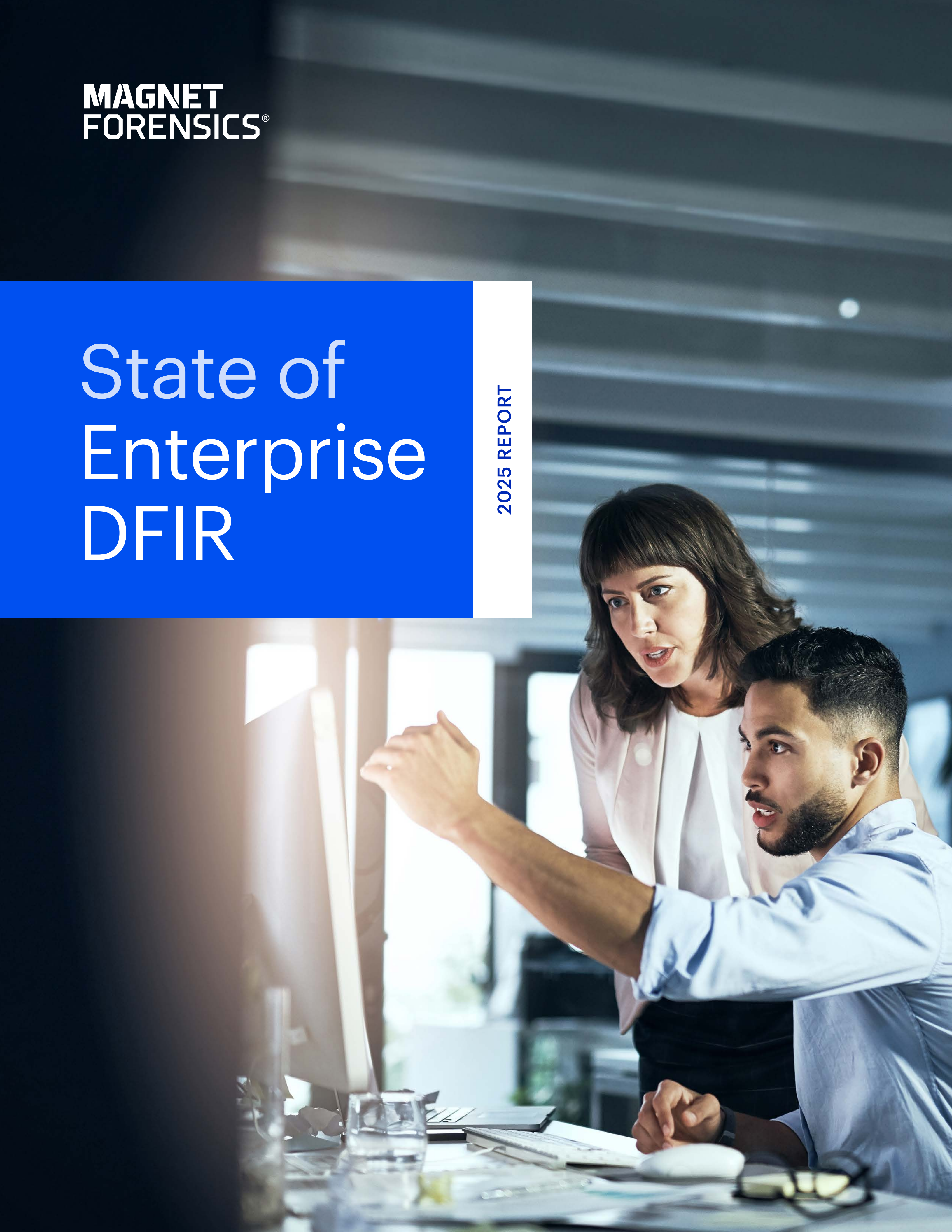
MAGNET FORENSICS®

State of Enterprise DFIR

2025 REPORT



Contents

Executive summary

This report, the fifth in our annual series, draws its insights from a comprehensive survey of private sector digital forensics and incident response (DFIR) professionals. Our aim is to provide information tailored to the needs of enterprise decision-makers—particularly those involved with IT, cybersecurity, and governance.

Taking a high-level view, the survey reveals four significant findings.

1

DFIR professionals bring a unique skill set to support essential corporate functions, namely:

Risk management: Cyber risk, internal matters, legal matters

Governance: Supporting regulatory compliance

However, while these areas strongly benefit from—or in some cases outright require—skills that only DFIR professionals have, survey responses suggest leadership may not fully appreciate this reality.

2

In a digital world where expansive IT environments, remote and hybrid work models, and BYOD policies are the norm, remote collection and multisource analysis capabilities are fundamental requirements.

Unfortunately, 71% of DFIR practitioners report that performing remote collection is problematic, hampering their ability to conduct efficient and effective investigations.

Similarly, respondents depend upon mobile collection more than ever before. But even as the number of devices increases and the value of the data they hold grows, DFIR professionals face an assortment of challenges gaining access to devices and performing the Full File System (FFS) extractions so crucial to investigations.

Modern tooling can address these remote collection and mobile extraction issues, but organizations need to equip their DFIR practitioners with these capabilities.

3

Keeping pace with technological change and well-resourced adversaries is already challenging enough, but DFIR practitioners also encounter internal obstacles.

Budgetary constraints, time-consuming repetitive tasks, and lack of access or permissions are common impediments and all are well within the organization's control.

Likewise, many respondents report several challenges when working with their colleagues in IT—especially when it comes to deploying and integrating new tooling.

Considering how important it is to keep a DFIR stack up to date, organizations would do well to address these very manageable internal issues.

4

Finally, the survey revealed that AI and SaaS are already transforming corporate digital forensics.

In just a year, the share of respondents who indicate they're actively using AI in their investigations jumped from 21% to 94%—a truly staggering increase.

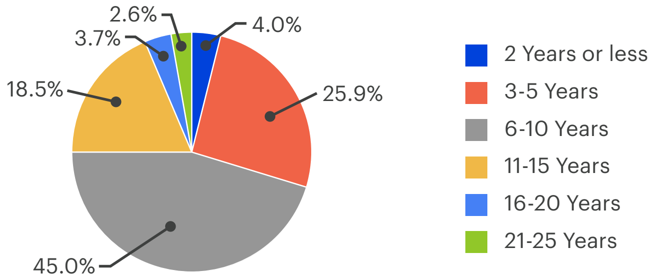
In a similar vein, 79% of respondents report already using SaaS-based digital forensics tools.

Clearly, the desire for improved efficiency, scalability, and flexibility outweighs concerns about integration hurdles and security.

