RESEARCH AND ANALYSIS BY:

IDC

MAGNET FORENSICS®

STATE OF ENTERPRISE DFIR

2022 REPORT

Table of Contents

Analyst:

Ryan O'Leary
Research Manager, Privacy and Legal Technology, IDC

Executive Summary

Digital forensics and incident response (DFIR) teams are currently experiencing a fundamental shift. The cyberthreat landscape is evolving rapidly as bad actors discover new ways to breach security perimeters. Insider threats are also greater than ever; and some modern tactics, such as zero-trust environments, simply aren't designed to protect against a maliciously acting insider.

Data volumes alone create a significant problem for DFIR teams. As of 2020, the world was creating 59 ZBs a year and storing 4.2 ZBs according to IDC's Global Datasphere. DFIR professionals are dealing with the largest amount of data in history, data that they have to sift through to find evidence they need for their investigations.

Hybrid and remote work are now the norm for the foreseeable future and the volume of audio and video files are expanding with the shift to remote meetings. All of these forces come together and create a dynamic new environment that everyone, including DFIR professionals, must adapt to.

This annual report is about the current state of digital forensics and incident response for today's enterprises, corporations, and forensic service providers. The aim of this report is to provide market-driven and research-based insight to leaders who are making decisions for their DFIR labs so they can best prepare themselves and their teams for change.

The findings presented are based on a survey conducted by Magnet Forensics in collaboration with IDC which explore the current state of DFIR within the context of the macroeconomic forces surrounding enterprise technology. Readers should be able to evaluate their lab and technology based on the benchmarking reported by their peers to effectively plan for the future.

This report highlights:

- **How DFIR teams have been impacted by hybrid work and data volume growth**
- **The state of DFIR within financial services, healthcare, and technology sectors**
- **The most concerning security threats now and in the future**
- **The size, organizational placement, and resource needs of DFIR teams**

Survey Overview and Demographics

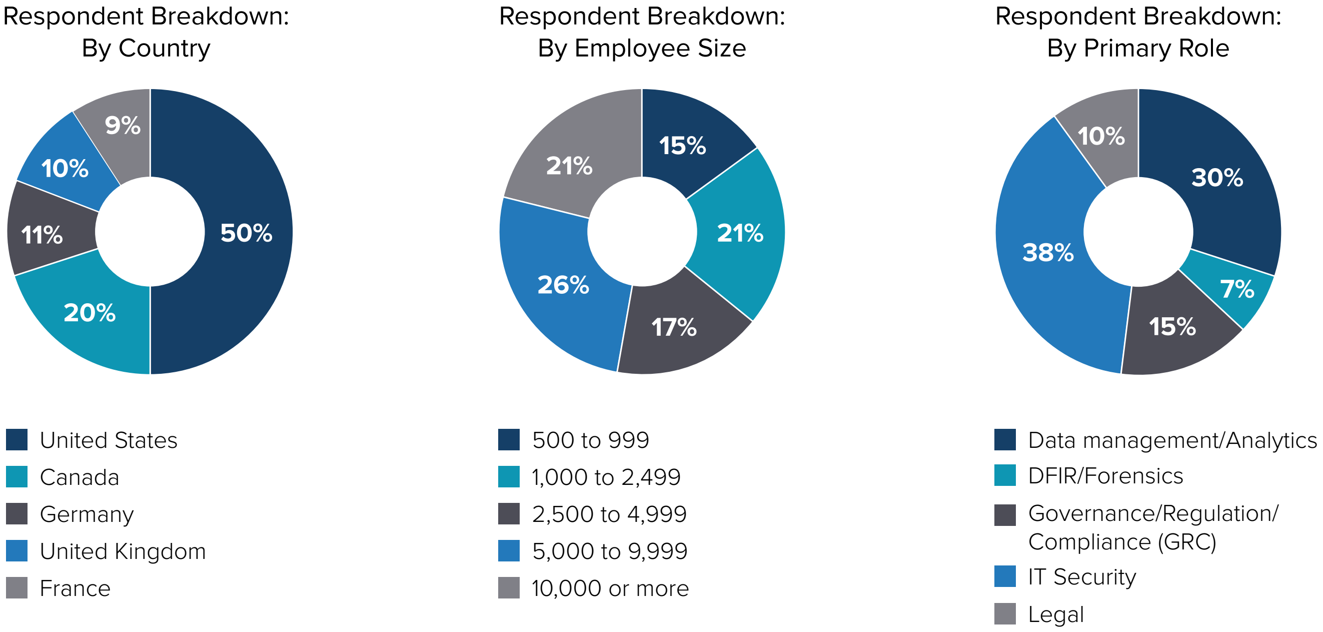
The web-based survey was completed by 466 respondents from September 15th, 2021 to October 15th, 2021.

The survey targeted North American and Western European DFIR teams; **50% of the respondents were employed within the United States, 20% were from Canada, and the remaining 30% from the U.K., Germany, and France**.

The respondents were from organizations with 500 or more employees across a broad range of industries.

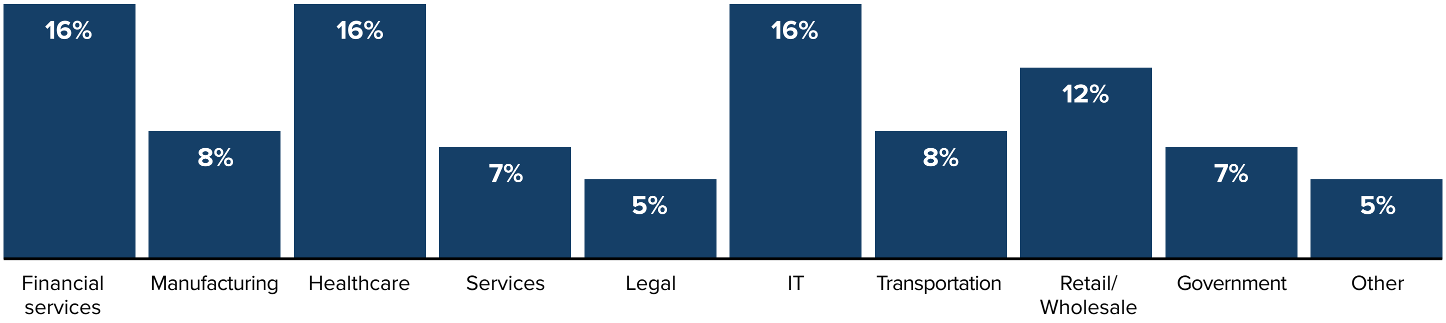
FIGURE 1

Firmographics (% of respondents)



Sample size (n) = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Respondent Breakdown:
By Industry



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Finally, the study ensured that respondents spent at least some of their time each week engaged in digital forensics activities and had some influence over DFIR technology purchase decisions. On average, respondents spent approximately 13 hours per week on forensics activities, and close to half of the respondents influence purchase decisions.

FIGURE 2
Purchase Influence (% of respondents)

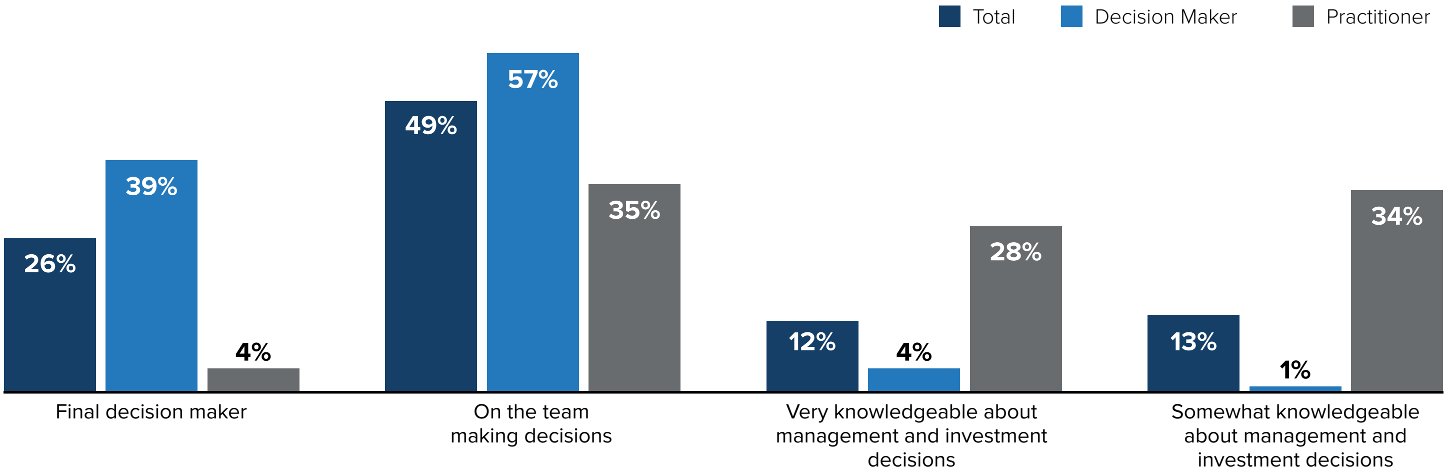
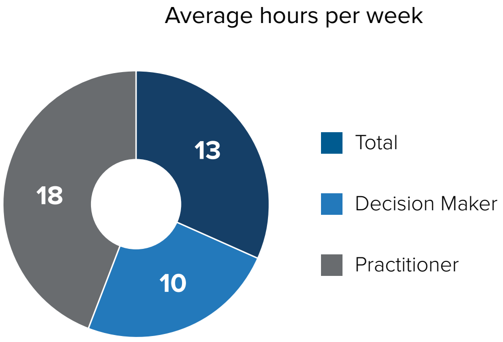


FIGURE 3
DFIR Focus



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Hybrid Work and the Data Explosion

Not only is the volume of investigations increasing but their complexity and diversity is increasing. While remote and hybrid work existed in a pre-pandemic world, things changed drastically in March 2020; and the seemingly overnight closure of offices and continued closure of offices worldwide has irrevocably changed the way the world works.

