulatory agencies are involved, an organization is entirely at the mercy of that agency in setting the scope of its investigation.
- **Cross-departmental responsibilities.** Investigations can implicate a wide range of departments and organizational units, from HR, IT, and compliance to the C-suite, risk managers, data privacy officers, and the legal team, both in-house and outside counsel. Keeping everyone on the same page—while maintaining discretion and data security—can be a substantial challenge.
- **Unknown unknowns.** If bad actors communicated explicitly about their intentions, it would be quite easy to search for evidence of their misdeeds. Unfortunately, they generally hide their actions behind code words or other veiled references—leaving organizations to figure out how to uncover those unknown unknowns with few, if any, hints to start from.
- **Cross-border data privacy issues.** When data relevant to an investigation resides in a jurisdiction with strict data privacy laws, transferring that data to another jurisdiction with weaker protections may create an entirely new compliance issue for the organization.



- **Volume and accessibility of data.** Data that is relevant to an investigation could be found almost anywhere: on the local drive of a laptop, on a mobile phone or tablet, in a file-sharing platform, in a cloud account, or within a browser-based application such as a project management or collaboration tool, among other possibilities. Organizations must sift through a tremendous volume of data—some of it hard to access or export—to find the facts they need.

litigation process as it exists in the United States. The need to defensibly preserve information and effectively search through it to find relevant facts, for instance. However, there are key differences between the information needs of discovery and those of a digital investigation.

During discovery, the goal is to find every potentially relevant piece of information that can reasonably be found. The point is to be exhaustive: the amount and depth of information disclosed



In spite of many similarities, there are a number of key differences between discovery and investigations.

- **Legal defensibility.** Many investigations ultimately lead to litigation or must report results to third parties (regulatory agencies, for example). To prepare for that possibility, organizations must manage data in a defensible manner, preserving chain of custody and ensuring that no data is modified or otherwise interfered with.

needs to convince the opposing side in a litigation (and the court) that a thorough good-faith effort was made. Thus, finding the evidence is the point of the exercise. To achieve that objective, legal teams have an indeterminate, and generally lengthy, timeline. Discovery can and often does span years—during which the costs just keep piling up.

The goal of an investigation, on the other hand, is either to find evidence in support of an allegation or to conclude that there's nothing there to find

Some of the challenges associated with searching through data for an investigation are similar to those faced during the discovery stage of the

and that the allegation was unprovable, false or mistaken. To that end, investigation teams should conduct a reasonable and diligent search for evidence of suspected malfeasance or noncompliant behavior, but they need not turn over every conceivable stone. The less exhaustive nature of digital investigations means the timelines are significantly shorter: an investigation often seeks to reach at least a preliminary conclusion in a matter of weeks.

Despite their differences, though, investigations have enough in common with discovery processes that they can benefit from the technologies developed for eDiscovery. The goals may differ, the tools need not.



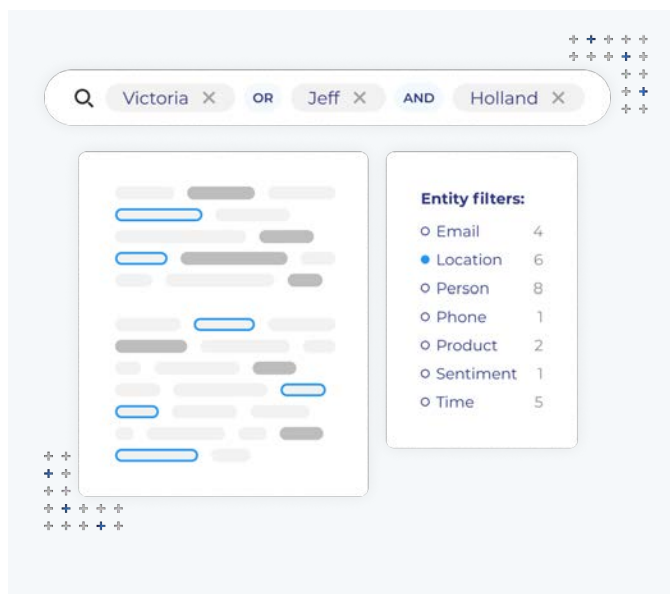
How eDiscovery technology helps digital investigations

To achieve different goals with similar tools, investigators use eDiscovery technology in similar, but different ways than eDiscovery experts.

