Bitdefender

Cybersecurity Assessment Report

2024

Bitdefender

Summary

This year's cybersecurity landscape continues to evolve, with cloud technologies and AI becoming increasingly central to corporate infrastructure and the threats they face. As these technologies drastically accelerate, the complexity of managing and securing them has intensified.

This year's research focuses on the prevalence of cloud adoption and organizations' significant concerns regarding protecting this infrastructure. A staggering number of enterprises are grappling with how to defend against sophisticated threats that now include AI-driven tactics, which pose new challenges and risks.

Moreover, the financial stakes of cybersecurity breaches remain high, with the costs associated with data breaches continuing to climb. Organizations cannot afford to falter on security and need solutions that effectively prevent problems before they escalate to a breach.

As we delve deeper into integrating AI into cybersecurity strategies, we raise a crucial question: are organizations truly prepared to face a growing attack surface that is increasingly dominated by intelligent, adaptive threats?

To help answer this, Bitdefender commissioned Censuswide, a third-party research firm, to survey 1,200 IT professionals ranging in title from IT managers to CISOs in various industry sectors who work in organizations with 1,000+ employees. The survey and analysis took place from March 2024 through May 2024. The respondents were geographically split equally between France, Germany, Italy, Singapore, U.K. and the U.S.

IAM and maintaining compliance are the leading security concerns when managing cloud environments.

96%
of respondents are concerned about AI's impact on the threat landscape.

64%
of respondents are planning on looking for a new job in the next 12 months.

57%
More than half of organizations experienced a data breach or leak in the last 12 months (up 6% from previous year).

Bitdefender

2024 Cybersecurity Forecast: Navigating New Frontiers

Managing cloud infrastructure is becoming increasingly complex and challenging. Today's businesses have embraced the cloud, with environments sprawling across multiple cloud and hybrid platforms. By adopting the cloud, they have realized enormous gains in efficiency and agility, but at a cost. Their attack surfaces have expanded dramatically, creating more areas to manage and protect.

While the core cloud platforms of AWS, Azure, and Google Cloud behave somewhat similarly, no two are identical. They all come with differences in configuration and operations, making identity and access management (IAM), data security, network configurations, and compliance a unique challenge. Any setup or operations failures may have wide-reaching consequences, exposing sensitive data and infrastructure to attackers.

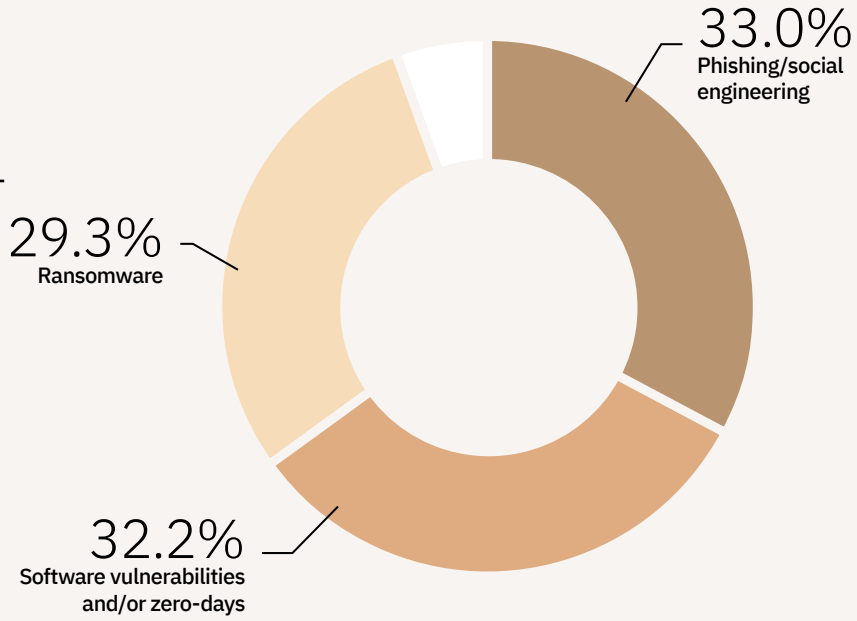
A shortage of qualified cloud cybersecurity talent makes this all the more challenging. Many IT professionals may possess deep expertise in one specific cloud platform, such as Azure, yet find themselves less familiar with others, like Google Cloud or AWS. This skill disparity can lead to gaps in an organization's overall cloud security posture.