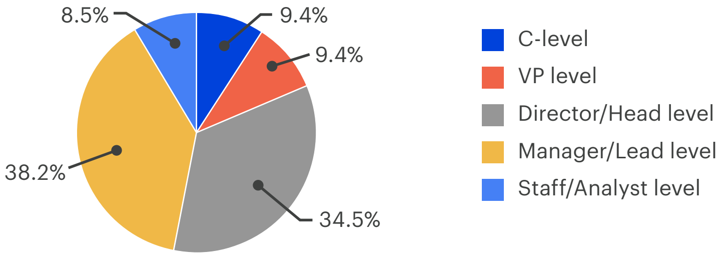
Survey demographics and methodology

This report is informed by a web-based survey of private sector digital forensics and incident response (DFIR) professionals and service providers conducted from September 11, 2024, to October 11, 2024. The 351 respondents who completed the survey represent a broad mix of organizations, workplace seniority, and domain experience. Their responses were aggregated anonymously to surface the insights revealed within this report.

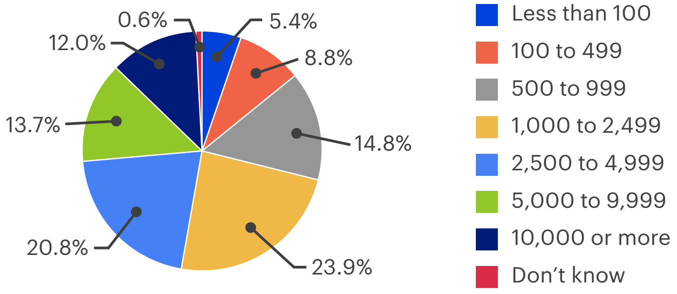
Respondents by DFIR experience



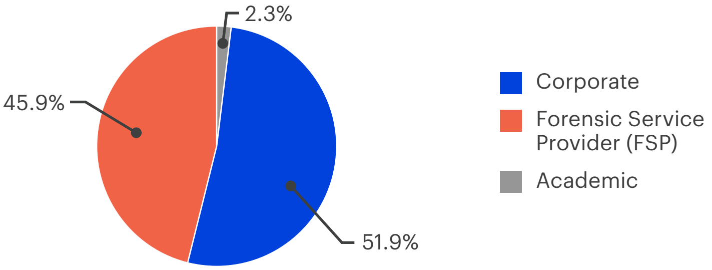
Respondents by workplace seniority



Respondents by organization employee count



Respondents by organization type



FINDING #1:

DFIR professionals are essential and uniquely skilled contributors to risk management and governance

- **The DFIR function is immensely valuable, but potentially overlooked and undervalued:** Today's corporate DFIR professionals divide their time between incident response, internal investigations, and supporting eDiscovery, bringing a unique skill set to these challenging, necessary, and highly valuable domains—but there are signs that organizations may be taking these contributions for granted.
- **DFIR supports regulatory compliance:** Phishing (including business email compromise) and malware-infected endpoints (including ransomware) are the two most frequent investigations; however, investigations relating to regulatory compliance are a close third—hinting at the important role DFIR plays in effective governance.
- **Third parties continue to provide value:** Consistent with prior findings, 49% of in-house respondents indicate their organization outsources at least some DFIR activities, primarily motivated by needing an impartial third-party review, an excessive volume of investigations, and cost-effectiveness.

Despite its wide-reaching impact, leadership may not recognize DFIR’s importance

> Many organizations view security as a cost center when it is actually an investment. A well-established DFIR team can return value to the organization by responding to security incidents quickly and efficiently, restoring services. It doesn’t matter if it’s an in-house team or a third-party. If they’re skilled, practiced, and using the right tools, these teams can truly bring value to the organization.”
>
> —
>
> **Ben Schommer**,
> CISO, Magnet Forensics

Digital forensics professionals have a unique skill set they leverage to support three broad categories of investigation: incident response, internal investigations, and supporting eDiscovery (Figure 1).

Continuing a trend documented in past editions of this report, survey respondents spend the largest portion of their time (43.6%) on incident response investigations. In this capacity, they help organizations to:

- Identify, contain, resolve, and recover from cyberattacks
- Prepare evidence that can be used to support cyber insurance claims, pursue legal avenues, and demonstrate duty of care to regulators
- Inform strategies and tactics to harden defenses against, and increase resilience to, future attacks

DFIR professionals’ ability to dig into the details, extract evidence, identify root causes, and reconstruct attacks—among other capabilities—will only grow in importance as organizations large and small continue to try to manage the everyday risks of cybercrime.

Time spent by investigation type

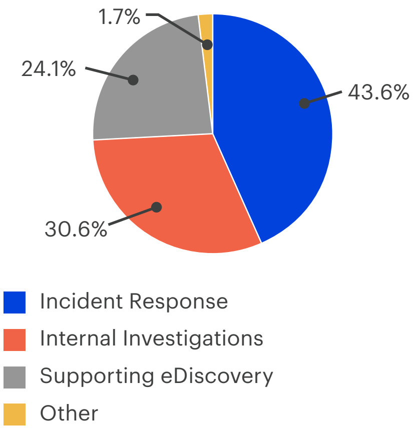


Figure 1: Please indicate the percentage of time you spend on the following investigations.

Internal investigations account for the second-largest portion of time (30.6%). These include human resources issues, policy violations, and asset misuse, and are essential for maintaining an organizational environment built on trust and respect—and for holding accountable those who violate these ideals.

The third major investigation category is supporting eDiscovery—essential for litigation and government-led investigations—which DFIR professionals report takes up 24.1% of their time.

Frankly, the knowledge and skills to perform these investigations in a forensically sound manner and to produce evidence that will withstand potential legal challenges cannot be found outside the DFIR community. Unfortunately, there’s enough perceived overlap and false equivalences that the unique capabilities, contributions, and, ultimately, value DFIR professionals provide may be overlooked.

83%

72%

72% of respondents agreed or strongly agreed with the statement that “My organization’s leadership recognizes the importance of DFIR”—down significantly from last year’s 83%.

Worryingly, there are signs some leaders are taking DFIR for granted. When asked to what degree they agreed with the statement “My organization’s leadership recognizes the importance of DFIR,” 72% of respondents somewhat or strongly agreed.

On the surface, this number is a welcome indicator that the DFIR community is held in high regard. However, it represents a statistically significant decline from last year’s 83%—and could portend decreasing awareness of just how much today’s organizations rely upon DFIR professionals.

Cyber incidents drive the most investigations, but regulatory compliance isn’t far behind

Looking more closely at investigation types (Figure 2), we see phishing (including business email compromise, or BEC) and malware-infected endpoints (including ransomware) once again top the list, consistent with last year’s report.

Their staying power—despite massive global spending on cyber defense and an impressive stream of law-enforcement takedowns—speaks to the strong motivations and dangerous capabilities of today’s threat actors.