Both eDiscovery and digital investigations require the ability to rapidly and accurately sift through reams of data, discarding unhelpful or irrelevant data sources, surfacing important facts, and identifying hidden patterns. The tools developed for eDiscovery are therefore tremendously applicable to investigations. Those tools fall into four broad categories:

1. **Automation tools** such as deNISTing, deduplication, data processing, email threading, and optical character recognition. These techniques can quickly eliminate extraneous data files, organize messages into related threads, and allow investigation teams to focus on the data that might help their search rather than getting bogged down in duplicate files or missing clues in image files that haven't been converted to searchable text.
2. **Context tools** such as entity search, basic entity extraction, foreign language extraction, language translation, and dark language detection. These basic analytics capabilities can quickly detect concepts such as persons, places, and things and can then group like concepts

together. For global organizations where employees use multiple languages, language extraction and translation tools are crucial for conducting efficient and rapid investigations that incorporate data sources written in other languages. These capabilities are founded in part on natural language processing (NLP),



a branch of artificial intelligence (AI). Dark language detection—which can unearth code words—is particularly useful in the context of investigations.

3. Proactive intelligence tools such as technology-assisted review (TAR), topic modeling, concept clustering, and document classification. These approaches use AI—both the older predictive coding models and the newer continuous active learning approaches—to group documents into related sets and determine which are most likely relevant or helpful.

4. Emerging intelligence approaches such as relationship analysis, auto-detection and auto-redaction of sensitive entities, network analysis, sentiment analysis, and anomaly detection. These advanced analytics tools represent the next frontier for legal technology, and they're particularly helpful for investigation teams, as they can quickly uncover relationships between parties—even when those relationships are carefully concealed—based on communication patterns. Auto-detection and auto-redaction of sensitive entities also help organizations protect private data when an investigation involves cross-border data transfers and the accompanying data privacy considerations.

According to our [2021 State of AI and Technology Adoption in Legal Discovery](#) report, investigation teams have embraced many—but not all—of these tools. For example, the large majority of investigation teams are using TAR to quickly review

datasets. About 75 to 80% are using entity search to identify concepts such as persons or locations without knowing specific names or keywords for those concepts.

But other tools that would be enormously helpful in the context of investigations are underutilized.