Organizations want to "use the cloud with confidence" but are concerned about security challenges offsetting the benefits they get from the cloud. This survey was conducted to help organizations understand the different security pain points felt across the industry. By understanding the vulnerabilities and risks associated with cloud infrastructure, we aim to equip our readers with the knowledge and strategies to navigate these challenges effectively.

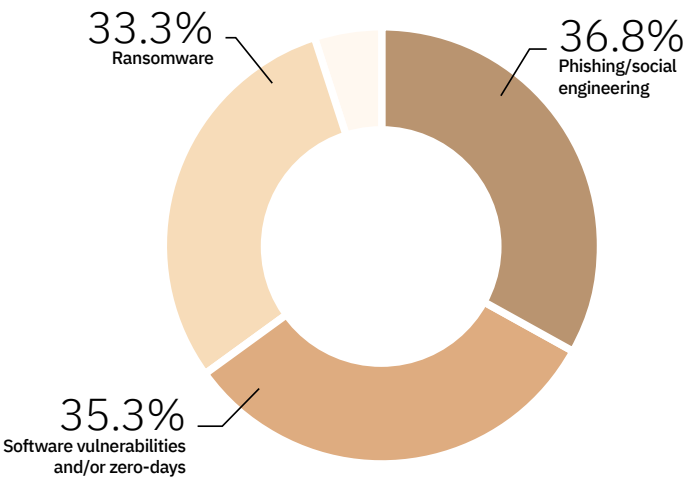
Question

What types of threats, if any, are you most concerned about?

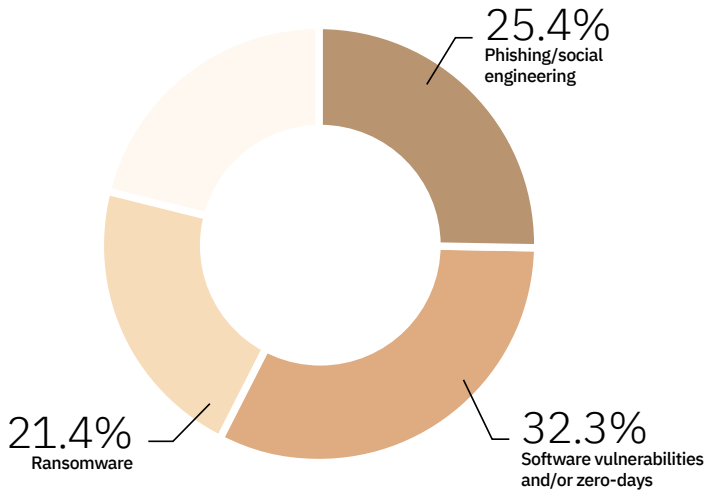
Respondents selected up to three of their top choices.