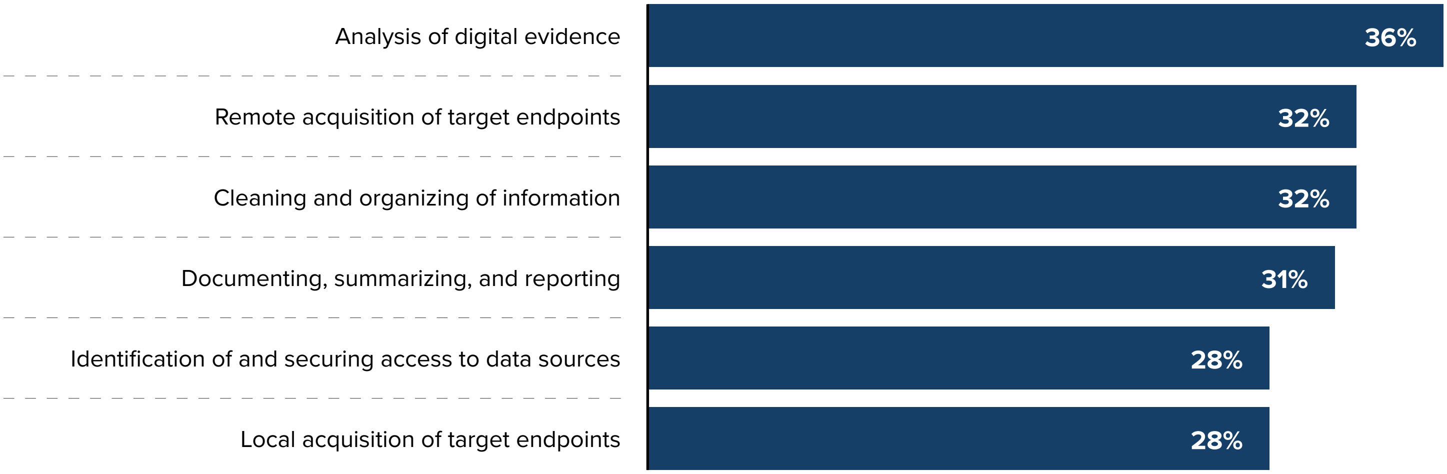
New technologies have been adopted to enable an entirely remote workforce. Information is being passed around organizations in the form of larger video files and ephemeral messaging, and on devices that may not be managed by the organization. **So not only is the volume of data larger, it is also now even more inaccessible.**

When asked to what degree improvement was needed for certain functions within the DFIR department at their organizations, **close to one third of respondents answered that major improvements or a complete overhaul were needed with regard to analysis, acquisition, and cleaning of data.**

FIGURE 4

Improvement Areas (% of respondents)

Q. To what degree can your organization improve on each of the following functions? (Major improvements or a complete overhaul needed)



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

When broken out even further:

approximately **14%** **of respondents indicated that analysis of digital evidence needed a complete overhaul.**

more than **10%** **of respondents indicated that remote acquisition of endpoints needed a complete overhaul.**

These numbers may seem small, but selecting "complete overhaul" is a significant criticism of the current state of these organizations' capabilities. This is understandable, given that many labs have legacy DFIR tools in place that aren't designed to meet the needs of today's challenges.

The Problem of Plentiful Data

DFIR teams struggle to analyze all of the data they collect. The area of analysis was identified as both a current and future area for improvement. Without a modern DFIR toolkit that leverages an artifacts-first approach and automation, it stands to reason that the more data there is, the more time is needed to thoroughly analyze it.

In addition to the volume issue, there is also the diversity of data that now exists. **Computers are not the only sources of evidence anymore — there are mobile devices, cloud-based apps and services, and the exponentially growing realm of Internet of Things (IoT) devices.** When data volume and diversity are both increasing, the challenges facing DFIR teams are painstakingly clear.

As mentioned, remote work continues to challenge DFIR teams as well:

66% **of respondents stated that remote acquisition needed at least some improvement.**

The obstacle to remote acquisition is likely a technological one, and more specifically related to the diversity of data sources.

DFIR professionals need to be empowered with tools that make their jobs easier. Additionally, DFIR teams must be able to investigate employees and the relevant evidence and artifacts now contained remotely on employee devices, and they need to be able to collect that data covertly.

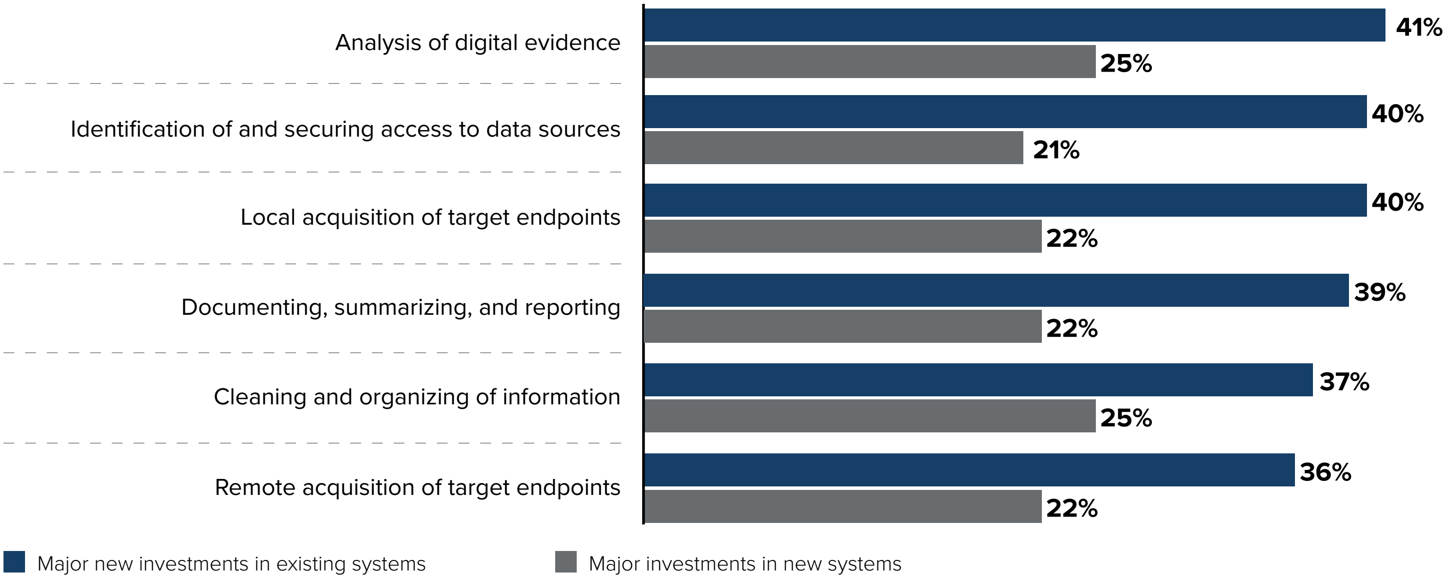
This is exactly why

59% **of respondents indicated that remote acquisition of target endpoints will need major investments in new systems, or major investments in existing systems.**

FIGURE 5

Investments to Shore Up DFIR Capabilities (% of respondents)

Q. Over the next two years, what level of new investments do you expect your organization will put into each of the following functions?



n = 466, Source: *Magnet Forensics' 2022 State of DFIR Study*

DFIR teams need at least some improvement within their toolset. These teams need help collecting and analyzing data, not only because of the volume and difficulty but because of the speed required based on the current threat landscape.

Ransomware Is Keeping DFIR Teams Up at Night

According to IDC's *2020 Data Protection and Privacy Survey*, threat actors are alarmingly successful at penetrating corporate environments.

Close to
25% **of organizations are reporting ransomware infections weekly.**

As malware evolves, these individual events are being combined into single attacks: Malware first exfiltrates data and then encrypts it, allowing a bad actor to command a ransom for releasing the encrypted data keys — and also extort the organization to prevent the release of the data publicly.