Indeed, an ever-evolving array of tactics, techniques, and procedures (TTPs) make today’s attacks very difficult to detect, and all but ensure the ongoing need for state-of-the-art DFIR capabilities.

> In this year’s survey, we introduced two new options—regulatory compliance and mergers and acquisitions—to help account for the rich, varied, and evolving needs fulfilled by today’s corporate DFIR practitioners.

In third place—albeit just barely—is regulatory compliance. With many jurisdictions introducing **mandatory reporting requirements for cyber incidents**, we can expect DFIR’s contributions in this area to grow.

Moreover, it’s worth recognizing compliance activities extend well beyond those strictly associated with regulations. For example, in the previous section we noted DFIR supports insurance claims—both by providing evidence of malicious activity and by demonstrating an organization has lived up to their duty of care (and thereby qualifies for coverage).

Similarly, many certifications, standards, and contracts (e.g., with customers and vendors) also include requirements or provisions relating to digital controls. When conflicts or disagreements occur, it may fall on the corporate DFIR role to demonstrate such requirements or provisions were satisfied.

Specifics aside, two facts are clear:

1. Corporate DFIR professionals perform a wide range of investigations.
2. The range itself will continue to grow—as it always has—in response to evolving corporate needs.

Frequency of incidents (most to least)

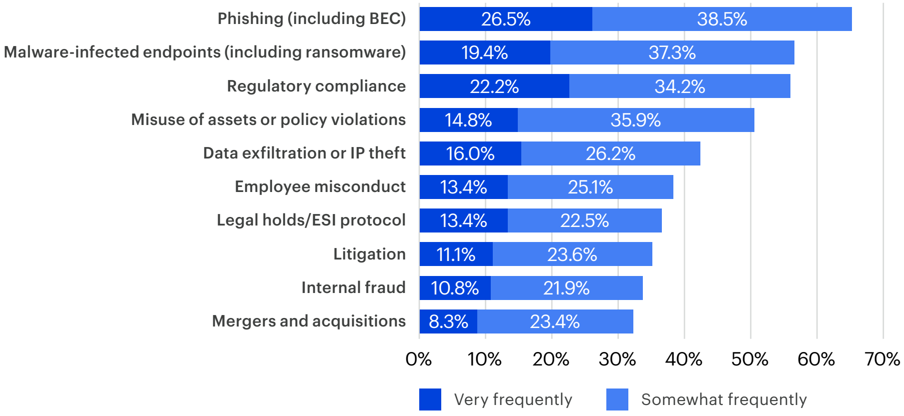


Figure 2: Please indicate how frequently your company/organization encounters the following types of investigations.

Third parties provide impartiality and cost-effectively augment in-house capabilities

Third parties capable of providing digital forensics services are an important part of the overall corporate DFIR landscape.

49%

of in-house respondents indicate their organization outsources at least some DFIR activities—a slight increase over last year's 44%.

Forensic Service Providers (FSPs) focus almost exclusively on digital forensics and offer a wide variety of tools and highly experienced practitioners.

Other organizations—including Managed Detection and Response (MDR) providers, those that provide a Security Operations Center as a service (SOCaaS), and the slightly more generalist Managed Security Service Providers (MSSPs)—offer forensics capabilities in the context of cybersecurity.

When asked why their organization turns to third parties, the top three reasons in-house respondents chose were the need for an impartial third-party review, an excessive volume of investigations, and cost-effectiveness (Figure 3).

Interestingly, when asked why corporate customers worked with them, third-party forensics providers had the same three reasons atop the list, but in the reverse order.

While opinions may differ slightly—with an ever-growing volume of investigations and an unavoidable need (in at least some investigations) for complete impartiality—it's abundantly clear corporations will continue to rely on third parties for DFIR services.

36%

of investigative work is estimated by in-house respondents to be performed by third-party service providers.

Reasons for using third-party service providers

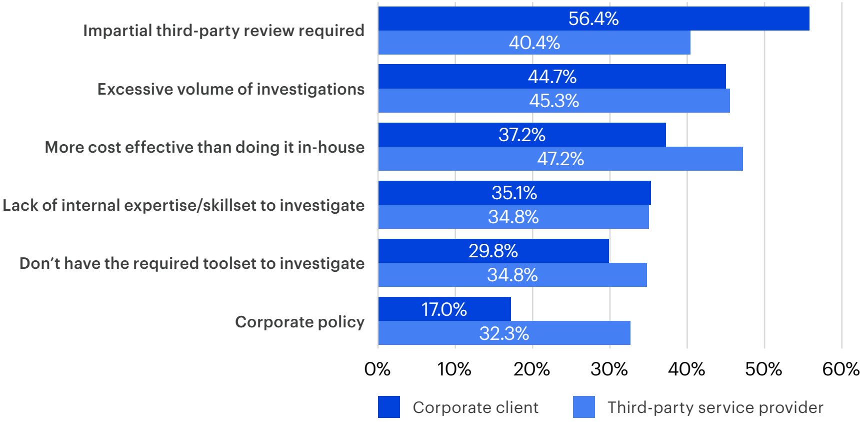
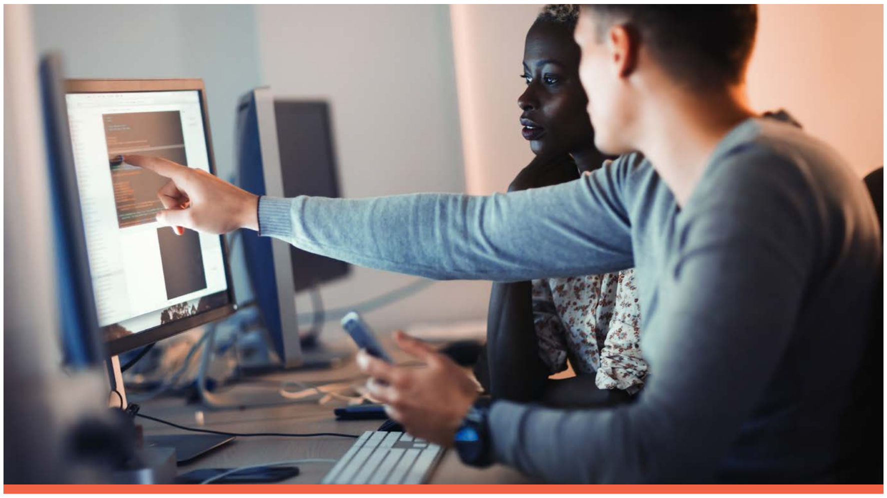


Figure 3: What are the main reasons that digital forensics investigations are outsourced to third parties?