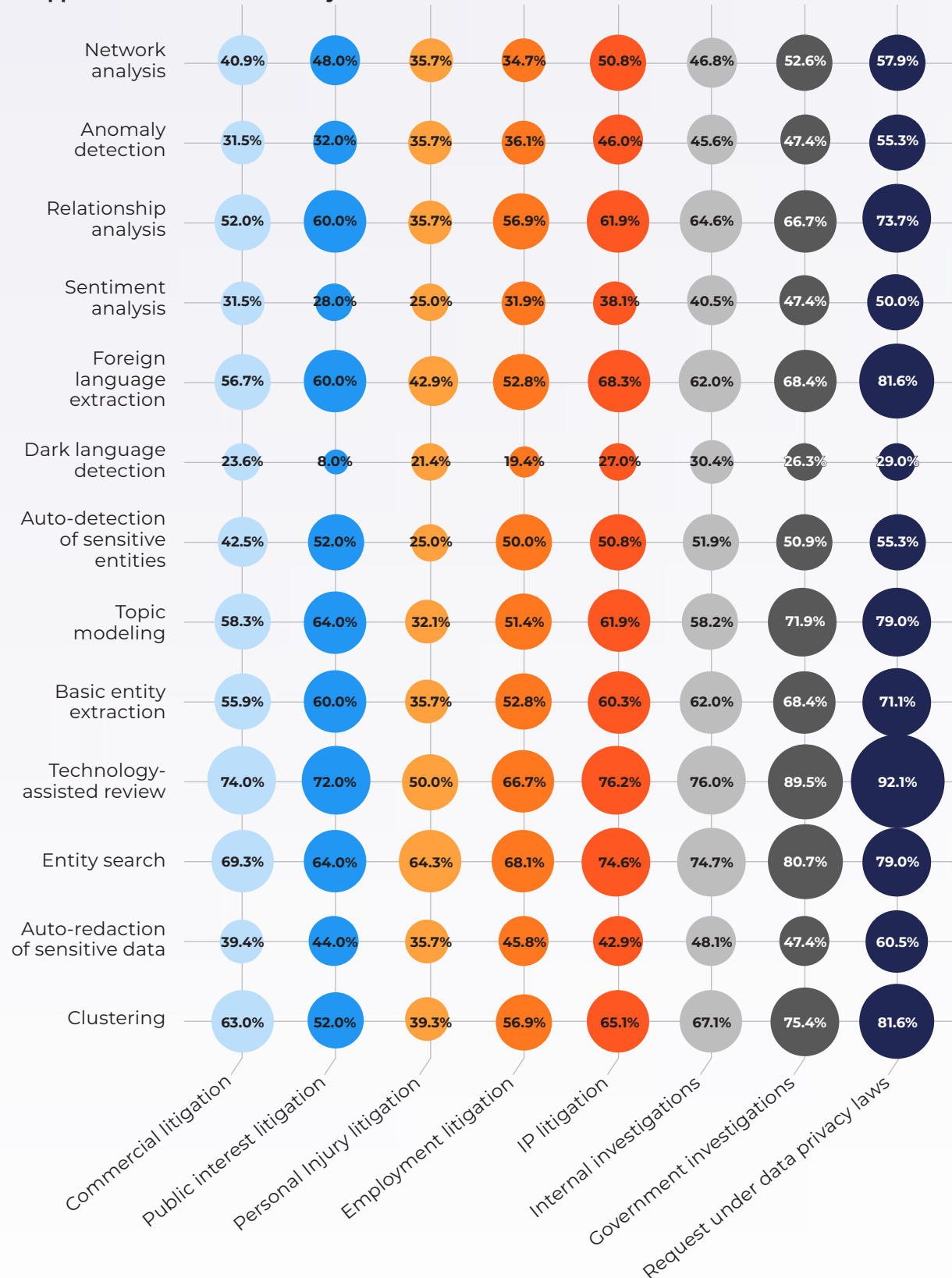
75-80%

of investigative teams are already using Technology Assisted Review to seek out evidence without specific keywords.

Not even half of investigation teams are using anomaly detection to recognize unusual patterns of behavior; fewer than a third are using dark language detection to highlight potential code words or suspect behavior.

To better understand the applicability of these technologies to investigations, let's look at a few specific use cases.

AI applications across eDiscovery use cases





Practical tips

Use case examples of eDiscovery during investigations

A summary of eDiscovery tools that lend themselves well to being applied at various stages of the digital investigations process.

Early Case Assessment (ECA)

In a proactive ECA investigation, an organization seeks to quickly determine the key facts of a potential case to determine how it will ultimately play out. How long will the underlying matter take to work its way through the court system? What is its outcome likely to be? How much will it cost to reach that probable conclusion?

With these answers, legal teams can make a well-informed decision about how to proceed. Often, settling a case early is the most cost-effective—and least damaging—way to manage it.

But if an organization's ECA process isn't designed to handle the rising volume of business data, the costs of ECA can spiral out of control, negating its potential cost savings. Fortunately, eDiscovery

techniques using AI can quickly cut through excessive data to highlight the key facts of a matter, pinpoint helpful custodians, and decide on a reasonable strategy for handling the matter.