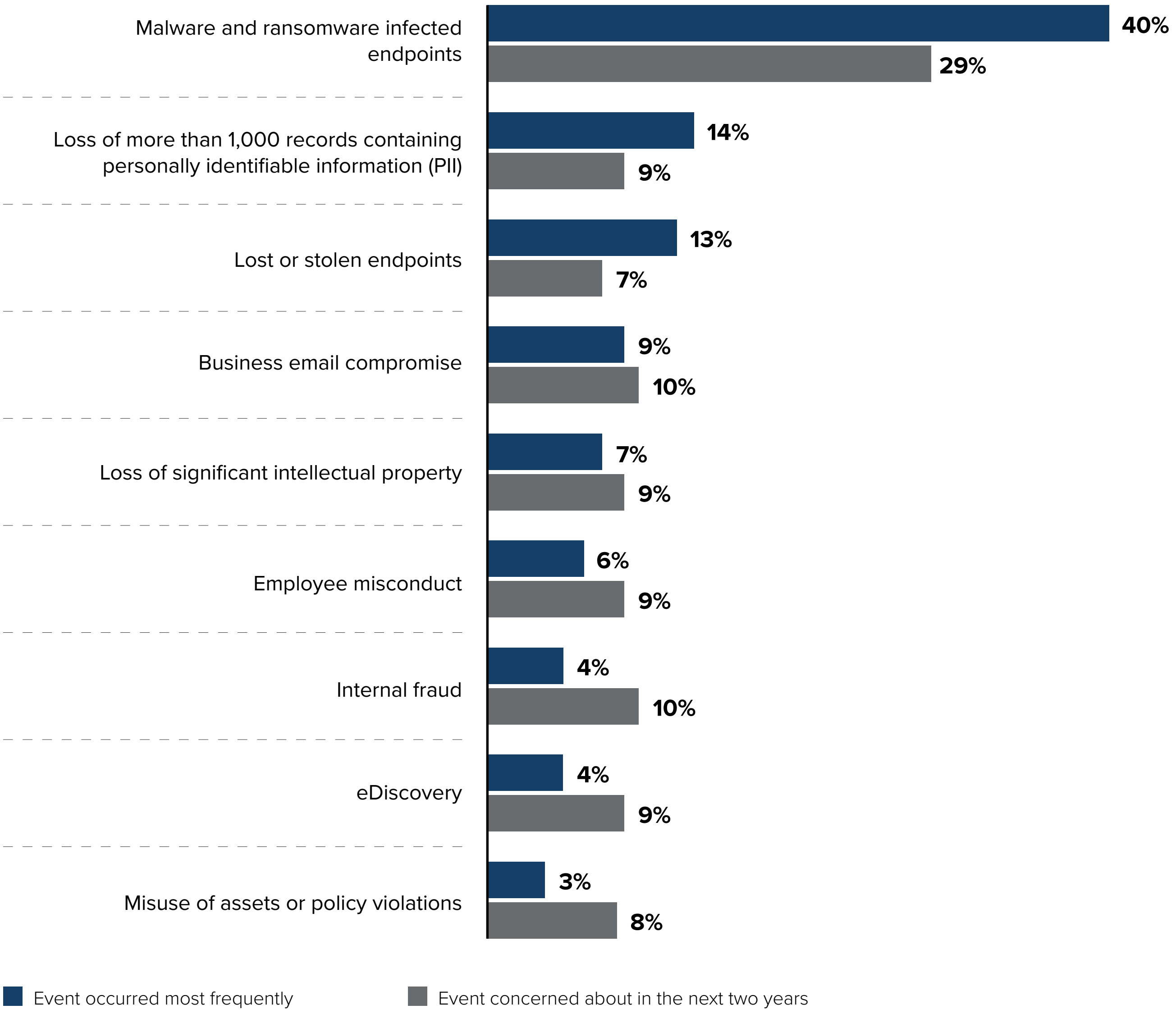
This particularly poses a challenge for DFIR Practitioners, due to the need to quickly mitigate ransomware before it can propagate and cause widespread damage. **Ransomware is harder to mitigate with security technologies that require more analysis and time**. Respondents to the study indicated that ransomware was indeed keeping them up at night.

Overall, ransomware is the biggest challenge facing Practitioners today, and will continue to be a main concern for the next two years.

FIGURE 6

Frequency of Security Threats (% of respondents)

Please rank the top-most event that occurred in the past year, and that you are most concerned about in the next two years.



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Ransoms Are Paid at Least 87% of the Time

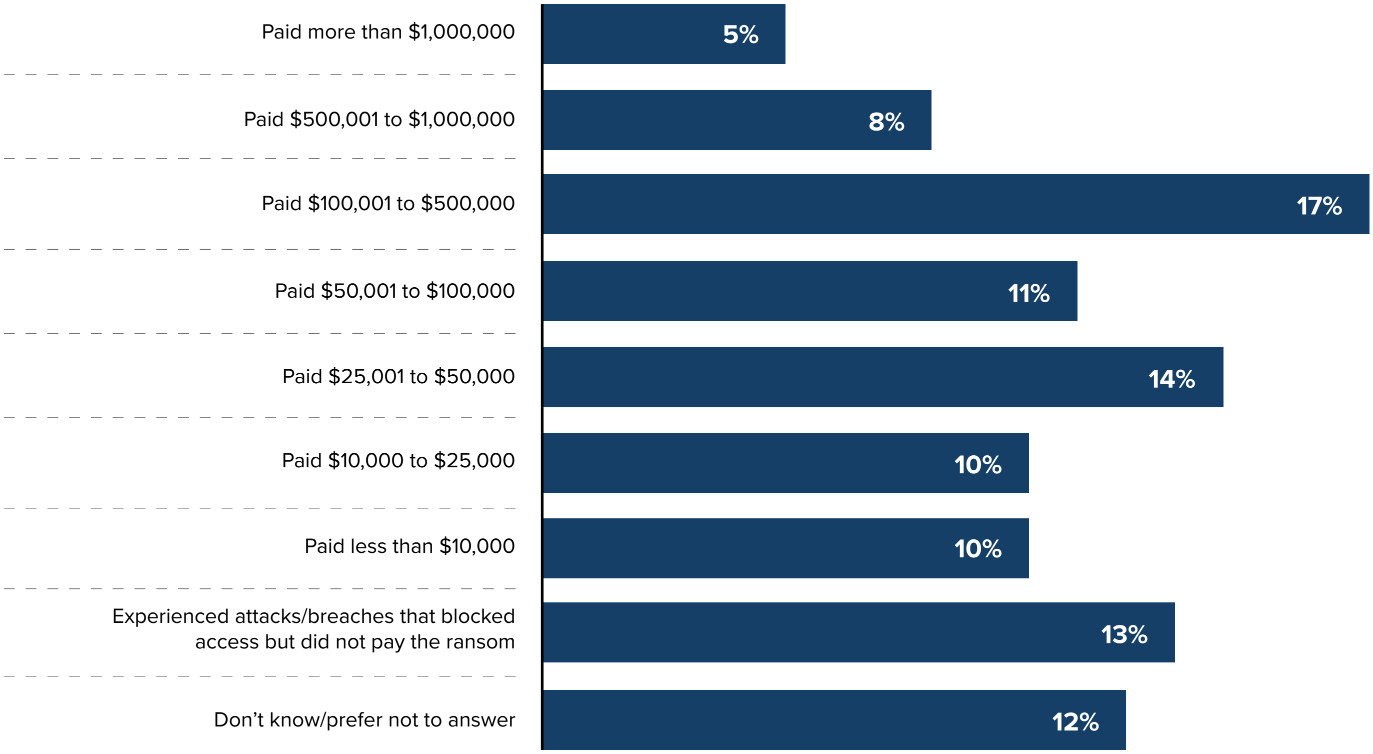
The cost of ransomware to an organization can be staggering and, unfortunately, in some cases can cause financial ruin.

It is essential for organizations to invest in their DFIR teams and enable them with the tools needed to protect the reputation and data of their organizations. **If DFIR teams don't receive the investment they desperately need, then organizations face incredible risks.** Without the proper tools, people, and processes in place, it's often "easier" to pay a ransom and resume operations.

FIGURE 7

Ransomware Payouts (in US$) (% of respondents)

Q. If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid?



n = 292, Source: IDC *Future Enterprise Resilience & Spending Survey Wave 6,* July 2021

Solving Challenges with Technology

Like many professions, there is a skills shortage in the area of DFIR, so it may not be possible to solve problems by adding head count. Technology is going to be the answer for most enterprises when trying to solve the challenges posed by hybrid work environments and data explosion.

Choosing the right product to fit into your existing technology stack — or, in some cases, replace it, given that a "complete overhaul" of some areas is needed — is an important decision that involves many variables, not least of which is the feature set and benefits offered. Survey respondents were asked to rank the most important features to have in a primary digital forensics tool.

The three most important features of primary forensics tool were:

- **Collects from many data sources**
- **Analyzes all of the evidence in one case file**
- **Performs the majority of the workflow with one tool**

The responses indicate the desire to have an all-in-one tool to manage DFIR tasks. Although streamlining tools through interoperability is top of mind for many DFIR leaders, respondents interestingly did not emphasize interoperability with other tools.

While DFIR labs should always employ a toolkit approach and validate their findings with more than one tool, having a primary or go-to tool for the majority of DFIR tasks can help save time and money.

DFIR labs should consider investing in a comprehensive, modern "all-in-one" tool as their go-to digital forensics acquisition and analysis tool that can collect from many data sources, often globally dispersed, and synthesize that data into one case file.

The need to surface evidence quickly and streamline workflows to keep up with the evolving world is at odds with a technology stack that contains a multitude of point solutions.

Not only did our analysis reveal that the ability to collect from multiple data sources is a priority, but more than

1 in 3 Practitioners responded that it is the major priority for improvement over the next two years.

No longer can organizations deploy tools that are aimed specifically at one task, such as collecting mobile data. DFIR tools need to do it all.