FINDING #2:

Remote collection and multisource analysis are vital, but mobile devices present particular challenges



- **Remote collection is critical, but problematic:** Today's investigations draw upon a wide range of data sources, led by remotely collected computer data, but 71% of DFIR practitioners report remote collection is at least a moderate problem—one that's exacerbated by remote and hybrid work models.
- **Mobile devices matter more than ever before:** Consistent with last year's findings, two-thirds of respondents report the number of mobile devices in investigations is growing; additionally, 56% of respondents report always or often using data from mobile devices and tablets acquired through a forensic tool.
- **Mobile extractions are especially challenging:** DFIR professionals prefer Full File System (FFS) extractions over Logical extractions, but collecting data from mobile devices presents an assortment of challenges—leading 32% of respondents to report the growing number of mobile devices will make digital forensics more challenging in the future.

Remote collections remain essential in a world of hybrid work

For most organizations, digital transformation and growth are accompanied by more data, spread across more devices and data stores.

As a result, today's digital forensics professionals frequently work with computers, mobile devices, cloud data (e.g., software-as-a-service applications, cloud storage), and—albeit to a lesser extent—Internet-of-Things (IoT) devices.

59%

of respondents report either always or often using remote computer data acquired through a forensic tool in their investigations.

Consistent with last year's findings, survey respondents indicate they most frequently rely upon remote computer data acquired through a forensic tool in their investigations, with 59% reporting they always or often do so. This number just edges out mobile devices and tablets acquired through a forensic tool, at 56%.

64%

of respondents consider growth of the remote/hybrid workforce to be a moderate to extreme problem for investigations.

However, the evolution of the modern work environment is creating problems for DFIR practitioners. One large-scale change is the continually rising number of mobile devices; another is the adoption of remote and hybrid work models.

Both trends can prevent investigators from having physical access to a device.

We'll have more to say about forensic tooling in a few pages, but for now we'll simply highlight that the ability to perform remote collections—already a valuable feature of any primary forensic tool—is growing in importance.

71%

of respondents consider difficulty acquiring from remote and/or off-network endpoints to be a moderate to extreme problem for investigations.

> In the DFIR world, a reliable remote collection solution that can seamlessly pause and resume collections as endpoints become available revolutionizes the investigative process by eliminating the need for physical access to devices. This capability reduces delays and minimizes the need for travel, enabling faster results while maintaining precision in handling critical digital data."
>
> —
> **Jeff Rutherford**,
> Forensic Consultant

Mobile devices provide essential evidence, but collection challenges are common

Consistent with last year's report, the majority (65.5%) of survey respondents indicated the number of mobile devices in investigations is increasing (Figure 4).

Along those same lines, 56% reported always or often using data from mobile devices and tablets acquired through a forensic tool in their investigations.

There are several reasons why mobile devices are growing in importance as evidence sources, but perhaps the main reason is the most obvious: people use their phones (and, to a lesser extent, their tablets) for everything.

The number of mobile devices in investigations...

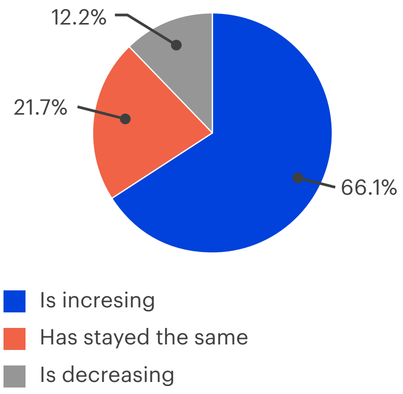


Figure 4: The number of mobile devices in investigations is...

Consequently, a mobile device may hold information relating to communications (e.g., email and instant messaging), calendars, the user's whereabouts, web activity—and much more.

As a result, mobile devices can be difference-making data sources for a range of investigation types, including fraud, intellectual property theft, policy violations, litigation support, insurance investigations, and eDiscovery.

56%

of respondents report always or often using data from mobile devices and tablets acquired through a forensic tool in their investigations.

Mobile devices can also offer threat actors an attractive combination of privileged access to protected environments and corporate data, with fewer and less restrictive security controls. Consider that:

- The vast majority of organizations have gone the bring-your-own-device (BYOD) route for mobile devices, but
- Fewer than half of companies with a BYOD policy also employ a mobile device management (MDM) solution

This permissiveness creates an opportunity for malicious activities, whether conducted willfully by the device owner or by an adversarial third party that has successfully compromised the device.

Why cloud data alone isn't enough

While cloud backups of mobile devices (e.g., iCloud for iPhones) are a good start, they should not be considered a substitute for direct device extractions or other data sources, for the simple reason that these backups often exclude important artifacts such as:

- Non-iTunes media files and unsupported app data
- Touch ID, Face ID, and Apple Pay settings
- Unencrypted Activity, Health, and Keychain data
- Deleted data, system logs, and network usage logs
- Temporary files and detailed app-specific data

When considering incorporating cloud backups into collections, be mindful that:

- Encryption affects data included in backups
- Synced data (e.g., iCloud Photos) is stored separately from backups
- Backup scope may be limited by cloud storage space

A comprehensive and detailed data extraction can provide investigators with critical evidence and information, so it's not surprising the majority (68%) of respondents prefer to perform Full File System (FFS) extractions over Logical extractions.

While a Logical extraction is faster, it's limited to the subset of data available through the device's operating system. In contrast, FFS provides a complete copy of all data stored on a mobile device. The accompanying Keychain or Keystore files allow the extraction of application database files, giving the examiner the ability to:

- Recover deleted artifacts
- Manually parse artifacts for unsupported applications
- Decrypt encrypted artifacts and end-to-end encryption communication applications

However, there's a severe disconnect between what investigators want to do and what they're able to do (Figure 5):

- Nearly half (49.9%) of respondents reported the challenge of limited data extracted from the device
- 43% reported that access and extraction take too much time

But before DFIR practitioners can encounter and address data extraction issues, they must first overcome:

- An inability to collect from devices remotely (46.7%)
- An inability to gain access to the device (41.3%)

Unfortunately, while mobile devices can represent a veritable gold mine for investigators, acquiring data from these sources isn't easy and typically requires highly specialized digital forensics tools.

Perhaps these reasons are why nearly a third of respondents expect the growing number of mobile devices to make digital forensics even more challenging than it is already.

32%

of respondents indicated the growing number of mobile devices will make digital forensics more challenging in the future—up from 26% in last year's report.