To make the most of ECA, leverage tools such as:

- **Relationship and network analysis** to examine the timing, frequency, and intensity of communications and activities between different individuals, and discern relationships among them. These tools can uncover additional custodians or parties of interest and rapidly bring a fuzzy allegation into clear focus.
- **Concept clustering** to identify related concepts within or across different documents and data points and to uncover new areas for investigation and analysis.

- **TAR** to quickly focus on highly relevant documents and gain a sense of the overall strength or weakness of a case—and to just as quickly disregard documents that are not helpful.

anything in between. Helpful technologies for internal investigations include these:

- **Entity search and basic entity extraction** to identify key concepts—be they people, activities, places, or events—and group those concepts



Once an investigation is triggered by a report or request, the clock starts ticking to avoid reputational and/or financial damage.

Internal investigations

When an organization learns of potential employee misconduct or internal noncompliance—whether that concern is reported by an employee, pointed out by a regulatory agency, or detected during a standard audit—it must act quickly.

The investigation team's first priority is to determine whether that complaint is founded so that it can take prompt remedial action or whether it is a false alarm that it can just as swiftly close the book on. In those cases where an allegation is founded, the organization must also prepare for the possibility of legal action or a regulatory agency's intervention.

Internal investigations run the gamut of everything from accounting fraud to sexual harassment and

together. These tools can give an investigation team a quick sense of who the major players are and what happened.

- **Dark language detection** to identify code words or phrases that may indicate malfeasance. These tools can quickly and accurately pinpoint potential areas of concern so the investigation team doesn't waste time looking for suspicious conversations and can instead focus on the most likely suspects first.
- **Anomaly detection** to notice those moments when a pattern—be it a pattern of communication, financial transfers, or work hours—has changed, potentially indicating misconduct.

Regulatory investigations

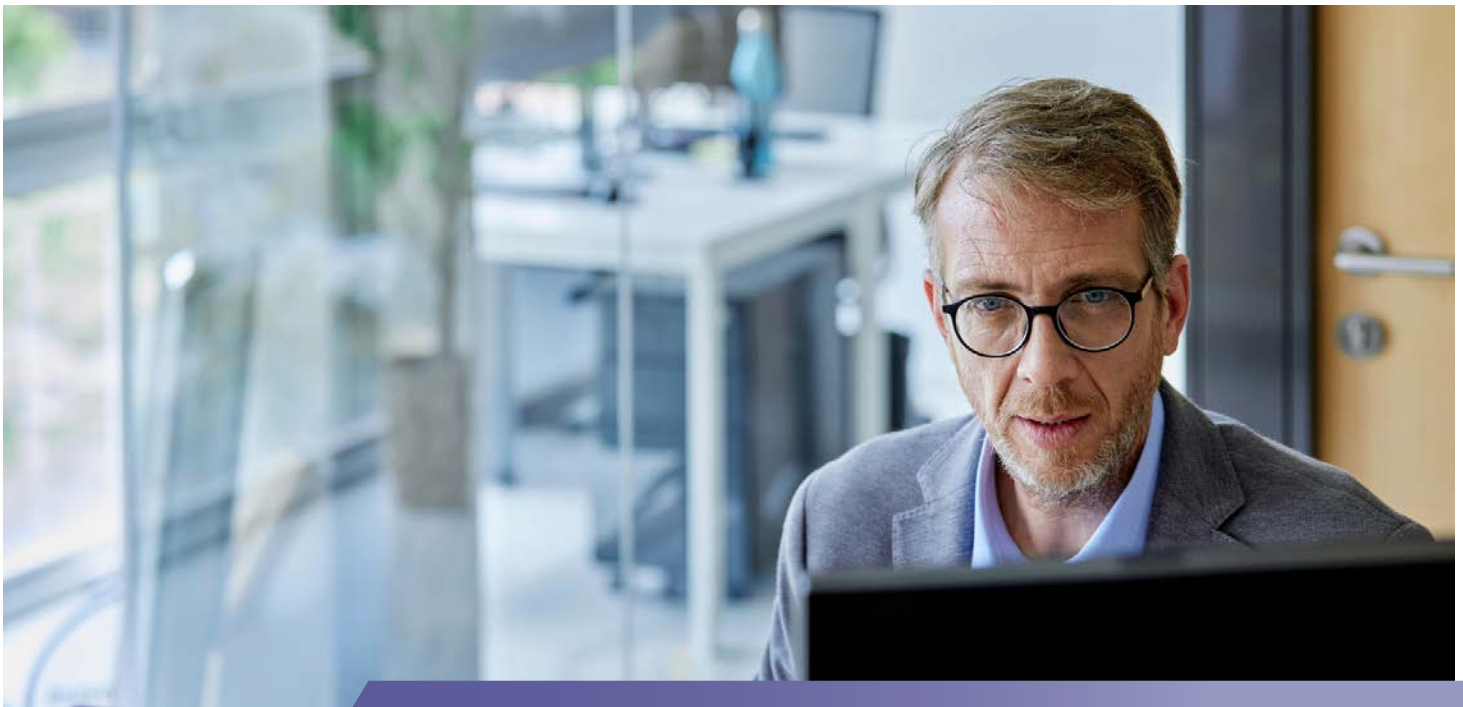
Regulatory agency investigations can take several forms, from investigations prompted by a whistleblower complaint, regulatory inquiries, and subpoenas to second requests in proposed mergers and acquisitions or more general government oversight into corporate compliance.