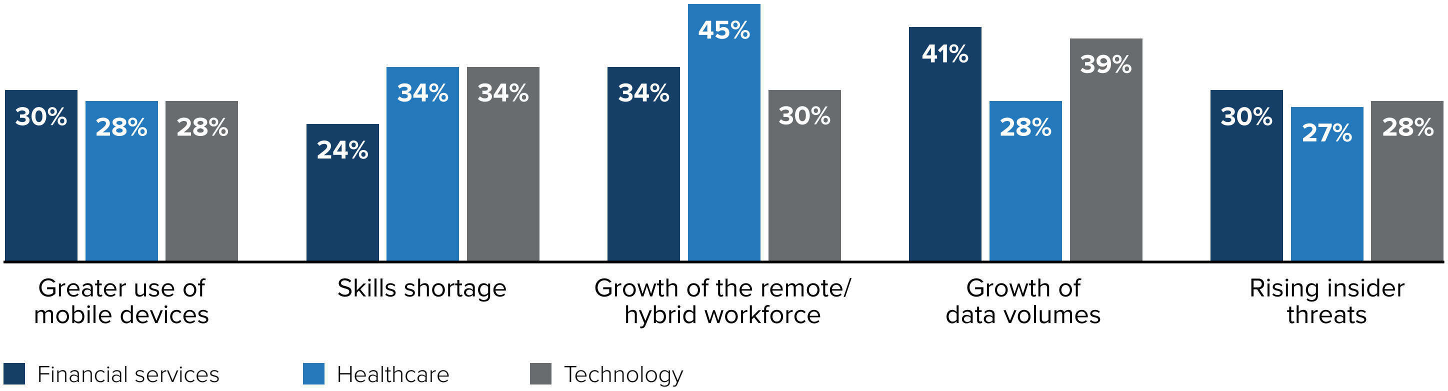
This trend continues within specific industries as well.

Industry Spotlights

FIGURE 8

Top 5 Challenges Facing Digital Forensics, by Industry (% of respondents)

Q. What are the most challenging aspects of digital forensics activities today in your organization?



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Industry Spotlight: Financial Services

Financial services organizations have a great deal of sensitive information and stringent regulatory requirements. DFIR functions and tools are a key component of the incident response process for these organizations.

The external threats are great, but internal threats are especially pervasive within financial organizations. Financial services respondents think that rising insider threats will be the most challenging aspect within the next two years.

38% **of respondents indicated insider threats as one of their top challenges, and also indicated concern with evolving cyberattack techniques.**

DFIR tools are instrumental in responding to and rectifying cyberattacks and insider threats. Both pose a great risk to financial services organizations. Planning must begin now.

On average, financial services organizations reported having close to nine DFIR employees. These employees have a mean experience level of approximately six years within DFIR, with 83% of employees having at least three years of experience. Financial services organizations tend to align their DFIR departments closely with information security departments.

Financial services respondents were aligned with the overall results in that malware and ransomware are the most frequent security events impacting their organizations. Financial services is still a highly on-premises environment due to its aversion to risk. As such, local acquisition of target endpoints was highlighted as a major area for improvement. It was the second-highest-ranked area for improvement, behind analysis of digital evidence.

Financial services organizations also specifically noted that threat hunting and memory analysis need significant additional resources in the coming years. In that vein, from a technology perspective, financial services organizations are primarily focused on a toolset that can collect from many sources and then synthesize it into one case file. In fact, **two out of five financial services respondents indicated that the ability to collect from many different sources is the priority for a forensics tool.**

Not far behind was the ability to analyze evidence within one case file. This is because the most challenging day-to-day aspect for financial services providers is the growth of data volumes. The stakes are high for financial services firms: Incidents can lead to jail time and very bad press. Investment in DFIR needs to be a priority.

Financial services respondents were aligned with their technology peers in indicating that the growth of data volumes is the biggest challenge they face today.

Industry Spotlight: Healthcare

Healthcare was another solid portion of the respondents, with 74 respondents. Healthcare is also a risk-averse industry that tends to have a large amount of on-premise deployments.

The average experience level of DFIR employees within healthcare was more than five years, with 81% having at least three years of experience. Healthcare respondents reported an average of under nine DFIR employees per organization.

Healthcare respondents were very much in line with the overall results as well, **indicating that malware and ransomware were their two most frequent security events,** aligned with other heavily regulated industries.

As expected, when asked about the level of concern for various data sources over the next few years, healthcare respondents indicated that on-premises storage was the biggest concern.

Not too far behind was IoT devices. When healthcare IoT devices are compromised, lives are lost or endangered, so the importance placed on them is warranted. This is a major concern for all. So it follows that, when asked which areas need significant additional resources, healthcare respondents cited cloud forensics by a wide margin.

Cloud is relatively new to healthcare. The industry likely needs help to catch up to those industries that aren't as risk-averse and have been living in the cloud for many years.

Finally, when it comes to technology, the primary area of focus for healthcare was network scalability: **Two out of five healthcare respondents selected network scalability as the area that needs improvement,** further signaling that they are playing catch-up when it comes to the cloud.

Healthcare respondents, to a higher degree than their non-healthcare peers, indicated that the most challenging aspect of digital forensics today is the growth of remote workers.

Almost one in two healthcare respondents said that the hybrid workforce was the biggest challenge. But when looking to the future, 35% — the highest percentage — indicated that growing data volumes are the most concerning. This is understandable when considering the amount of privacy regulation specifically targeted at healthcare. More data means larger-scale investigations and more vulnerability.

Healthcare organizations will want to prioritize scalable solutions capable of handling large volumes of diverse data.

Industry Spotlight: Technology

The technology sector is the most advanced when it comes to the adoption of modern, cutting-edge technology and processes, including DFIR tools. However, when it comes to team size and tenure, the technology sector lags behind its heavily regulated industry counterparts, financial services and healthcare. The opportunity for automation to aid the technology sector is ripe.

Technology respondents made up 74 of the 466 overall respondents. Technology industry players tend to be less risk-averse and more cloud-first organizations. Technology players on average reported approximately seven DFIR employees per organization, much lower than their heavily regulated peers. Technology players' DFIR teams average a little over five years of experience, and 76% had at least three years of experience.

When asked about the frequency of security events, **technology companies reported a much higher level of ransomware impacting endpoints than any other industry.**

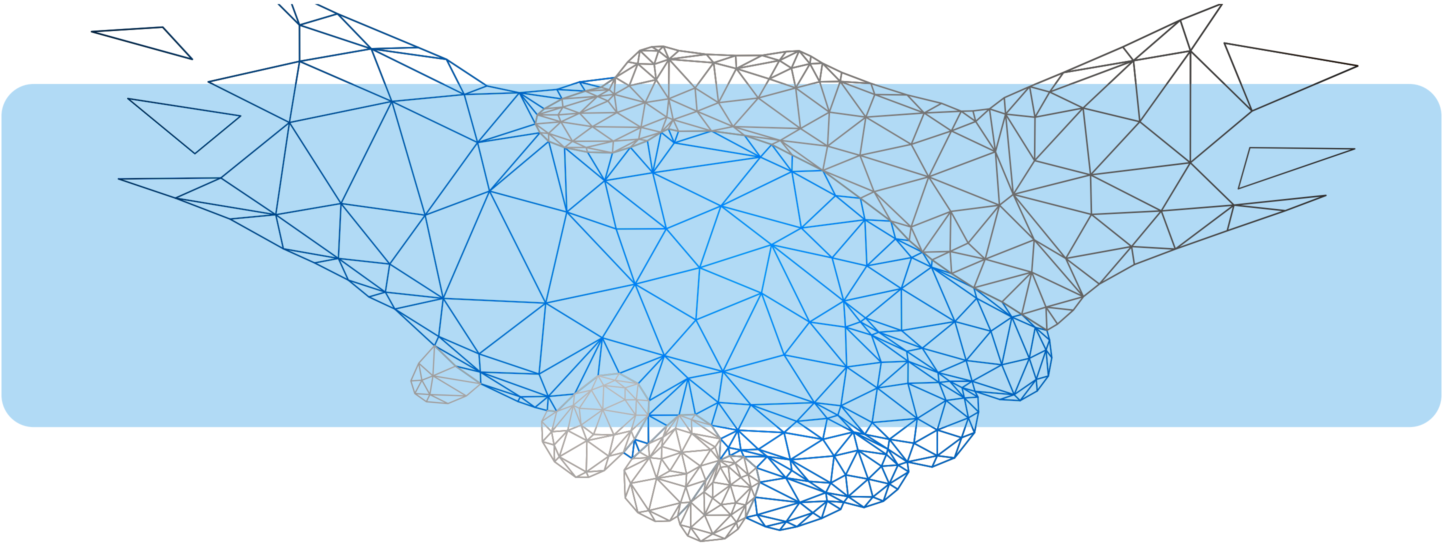
Every other industry ranked malware first, where technology ranked ransomware as much more pervasive (with a mean summary of over 7 to over 6).

Technology respondents did not have a significant outlier in areas of concern over the next two years when it came to data sources. Technology sector companies likely have so many different pieces within their IT infrastructures that the risk posed is equally great across all areas. The same was true when asked what additional resources are needed: The answer was "all of them"!