Challenges with mobile collection and analysis (most common to least common)

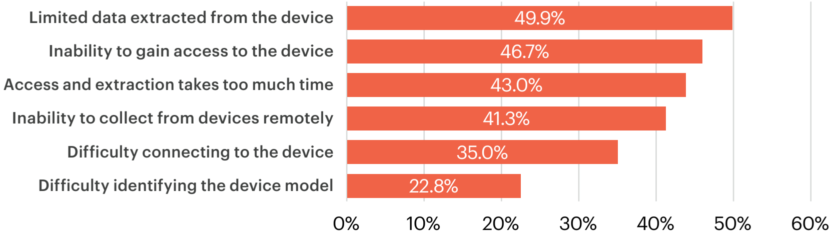
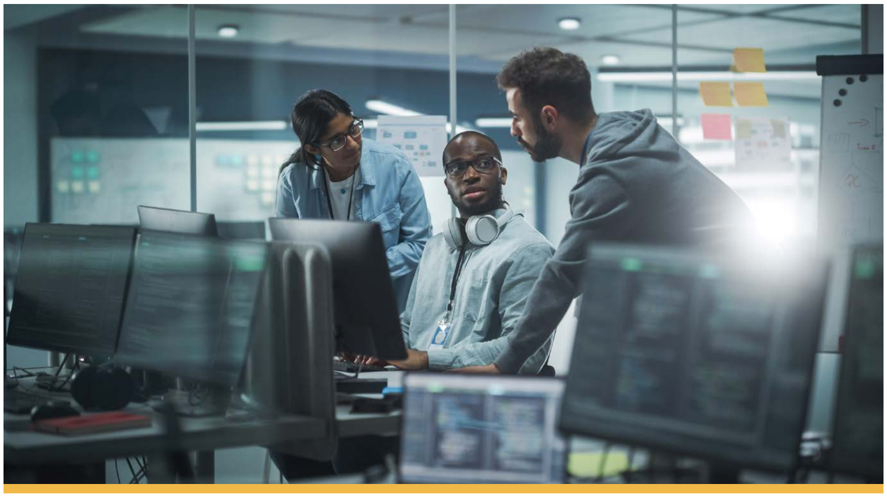


Figure 5: What challenges have you experienced with mobile collections and analysis?

3

FINDING #3:

DFIR practitioners face unnecessary internal obstacles



- **Many common challenges are internal:** For the third year in a row, evolving cyberattack techniques are the largest challenge to investigations; however, respondents also reported problems due to budgetary constraints, time-consuming repetitive tasks, and lack of access or permissions.
- **More integration between tools is needed:** To enable effective and efficient investigations, it's crucial DFIR professionals are equipped with modern tooling that can collect data from a range of sources—but many are forced to use multiple tools that are poorly integrated, which lengthens investigations and contributes to burnout.
- **Greater cooperation and coordination with IT is needed:** The majority of respondents reported that working with IT is at least moderately challenging—with the most commonly cited problem pertaining to integrating new forensics solutions with existing systems.

Evolving cyberattack techniques remain the largest problem for investigations

In recent years, many organizations have invested in stronger cyber defenses—including vulnerability management programs, security operations, stricter Identity and Access Management (IAM) configurations, and cloud defenses. Threat actors have responded with TTPs that make it especially hard to detect, contain, and investigate their intrusions. Two of the most notable developments are the combined use of infostealers and stolen credentials, and living-off-the-land techniques.

3 years

This is the third consecutive report in which evolving cyberattack techniques emerged as the largest challenge.

It's not especially shocking, then, that respondents indicated evolving cyberattack techniques continue as the trend that poses the greatest challenge to their investigations (Figure 6).

Of course, what adversaries do is beyond an organization's control; however, DFIR practitioners also report several common challenges that can be addressed directly.

For example, budgetary constraints (selected by 41% of respondents), time-consuming repetitive tasks (39.6%), not having the right access or permissions to acquire data (35.4%), and too many tools that are not integrated with each other (34.2%) all have available solutions.

Unfortunately, the percentage of respondents agreeing with the statement, *"Our DFIR professionals are equipped with the resources needed to be successful"* has declined significantly year-over-year, from 77% to 68%.

77% ︾ 68%

68% of respondents agreed or strongly agreed with the statement, "Our DFIR professionals are equipped with the resources needed to be successful"—down significantly from last year's 77%.

Leadership needs to recognize DFIR capabilities must continually evolve to keep up with investigative needs, and policies must permit practitioners to do their jobs, otherwise effectiveness and efficiency will decline.

> "
> Having the right toolset is imperative for responding effectively to today's incident scenarios. By integrating tools like the MITRE ATT&CK® framework, and Sigma and YARA rules, analysts can collaborate with the global security community to systematically enhance detection capabilities and expedite root cause analysis."
>
> —
> **Doug Metz**,
> Senior Security
> Forensics Specialist

Investigation challenges (largest to smallest)

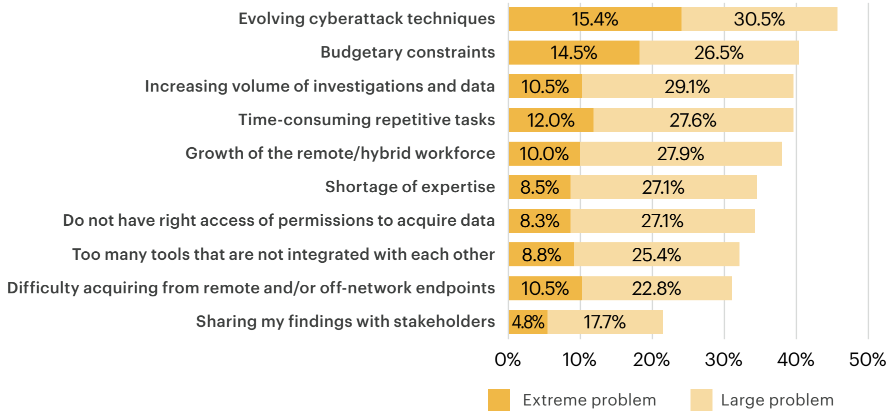


Figure 6: Please indicate to what degree the following potential challenges are problematic for your investigations, overall.

A piecemeal approach to collection hampers investigations and contributes to burnout

If a DFIR function were to be built from scratch, practitioners could choose a modern, open platform that not only extracts from and correlate across multiple sources, but also easily integrates with other systems.

However, the majority of DFIR technology stacks have been built incrementally over time—often resulting in a collection of specialized legacy tools coexisting with more modern options.

39%

of respondents agreed or strongly agreed with the statement, *"I am feeling burnt out in my job,"* a worrying increase over last year's already high 34%.

Unfortunately, while using multiple tools can expand a practitioner's collection and analysis options, it also has drawbacks. Survey respondents point to five interrelated challenges, in particular:

1. Extends the duration of investigations
2. Difficulty integrating data from multiple sources
3. Difficulty correlating between different tool outputs
4. Lack of integrated reporting
5. Increased likelihood of burnout

In this context, it's not surprising respondents from the corporate ranks and from forensic service providers both consider the ability to collect from many sources to be the most important feature in a primary forensic tool (Table 1).