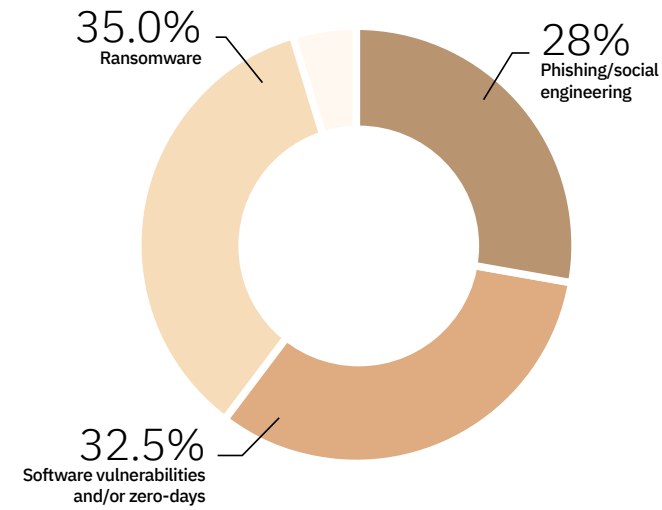
USA



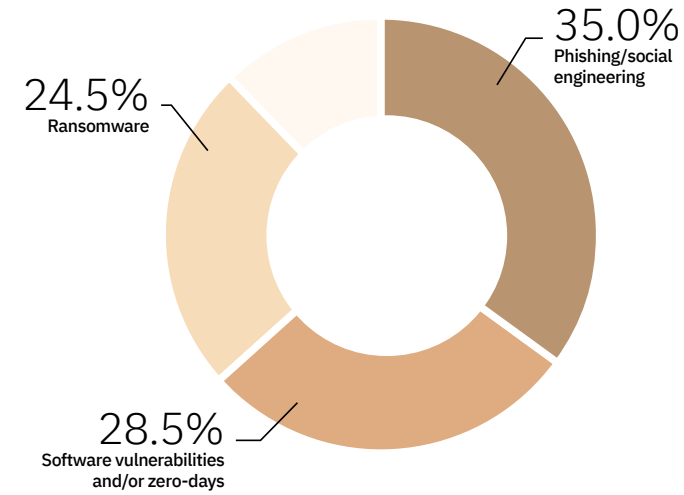
Germany



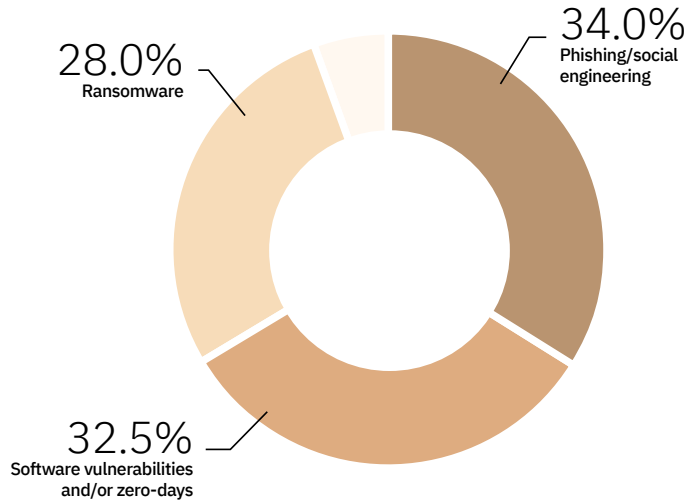
UK



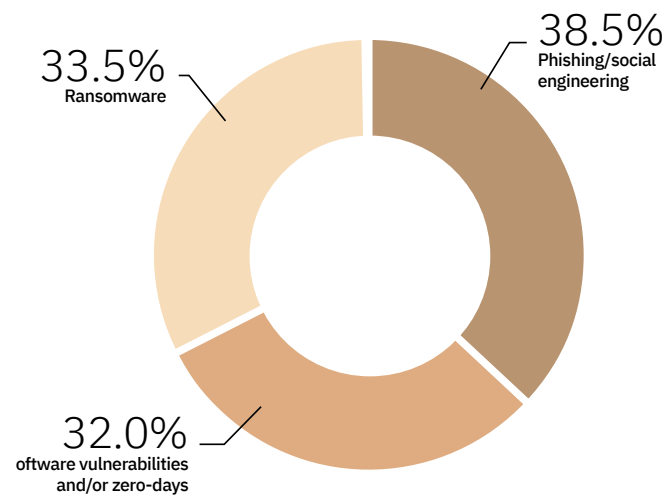
France



Italy



Singapore



Bitdefender

Cloud Computing: The New Frontier of Risk and Reward

One of the key challenges organizations face with cloud computing—its constant availability and global accessibility—also presents one of its greatest benefits. When leaders were surveyed about their top concerns, several interconnected issues emerged. For instance, 44% of respondents identified data breaches or leaks as a significant worry. Closely related to this, 43% expressed concerns over unauthorized access to cloud services, and another 42% were troubled by misconfigured cloud storage. These issues are critical as they significantly increase the risk of data breaches or leaks.