They need help with all aspects of DFIR, **which is why when asked about areas of investment from a technology perspective, the ability to collect from many different sources was cited as the major area for investment.**

When asked to look forward two years, technology respondents expected that the challenges of tomorrow would be different than the ones of today. Automation seems to be a key focus, given that the two most-selected responses were time-consuming, repetitive tasks and incorporating AI/ML into workflows.

Given their smaller teams and willingness to adopt new technology, **leveraging products that automate DFIR tools and tasks are a perfect fit for technology companies.**



Practitioners and Decision Makers: Same Team, Different Roles

Practitioners and Decision Makers have a common goal to protect the organization, but they approach it from different perspectives. By sharing how they each uniquely or similarly view DFIR, perspective from either side can be gained, leading to a shared understanding that can drive united change.

Practitioners are in the weeds and spend much of their time on DFIR activities. Practitioners are those within this survey that spent at least 20 hours per week on DFIR activities and were below a Director level.

Decision Makers are focused on more macro issues. These perspectives can appear competing at times but at the end of the day they are in fact complementary. Practitioners and Decision Makers just take different paths to get there.

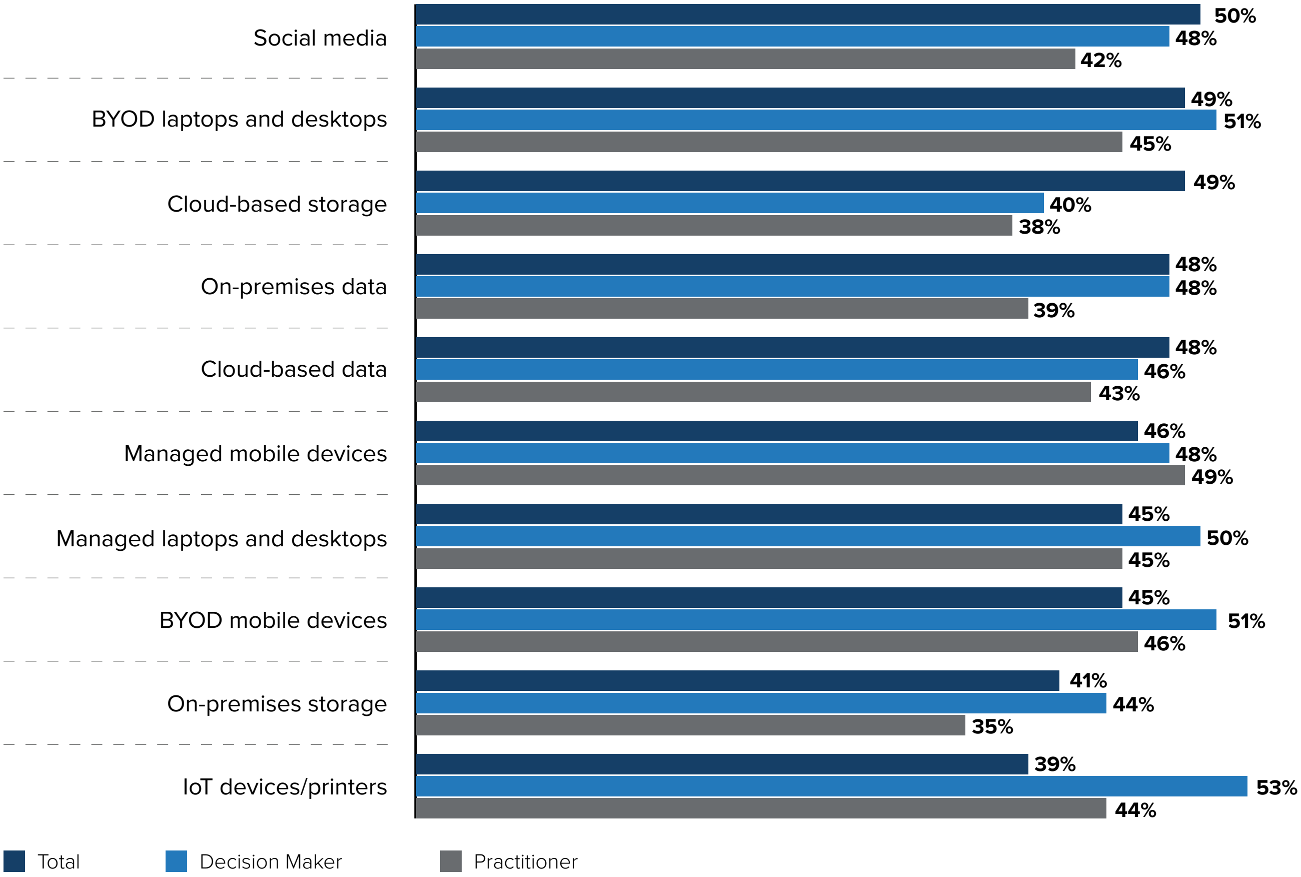
Varying Paths to the Same Destination

Decision Makers' and Practitioners' responses diverged in several different areas. Decision Makers had different concerns when it came to the level of risk posed by different technologies. Decision Makers were more concerned with the risks posed by legacy technology than Practitioners by a 9-percentage-point margin. **Decision Makers are at the forefront of transforming organizations into digital-first enterprises and are likely more concerned with the risks posed by sunsetting legacy technology.**

FIGURE 9

Concern with Data Sources (% of respondents)

Q. Over the next two years, what is your level of concern over the future risks posed by each of these areas where corporate data may be used or stored? (Extremely concerned and very concerned)



n = 466 (Decision Maker = 296, Practitioner = 170), Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Practitioners are more concerned with devices, both managed and BYOD. Practitioners are more concerned with their day-to-day tasks than Decision Makers. Practitioners likely spend many hours per week painstakingly collecting and analyzing the data within those devices. This is top of mind for them. Meanwhile, the responses to the question around "risks posed by different endpoints" are higher overall from the Decision Makers. Their concern with the macro, and generally all facets of the business, shines through in the data collected within this study.

Two Sides of the Same Coin

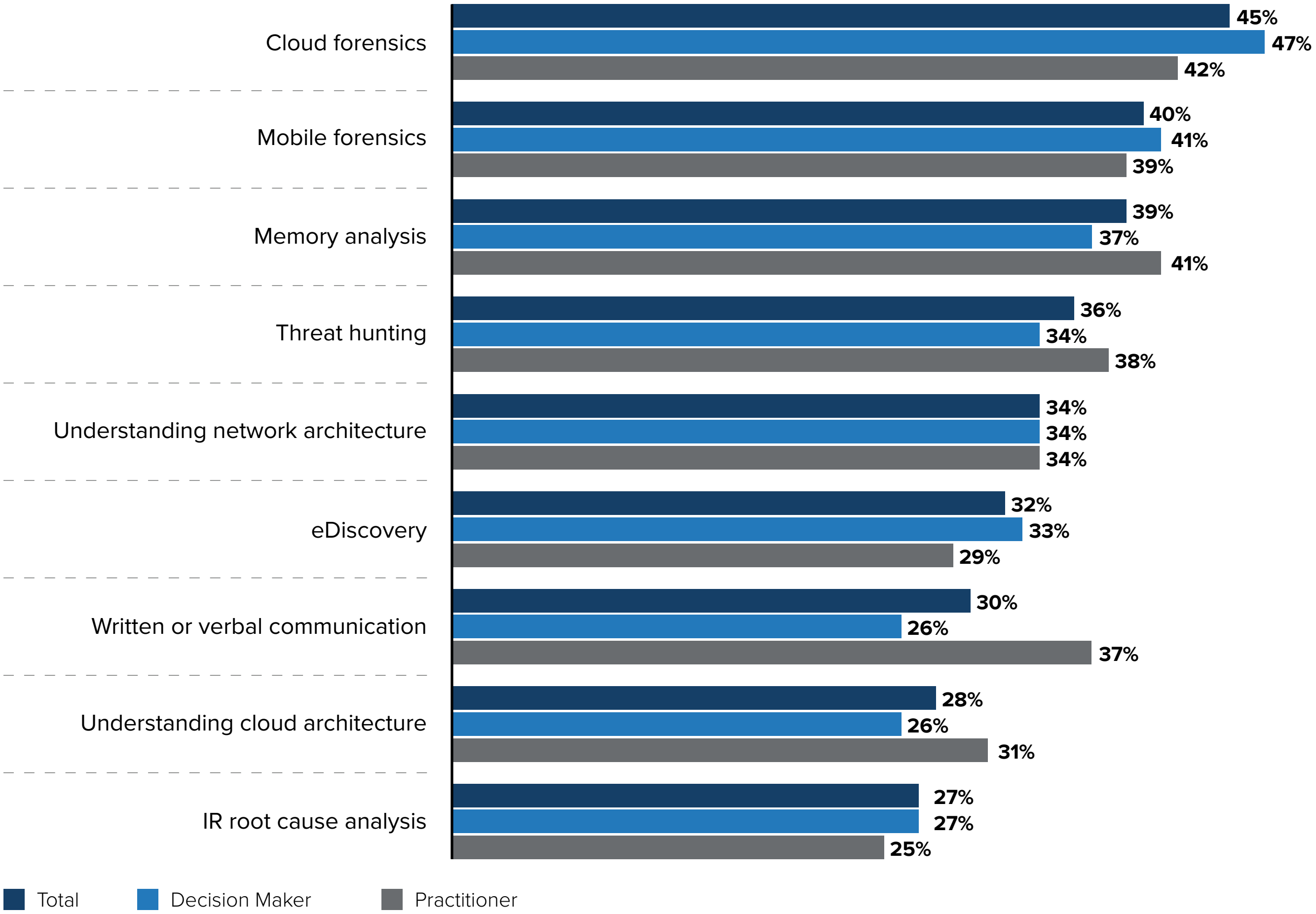
The survey asked the respondents about their pain points. This was another area of divergence for the Decision Makers and the Practitioners. Decision Makers were not as concerned with the *how* so much as the *what*. For instance, Practitioners noted that internal communication, both written and verbal, needed significant improvement. Practitioners placed much more importance on this aspect than Decision Makers, along with memory analysis, threat hunting, and understanding cloud architecture. Decision Makers placed more importance on cloud forensics generally.