The value of being able to collect from many data sources is underscored by the fact that although corporate practitioners and third-party service providers agree on this top feature, they have divergent opinions elsewhere.

Corporate practitioners prioritize ease of use, automation, interoperability, and remote collection—whereas respondents from service providers favor analysis of all evidence in one case file, remote collection, ease of use, and the ability to perform most of the workflow with one tool.

51%

of respondents report using a digital forensics automation solution to integrate multiple tools during an investigation.

These differences demonstrate that the needs of DFIR practitioners vary based upon their operating context. Accordingly, any initiatives aimed at expanding or otherwise altering the DFIR stack must include the practitioners themselves.

Corporate DFIR rank	Feature	Service provider rank
#1	Collect from many data sources	#1
#2 (tie)	Easy to use	#4 (tie)
#2 (tie)	Automation of repetitive tasks	#6 (tie)
#5 (tie)	Remote collection	#3
#8	Analysis of all evidence in one case file	#2
#4	Interoperability with other tools	#11
#11	Perform majority of workflow with one tool	#4 (tie)

Table 1: Ranking of capabilities considered "most important" in their primary forensic tool (listed in order of importance by all respondents)

IT challenges are impeding DFIR functions

> By fostering open dialogue and having routine knowledge-sharing exercises, digital forensics and IT teams can create a formidable alliance against both internal and external threats for organizations, but only if they work together."
>
> —
>
> **Trey Amick**,
> Director,
> Technical Marketing
> & Forensic Consultants

> Joint communications and shared responsibility is important. Corporate IT is an enabler for the business, and DFIR should be regarded as a critical business function. In reality, it's about ensuring all systems can support the DFIR function in line with broader business needs. To ensure this alignment, it should be written into SOPs and policies as a mandate."
>
> —
>
> **Gavin Hornsey**,
> Senior Solutions Consultant

DFIR platforms and tools are, fundamentally, information technologies—and acquiring, implementing, and integrating them typically involves the IT team in one way or another.

Alarmingly, though, a majority of respondents (58%) indicated they found working with IT to be at least a moderate challenge.

58%

of respondents indicated that working with IT is at least moderately challenging.

By far the most-cited challenge pertains to integrating a new solution with existing systems (Figure 7).

Integration is essential for enabling effective and efficient investigations, so it's worrisome that not only are DFIR professionals often forced to use legacy tools with comparatively limited integration options, but they also encounter friction when working with IT to integrate new solutions.

The IT department is ultimately responsible and accountable for the health of the organization's overall technology stack and environment, so any concerns they're raising should be presumed to have merit. However, the survey findings suggest there's considerable room for improved cooperation between teams.

Challenges encountered working with IT (most common to least common)

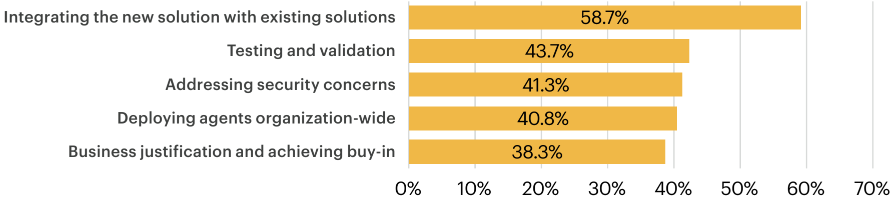
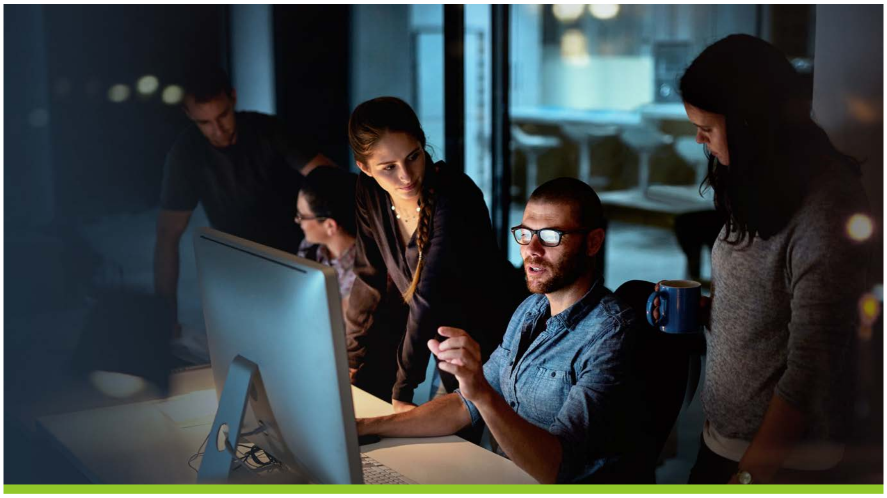


Figure 7: You mentioned in the previous question that you found the challenge of working with IT to adopt or deploy forensics security software at least a moderate problem. What in particular did you find challenging?

4

FINDING #4:

AI and SaaS are already transforming corporate digital forensics



- **AI has arrived in a big way:** 94% of respondents indicated they are already using AI in some way to aid with their investigations (a truly extraordinary jump over last year's 21%), most commonly to classify data and to analyze text and images.
- **AI is perceived as a double-edged sword:** 51% of respondents regard advances in AI capabilities as being beneficial for corporate DFIR, topping the list of beneficial trends; in dark-mirror fashion, those same AI advances also topped the list of trends that will make DFIR more challenging (selected by 56% of respondents).
- **The benefits of SaaS outweigh perceived obstacles:** 79% of respondents indicated they are already using SaaS-based digital forensic tools, most frequently citing improved efficiency, scalability, and flexibility as their motivations.

Adopted seemingly overnight, artificial intelligence is already improving investigations

As context, let’s start with a few data points from last year’s report:

- 47.8% of respondents regarded AI as the trend that will most help DFIR
- 91% of respondents were open to using AI to improve DFIR efficiency
- Only 21.4% had already purchased or were already using AI

Fast forward just 12 months and we have what might be the single most significant finding from this year’s survey: 94% of respondents are already using AI in some way to aid with their investigations.

As Figure 8 shows, the most common uses of AI with today’s corporate DFIR practitioners are high-accuracy data classification (selected by 64.7% of those who are already using AI) and analyzing text and images (60.5%).

Manually classifying and analyzing vast amounts of data can be extraordinarily tedious and time consuming, so applying AI has the potential both to improve quality and meaningfully expedite investigations.

94%

of respondents indicated they are already using AI in some way to aid their investigations.

It’s clear, though, that corporate DFIR professionals believe AI has even more to offer, as roughly half of respondents overall (i.e., whether or not they’re already using AI) indicated advances in AI represent the trend that will be most beneficial to digital forensics.