For all of these investigations, time is of the essence, and cooperation is critical.

Helpful technologies for government investigations include the following:

- **Data processing tools like deduplication and hashing** to eliminate duplicate files and irrelevant, unhelpful data sets even in the face of limited information about what exactly the agency is investigating.

- **Technology Assisted Review** to gain a broad sense of what the government's search parameters may reveal about its investigation within the tight timeline of a regulatory investigation.
- **Foreign language extraction and translation** to ensure that nothing is missed—even when it's written in a different language.



Conclusion

Unlocking the power of eDiscovery for efficient, effective investigations

Find out how adding eDiscovery tools to your investigative toolkit leads to better results.

Chances are your organization already has access to many of these tools and technologies as part of your eDiscovery toolkit. If you're not leveraging those tools in your investigations—or if the solutions you're using are too unwieldy or difficult to use in the rapid-fire pace of an investigation—now is the time to unlock the power of intuitive, accessible eDiscovery technology.

Investigations of all kinds are likely to rise as employees return to the office. Will you be ready?

Talk to a specialist!

IPRO's eDiscovery experts are standing by to help you improve your investigations, or to answer any lingering questions you may have.

[Request a demo](#)

[Ask a question →](#)



] IPRO

GOVERNANCE | INSIGHTS | DISCOVERY

The eDiscovery platform for legal fact-finding. Trusted by government, law firms and corporations.

Location

1700 N Desert Drive
Suite 101
Tempe, AZ 85281

Contact

www.ipro.com
info@ipro.com
+1.877.324.4776

Why IPRO? →

IPRO is reinventing the way organizations interact with their data. By transforming the EDRM and thinking “upstream” we bring insight far earlier in the eDiscovery process, enabling teams inside and outside your organization to collaborate transparently at any stage, before data is even collected. By thinking about and interacting with your data differently, you’ll eliminate waste and reduce risk.

© IPRO Technologies and/or its affiliates (“ZyLAB”).

No part of any IPRO blog, whitepaper, datasheet or any other marketing publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of IPRO. The information, data and content contained in such IPRO marketing publications is owned by IPRO and is subject to change without notice. IPRO assumes no responsibility for any errors that may appear.

IPRO DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event shall IPRO be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of these documents, even if advised of the possibility of such damages.