These seem to be two sides of the same coin. There is a lack of resources within forensics departments, both overall and with cloud forensics — specifically with cloud architecture understanding. Both Practitioners and Decision Makers are recognizing the issue but are not necessarily viewing it in the same way.

FIGURE 10

Areas of Additional Resources (% of respondents)

Q. Which of these specific areas of digital forensics need significant additional resources in your organization?



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

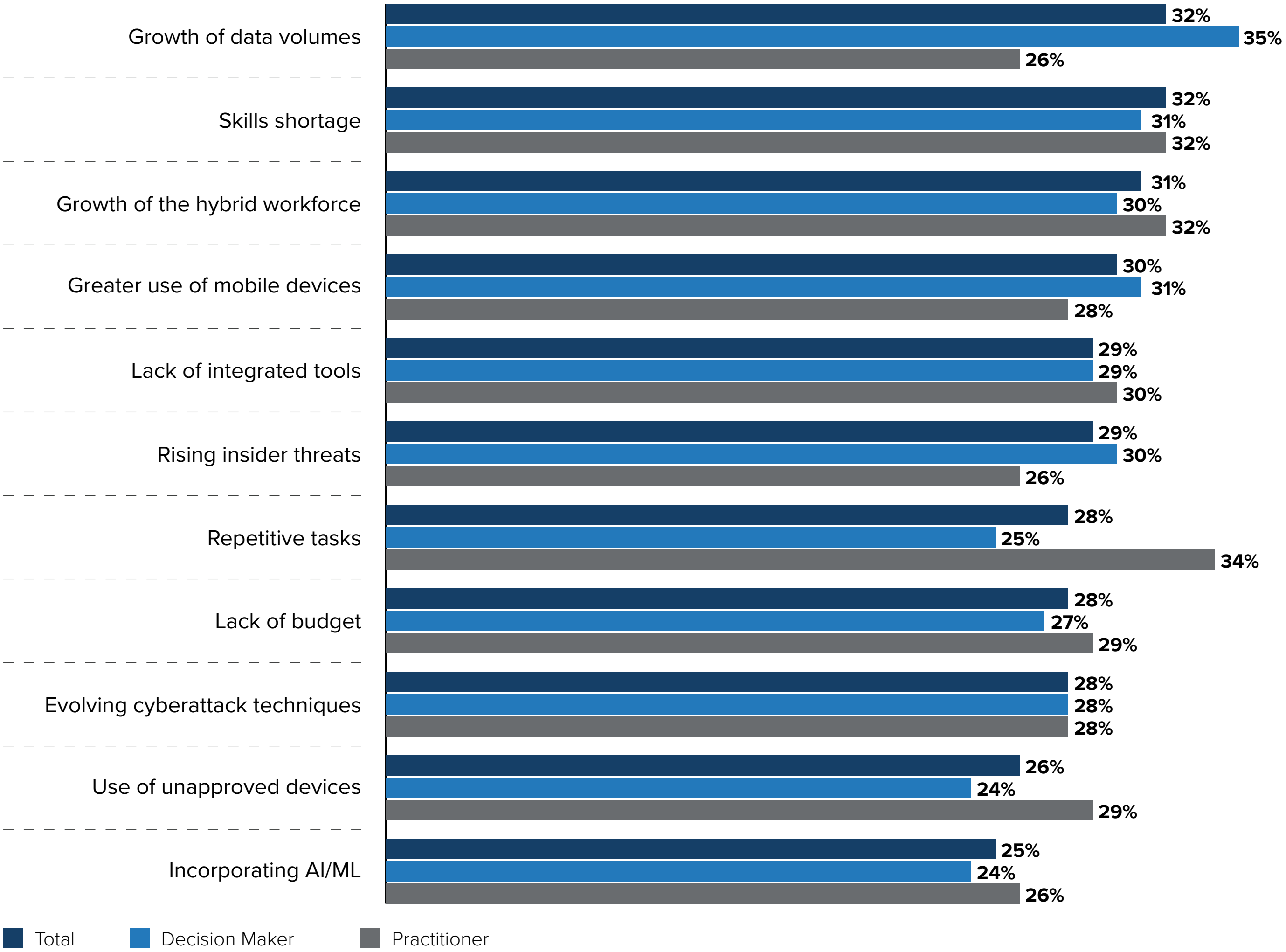
This differing perspective was also reflected when respondents were asked, *"What are the most challenging aspects of digital forensics activities today in your organization?"* The answers were aligned at the top for Decision Makers and Practitioners. However, the Decision Makers were again more concerned with steering the ship than with making sure the engine is running — rightfully so, as that is generally their main responsibility across organizations.

Practitioners highlighted what was top of mind for them. **Time-consuming, repetitive tasks were a top concern for Practitioners,** 9% more challenging to Practitioners than Decision Makers. Practitioners are the ones doing those tasks, so of course they are more challenging for them, and Practitioners assume this will continue to plague them over the next few years. Practitioners were more concerned with shadow IT than the Decision Makers were, because they see firsthand the vulnerabilities it creates. The different perspectives are understandable and make complete sense.

FIGURE 11

Challenges Facing Digital Forensics, by Participant Type (% of respondents)

Q. What are the most challenging aspects of digital forensics activities today in your organization?



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

Practitioners are the ones doing the day-to-day forensics activities, but the Decision Makers ultimately control the budget. **It is important that, ultimately, both perspectives are married to create a holistic view of an organization's DFIR activities and needs.**

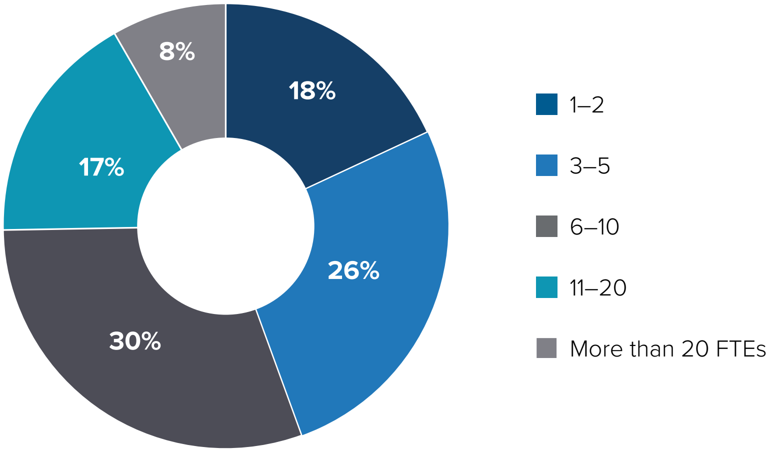
It should be highlighted that Practitioners feel, overwhelmingly, that there is a lack of communication within DFIR. Prioritization can only occur effectively when the picture is viewed in totality. Practitioners need support just as much as Decision Makers need to hear what is going on at the execution level. The digital-first world is changing rapidly, and DFIR teams need to be on the same page.

Structure of Forensics Teams

Digital forensics and incident response professionals play a very special role in any organization since they are responsible for protecting the organization—typically post-security incidents—by investigating possible threats that run the gamut from data breaches to insider threats to eDiscovery to HR investigations such as employee misconduct.