51%

of respondents indicated advances in AI represent the trend that will be most beneficial to digital forensics.

However, AI can also be put to malicious use by threat actors, for example to probe for vulnerabilities, develop exploits, craft convincing phishing lures, and—through image, audio, and video deepfakes—convincingly mimic team members. As a result, while AI topped the list of beneficial trends, it also topped the list of trends that will make digital forensics more challenging (selected by 56% of respondents).

For good and bad, AI’s influence on corporate DFIR is only in its infancy.

Top uses of AI in investigations

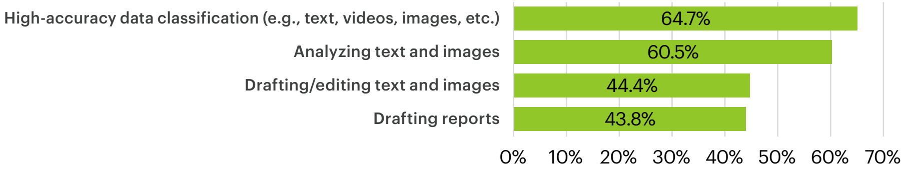
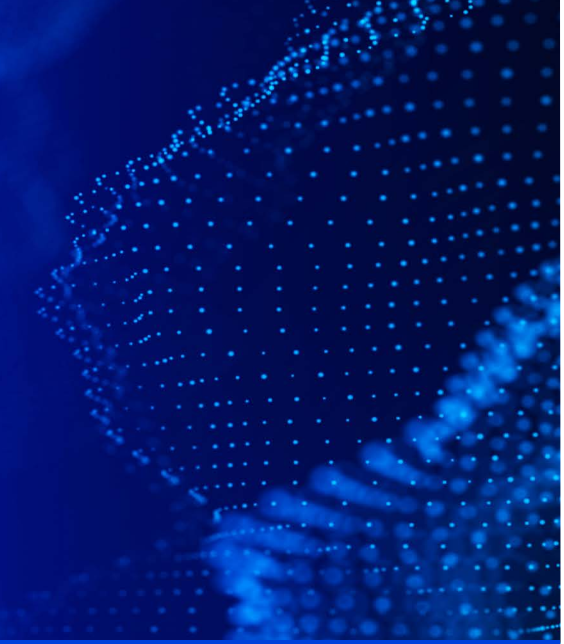


Figure 8: What are you using AI for in your investigations?



Magnet Forensics’ approach to AI

Magnet Forensics’ digital investigation solutions go beyond simple data recovery by incorporating AI to efficiently surface insights from any data source so you can get to the truth faster and confidently validate your findings in one click with links back to source data. With our AI solution for DFIR, Magnet Copilot, you can sift through vast amounts of data, quickly identify relevant details, and generate comprehensive reports. To learn more about Magnet Copilot, visit **magnetforensics.com**.

The vast majority of corporate DFIR practitioners already use SaaS-based tools

AI isn't the only technological trend transforming how organizations and their employees operate—the software-as-a-service (SaaS) model has also exerted a large influence on technology stacks around the world.

It's apparent the DFIR stack isn't immune to this transformation, as 79% of survey respondents indicated they are already using SaaS-based digital forensic tools. The leading reasons behind their adoption (Figure 9) are for improved efficiency, scalability, and flexibility—all of which are vitally important for an effective DFIR solution.

79%

of respondents indicated they are already using SaaS-based digital forensic tools.

Of course, change rarely comes without at least some friction, and adopters of SaaS-based digital forensic tools report challenges in integrating them with other systems, addressing data security and privacy concerns, and securing support from IT (Figure 10). Again, we see the recurring importance of integration and IT's role in equipping DFIR practitioners with modern tooling.

What's holding back the other 21% of organizations from adopting SaaS-based digital forensic tools? By far the most common barriers cited by survey respondents are budget restrictions and security concerns—although it's interesting to note more than 40% of respondents who adopted these tools did so at least partially to reduce costs.

Clearly, SaaS has already changed corporate DFIR, and we suspect what's happened so far is just the beginning.

Reasons for adopting SaaS-based digital forensics tools

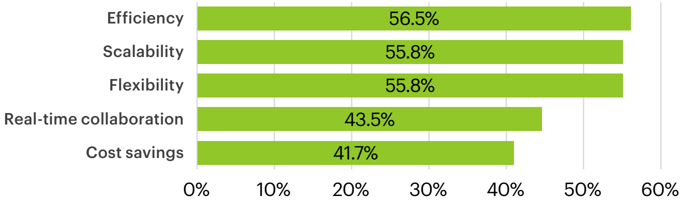


Figure 9: Why did you adopt a SaaS-based solution for your investigations?

Challenges encountered adopoting SaaS-based digital forensics tools

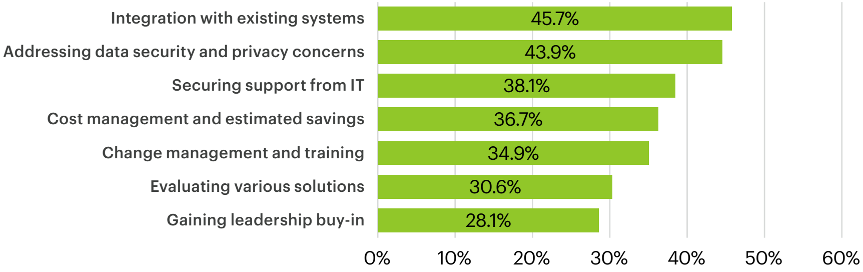


Figure 10: What were the most difficult parts of adopting a SaaS-solution for your investigations?

Conclusion and recommendations

DFIR continues to evolve in response to changing demands—but practitioners can't do it alone.

Recognize DFIR professionals make important and irreplaceable contributions to many important areas

DFIR in corporate environments largely began with investigations relating to internal matters. Over time, as cybersecurity took on greater importance, practitioners' specialized skills were applied to root cause analysis and preservation of evidence. DFIR professionals continue to meet the organization's needs in both these areas—and many others. In recent years, as data governance has risen in prominence, leaders tapped the DFIR function to support regulatory compliance and other obligations.

However, for reasons both obvious and subtle, DFIR professionals often operate behind the scenes. One consequence of this is that their significant contributions can be overlooked. DFIR is a highly specialized field that combines technical knowledge, investigative skills, intuition, and tenacity. Finding experienced professionals is always a challenge, so leaders should recognize and value the personnel they already have.

Equip your DFIR professionals with the tools they need

Like the rest of the IT environment, the DFIR technology stack is never complete. It must change with the times, so practitioners have the tools they need to extract and analyze ever-increasing volumes of data from a myriad of sources. In many cases, investigators lack physical access to the devices from which they need to collect data, making remote collection capabilities especially vital. Similarly, investigators frequently need to collect from mobile devices, yet they routinely encounter challenges when trying to do so.