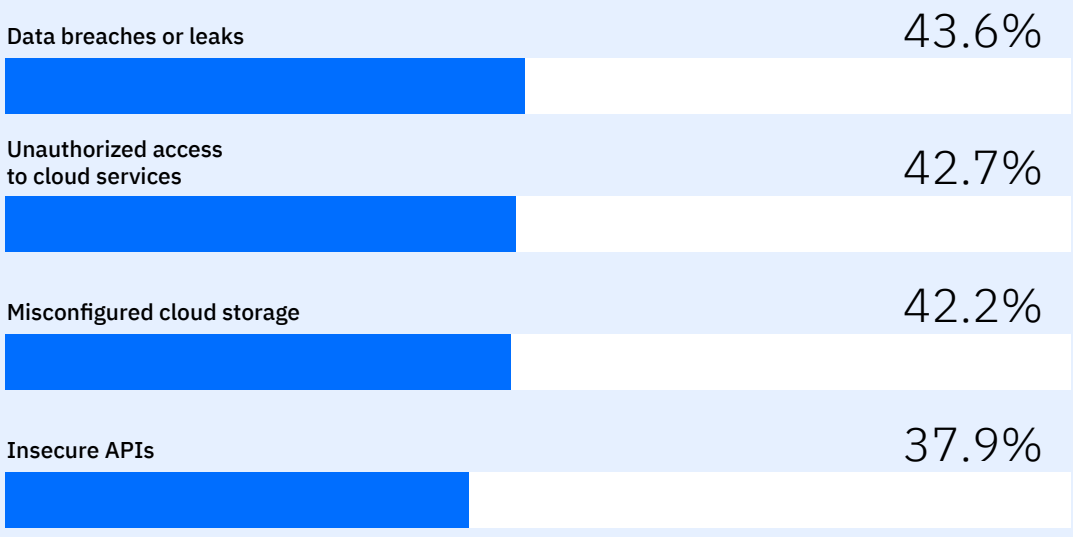
The Wall Street Journal noted the rise in data breaches, especially in cloud environments that are a tempting target for attackers.