FIGURE 12

DFIR Team Size (% of respondents)



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

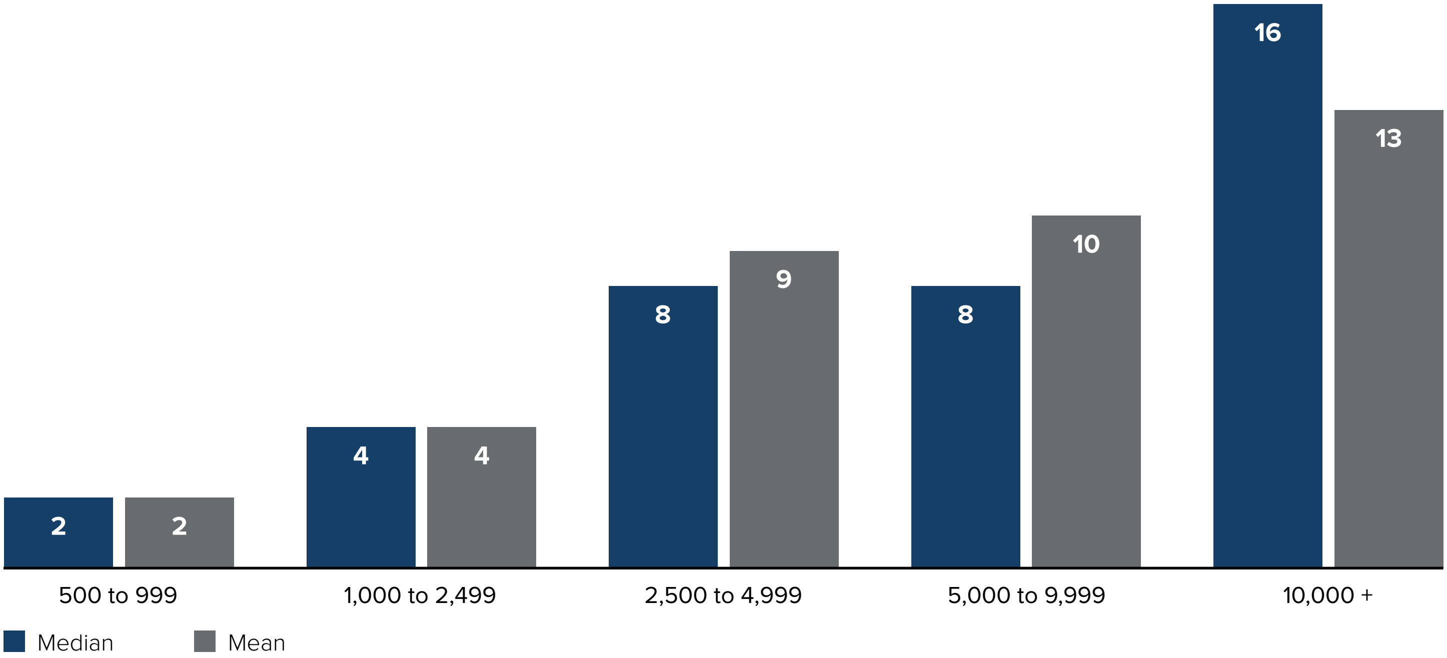
A DFIR team does not generate hard revenue dollars. It is a cost center that generates revenue for the organization by preventing losses and reputational damage that can be hard if not impossible to quantify. Thus, the DFIR budget is not as robust as that of profit centers, but it is a critical part of the organization. This tends to result in a relatively small departmental size. The median team size across all organizations was eight, with the mean a tick higher at 8.17, according to the study.

74% **of respondents indicated that their departments consisted of fewer than 10 people.**

As expected, this number scales with organizational size. Organizations from 500 to 999 employees operate with an average of just two employees dedicated to DFIR, while larger organizations average more than 15 employees dedicated to DFIR.

FIGURE 13

DFIR Team Size, by Organization Size (Number of employees)



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

If we assume an organization of 10,000 employees has 15.5 DFIR employees, that's just one DFIR employee per 644 employees. That is an astronomically small number for a department that must investigate and respond to incidents that can impact all of the devices within an organization, no matter where they are physically located. DFIR employees are asked to cover the entirety of the organization. According to IDC projections, **the data created worldwide will increase by 21% and broach 97ZBs in 2022.**

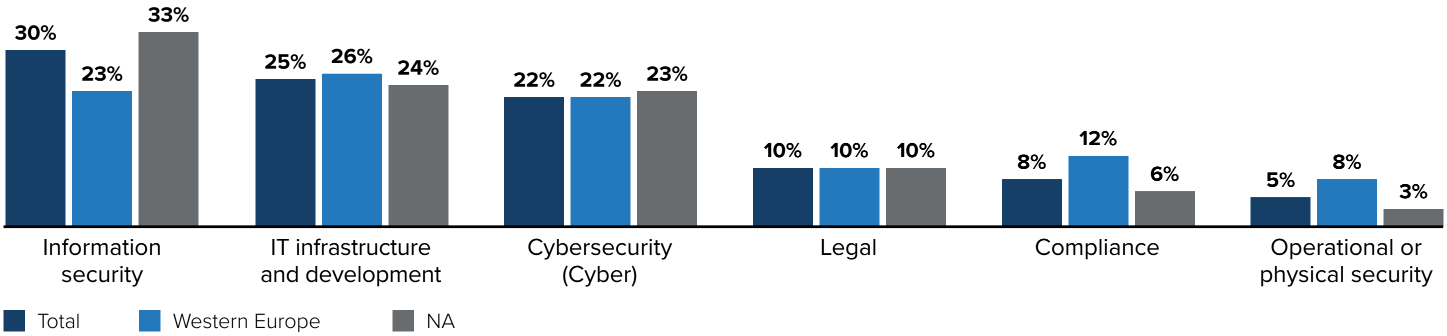
Threat actors are becoming more aggressive and sophisticated. Technology is needed to supplement the limited people power within these DFIR departments. However, organizationally, DFIR teams may have close alignment with other departments that can add bandwidth in crunch times, such as IT and cybersecurity teams.

Under the general umbrella of Security or IT, there is no consensus as to who owns DFIR across the enterprise landscape. Respondents were asked which department has the primary responsibility for DFIR within the organization. There was no consensus, only a plurality. DFIR is highly technical and as such many organizations pair it with other technical stakeholders such as Security and IT.

FIGURE 14

DFIR Responsibility (% of respondents)

Q. Which department or area has the primary responsibility for digital forensics or incident response investigations and workflows in your organization?



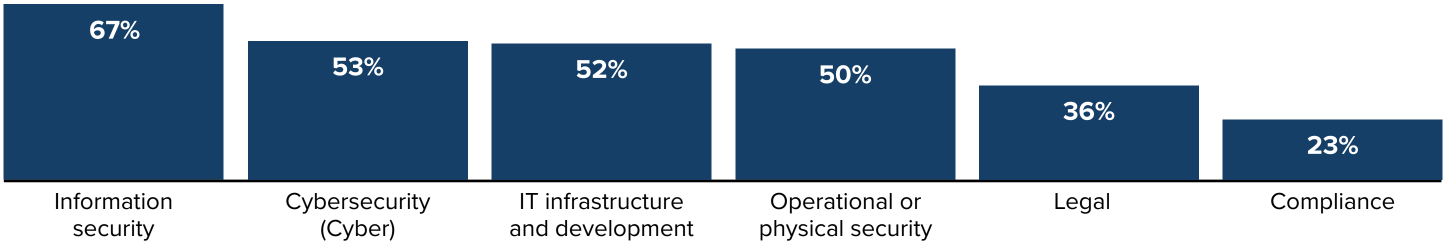
n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

North American companies tend to more heavily pair DFIR with Information Security than general IT.

FIGURE 15

Participation in DFIR Investigations (% of respondents)

Q. Which of the following departments also regularly participate in digital forensics or incident response investigations and workflows in your organization?



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

However, when the question was refined to ask not the primary affiliation but who regularly participates, the stakeholders and partner list increased.

36% **of respondents reported that the legal team is a frequent participant in DFIR activities,** while compliance teams participate the least.

DFIR has a large role to play within eDiscovery investigations, which accounts for the legal partnership indicated within the survey data.

Knowing that legal stakeholders are active participants in DFIR investigations, when thinking about which tool is at the fingertips of the DFIR examiner, it must be one that is forensically sound, can produce reports that are easy to digest for non-technical stakeholders, and likewise can produce exports that can be ingested by tools used on the legal side of the house, such as eDiscovery review platforms.

Outsourcing DFIR Activities

Increasing workloads have led a lot of organizations to outsource some of the activities traditionally under the purview of the internal DFIR stakeholders.

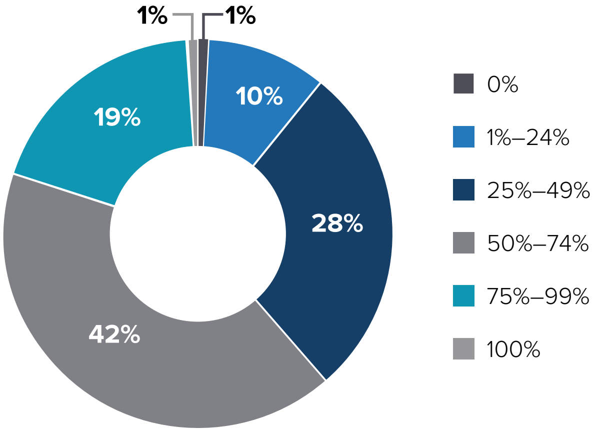
78% **of organizations outsource some of their DFIR tasks to third parties.**

Service providers are an integral part of the overall DFIR landscape. With 78% outsourcing to some degree, service providers are essentially extensions of the internal team and are basically coworkers.

FIGURE 16

Outsourcing Investigations (% of respondents)

Q. In the past year, what proportion of the total work of digital forensics investigations was outsourced to external third parties?