Modern tooling can help address these shortcomings, ensuring an organization's DFIR function can keep pace with evolving needs. However, it isn't enough merely to acquire new tools—they also need to be integrated such that they can be efficiently incorporated into existing workflows.

Identify and address internal challenges

Many factors are beyond an organization's control or influence. Yet many problems can be overcome with sufficient prioritization.

Budgetary constraints can be addressed by regarding DFIR as an investment in risk management and governance, not a cost. Time-consuming repetitive tasks can be tackled through automation and integration. A lack of access or permissions largely comes down to policy. Similarly, many DFIR professionals report challenges working with their IT department—despite everyone being on the same team.

Not addressing these issues is a choice—one that has significant consequences.

Understand that while technology can be transformative, people matter more

An efficient and effective DFIR function requires a mix of people, processes, and technologies in equal measure.

Advances in technology—most prominently in AI, SaaS, and automation—surely enable greater efficiencies and effectiveness. But it's important to recognize these advances exist to aid the human experts who bring their experience, skills, and intuition to the task at hand.

To get the most out of technology investments, organizations should take direction from their DFIR practitioners and consult their IT department to ensure deployment and integration aren't overlooked.

Contributors

This year's State of Enterprise DFIR report featured contributions from an experienced team of Magnet Forensics DFIR experts. Magnet Forensics is proud to count a large number of former digital forensic examiners and DFIR professionals, from both the public safety and enterprise sectors, as members of the team—providing a wealth of valuable knowledge and insights and shaping everything we do.

Trey Amick
Director,
Technical Marketing
& Forensic Consultants

Trey Amick is a forensics investigator with a background in both law enforcement and corporate investigations. As a detective with the Rock Hill Police Department in South Carolina, Trey was sworn as a Special Deputy United States Marshal and supported the U.S. Secret Service Electronic Crimes Task Force. Previously, he served in roles in both Patrol and Professional Standards. Most recently, as a corporate investigator, Trey managed the Enterprise Cyber Education and Awareness Team at Capital One, where he also served as part of the Cyber Technical Investigations Team.

Jeff Rutherford
Forensic Consultant

Jeff Rutherford was a Supervisory Special Agent with the Federal Bureau of Investigation with experience in Organized Crime, Crimes Against Children, Counter Terrorism, and Cyber-related investigations. Jeff joined the FBI in 2003, retiring in 2024. Jeff achieved specialized certification as a Technically Trained Agent and an FBI Certified Digital Forensic Examiner. Jeff holds certifications from IACIS (CFCE) and SANS (GCFA). Jeff has testified in both state and federal courts. While assigned to the North Texas Regional Computer Forensic Laboratory, Jeff conducted digital forensic examinations for various agencies (state, local, and federal) across North Texas. Jeff led the FBI Dallas Technical Operations Squad responsible for the capture, processing, and preservation of electronic surveillance evidence. In 2024, Jeff joined Magnet Forensics as a Forensic Consultant.

Contributors

Doug Metz
Senior Security
Forensics Specialist

Doug Metz is a Senior Security Forensics Specialist at Magnet Forensics. He joined Magnet in 2021, bringing over 13 years of experience as an Incident Response Manager. Doug currently serves as Vice President for the Delaware Valley Philadelphia chapter of the HTCIA. Doug blogs at **BakerStreetForensics.com** and hosts the "**Cyber Unpacked**" webcast, exploring topics in Digital Forensics and Incident Response for the Enterprise.

Gavin Hornsey
Senior Solutions Consultant

Gavin began his career in IT in 2003, a career that included systems administration, storage and backup engineering, and digital forensics—with experience in both public and private sectors. Having served eight years with the South Wales Police Digital Forensic and Cyber Crime Unit (DFCCU) in the capacity of expert witness while also being responsible for lab IT infrastructure, Gavin moved into storage before joining Magnet Forensics as a Consultant in Professional Services between 2019-2022. After a short spell consulting in the data management and protection field, he returned to Magnet Forensics in 2023 as a Solutions Consultant.

Tarah Ward
Senior Solutions Consultant

Tarah Ward, MCFE, GCFA, is a former digital forensics examiner with a background in the US Federal Government, supporting agencies focused on counterterrorism, cyber defense, and incident response. Her responsibilities included forensic lab management and conducting digital forensic investigations in both the US and overseas, completing two deployments to Afghanistan. She holds a BS in Digital Forensics from Bloomsburg University of Pennsylvania. Tarah is currently a Senior Solutions Consultant at Magnet Forensics where she provides support to customers with her combined knowledge of digital forensics and Magnet solutions.

About Magnet Forensics

Founded in 2010, Magnet Forensics is a developer of digital investigation solutions that acquire, analyze, report on, and manage evidence from digital sources, including mobile devices, computers, IoT devices, and cloud services. Magnet Forensics products are used by more than 4,000 public and private sector customers in more than 90 countries and help investigators fight crime, protect assets, and guard national security.

LEARN MORE

MAGNET AXIOM CYBER™

Magnet Axiom Cyber is a robust digital forensics and incident response solution for organizations that need to remotely acquire and analyze evidence from computers, cloud, IoT, and mobile devices.

MAGNET NEXUS™

Magnet Nexus is a remote endpoint collection and analysis solution built to save you time and to get you forensic insights faster. Generate immediate insights with real-time artifact hits, simultaneously collect and process data from multiple endpoints with a dynamically scalable solution, and collaborate from case setup to artifact tagging and analysis.

MAGNET VERAKEY™

Gaining access to business-critical communications and data on mobile devices is crucial to protecting your organization and employees. Magnet Verakey is a consent-based mobile forensics solution that is easy to use, comprehensive, and fast.

MAGNET AUTOMATE™

Harness the power of automation to unlock lab capacity, empower your experts, and finish digital investigations faster. Magnet Automate enables you to automate the processes and tools that already work in your lab to reduce manual tasks, focus your team's efforts, and reduce time to evidence.

MAGNET REVIEW®

Securely collaborate on digital investigations from anywhere in the world. Magnet Review is designed to address the needs of examiners, non-technical reviewers, and other stakeholders, helping them to work together to quickly and easily find the evidence they need.

Thank you for reading this year's report!
Share your feedback in this quick
2-minute survey >>

This report is current as of the initial date of publication and may be changed by Magnet Forensics at any time without notice. The information contained in this report is for general informational purposes only, and provided "AS IS", without any representations or warranties, express or implied. Magnet Forensics does not accept responsibility for any omission, error, or inaccuracy in the report or any action taken in reliance thereon.

MAGNET FORENSICS®