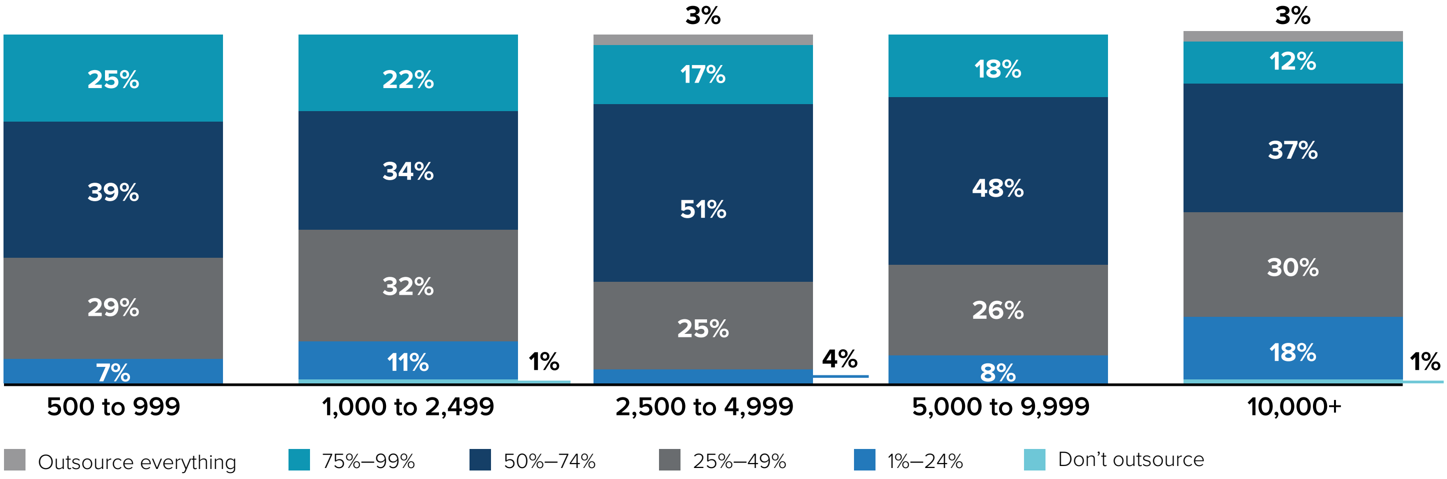


n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

When looking at the impact of organization size on outsourcing, midsize companies have the largest need and incidence of leveraging service providers. **Organizations with 2,500 to 4,999 employees outsourced on average 60% of their DFIR work, whereas the largest organizations outsourced only 50% of their work.**

FIGURE 17

Outsourcing Investigations, by Organization Size (% of respondents)



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

This is a significant amount of outsourcing, and it looks as though it is only going to continue. When respondents were asked how they expect their level of outsourcing to change over the next year, it seems not as much, which may be due to two factors. **First, DFIR is deeply tied into some very cyclical processes. Cybersecurity incidents, investigations, and eDiscovery all ebb and flow in unpredictable ways. There can be weeks and months of lulls and then a big crunch. Predicting a huge crunch that requires augmenting the internal team can be challenging. Secondly, organizations are already outsourcing at a high level, and perhaps there is not much more room for them to engage further with third parties.** The question becomes: What is driving this level of outsourcing?

Reasons for continued outsourcing of DFIR:

Predicting when external support is required is difficult

Outsourcing limits have already been reached

Overall, the main reason cited by respondents for outsourcing was not capabilities or workload of internal teams:

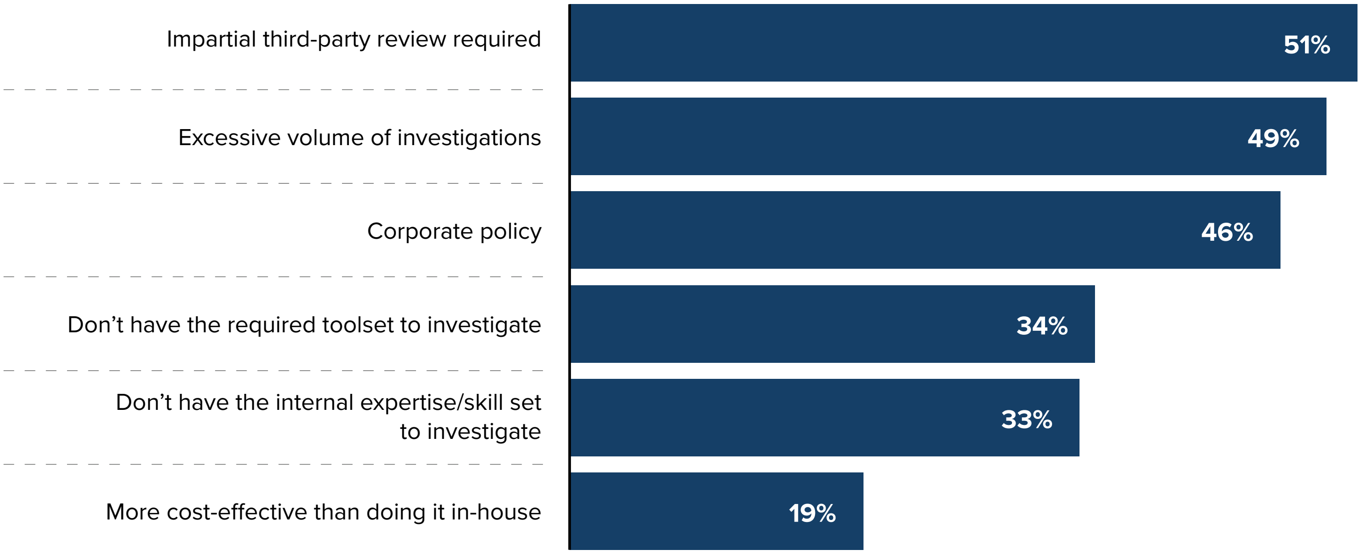
51% **indicated that they outsourced work because an impartial third-party review was required.**

Third-party reviews can be necessary in a variety of contexts, such as when providing expert testimony in an investigation. This signals that the ecosystem and partnership between internal and external professionals is symbiotic. Third parties add value and are a necessary partner in an investigation and in the analysis of forensic data.

FIGURE 18

Reasons for Outsourcing (% of respondents)

Q. What are the main reasons that digital forensics investigations are outsourced to external third parties?



n = 466, Source: *Magnet Forensics' 2022 State of Enterprise DFIR*

However, a close second driver behind the need for a third-party review is the fact that teams are overwhelmed with a large workload. Western European respondents listed the excessive volume of investigations as the leading driver for outsourcing work to third parties. Organizations under 2,500 employees further listed the volume of required investigations as the leading driver; organizations with 1,000 to 2,499 employees chose it as the leading driver at 58%. Regardless of the size of the organization or its geographic location, everyone is feeling the crunch of increased workload volumes. The current state of enterprise technology architecture and data is pushing internal and external teams to their limits. The problem will only continue as hybrid work, data, and threat actors' sophistication grow.

Conclusion

DFIR professionals are tasked with responding to incidents, investigating issues, and assisting with litigation support. The challenge of these tasks is becoming exponentially more difficult as the world shifts to hybrid work and data expands in size and diversity. While DFIR departments tend to be small, their task list is large, and as the world evolves, they must evolve too. DFIR Decision Makers and Practitioners need investment, and that investment needs to be in improved technology. DFIR teams need unified solutions that enable streamlined workflows and collect from a variety of data sources, and technology that can synthesize data into one case file for ease of use. These are the tools that will enable success now and in the future.

Message from the Sponsor

MAGNET FORENSICS®

Today's enterprise organizations are creating more data than ever before — data that is highly sought after by threat actors from outside the organization and from insiders with malicious intent. As well, the attack surface of organizations has increased over time. Bad actors are continuing to adopt new cyberattack techniques and technologies to exploit vulnerabilities in the security perimeter of businesses and take what they will.

One out of three DFIR professionals stated that they needed major improvements or a complete overhaul to their DFIR practice; with a legacy DFIR toolset in place, businesses are at a high risk of losing it all.

Magnet Forensics empowers enterprise organizations to quickly and easily find digital evidence across a diverse set of data sources — computer, cloud, mobile, and IoT devices — with modern solutions like **Magnet AXIOM Cyber** and **Magnet AUTOMATE Enterprise**.

MAGNET AXIOM CYBER™

AXIOM Cyber is a robust digital forensics and incident response solution for businesses that need to perform remote acquisitions and collect and analyze evidence from computers, the cloud, and mobile devices.

OFF-NETWORK REMOTE COLLECTION

Quickly and covertly perform remote collections of Mac, Windows, and Linux endpoints even when they aren't connected to your corporate network.

LEVERAGE CLOUD COMPUTING

The benefits of hosting your applications in the cloud ranges from cost savings to more centralized operations. Deploy AXIOM Cyber in Azure or AWS to leverage the benefits of cloud computing.

ALL DATA IN ONE CASE FILE

AXIOM Cyber is the complete investigation platform with the ability to recover, analyze, and report on data from mobile, computer, and cloud sources in one case file.

MAGNET AUTOMATE ENTERPRISE™

AUTOMATE Enterprise is an automation solution purpose-built for enterprises to concurrently collect and process evidence from multiple targets and data sources so businesses can respond to security events faster.

PARALLEL PROCESSING

Automatically process and create exports for multiple sources of evidence (computer, mobile, and cloud) in parallel. Plus, you can remotely collect data from multiple target endpoints.

BUILD STREAMLINED WORKFLOWS

The drag-and-drop workflow builder makes it easy to define and implement workflows that seamlessly integrate solutions from your forensic toolkit, including EDR tooling.

THE MAGNET DFIR ECOSYSTEM

Be more efficient with one DFIR ecosystem from Magnet Forensics: after data has been processed using AUTOMATE Enterprise, export evidence as a Magnet case file so it can be examined with AXIOM Cyber.

To learn more, please visit:

magnetforensics.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

@idc @idc idc.com