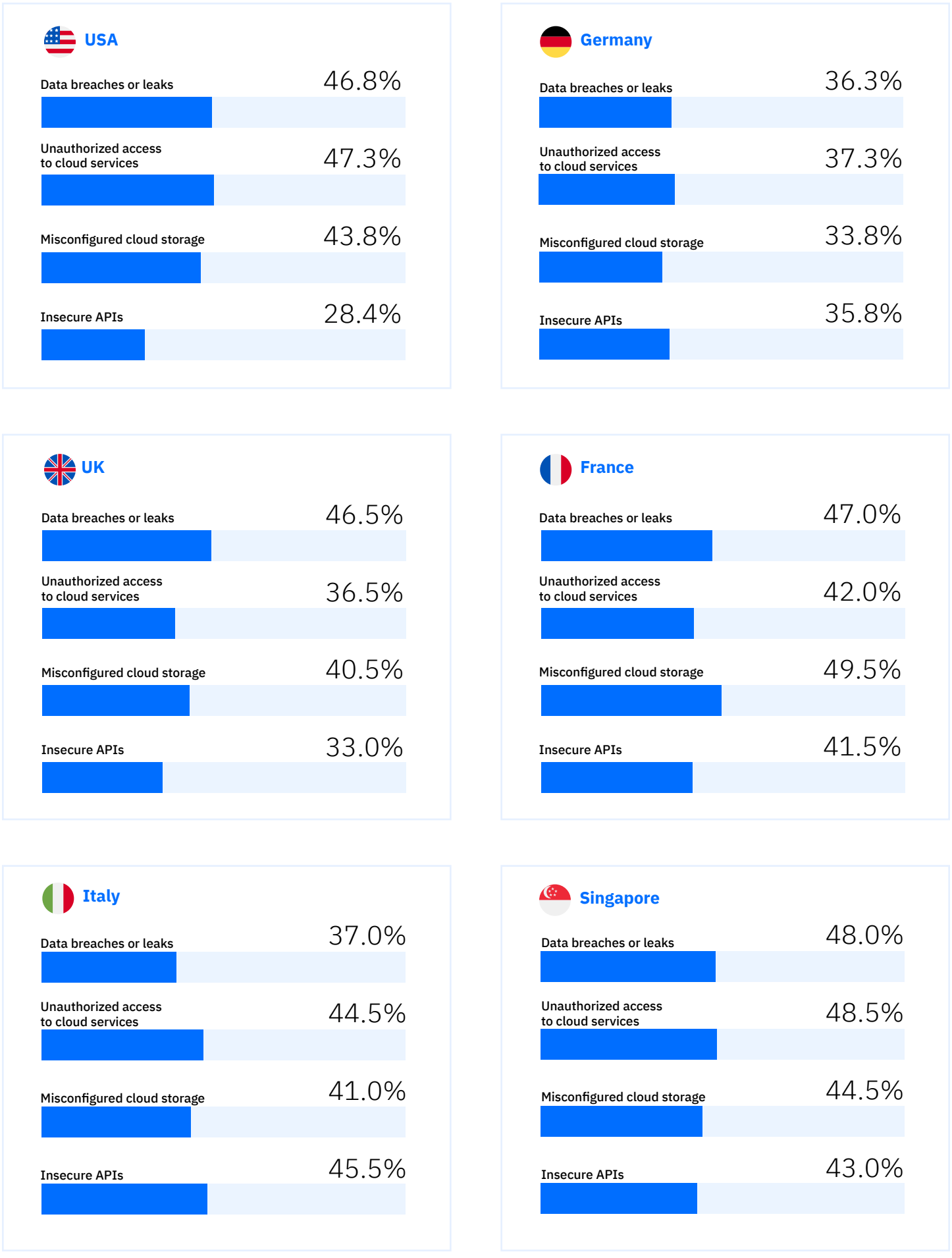
Question

What component of your cloud infrastructure and services are you most concerned about, if any, in terms of vulnerability and risk?

Respondents selected up to three of their top choices.

Overall




USA
Data breaches or leaks 46.8%
Unauthorized access to cloud services 47.3%
Misconfigured cloud storage 43.8%
Insecure APIs 28.4%
Germany
Data breaches or leaks 36.3%
Unauthorized access to cloud services 37.3%
Misconfigured cloud storage 33.8%
Insecure APIs 35.8%
UK
Data breaches or leaks 46.5%
Unauthorized access to cloud services 36.5%
Misconfigured cloud storage 40.5%
Insecure APIs 33.0%
France
Data breaches or leaks 47.0%
Unauthorized access to cloud services 42.0%
Misconfigured cloud storage 49.5%
Insecure APIs 41.5%
Italy
Data breaches or leaks 37.0%
Unauthorized access to cloud services 44.5%
Misconfigured cloud storage 41.0%
Insecure APIs 45.5%
Singapore
Data breaches or leaks 48.0%
Unauthorized access to cloud services 48.5%
Misconfigured cloud storage 44.5%
Insecure APIs 43.0%

Bitdefender

Unlocking the Puzzle of Cloud Security

Organizational lack of visibility in the cloud is one of the main issues that can lead to a breach. However, nearly half (47%) of all organizations indicated that they rely on native security offerings from their service providers, believing that they are sufficient.

As threats evolve, these native offerings are not enough. There's a growing need for more advanced tools to adeptly detect and correlate data across multiple sources, identifying genuine threats amidst the volume of native alerts that can overwhelm teams. To add value, these advanced systems need to simplify, not complicate, user experiences, enabling teams to enhance their operational visibility and control without requiring disproportionate increases in expertise.

This balance is essential for ensuring that cloud environments are secure but also manageable and efficient, as many teams (48%)* face significant skill gap challenges they address by implementing automated security tools.

For those monitoring their risks in the cloud, many others (45%) conduct regular audits and assessments to validate that their environment remains secure. Moreover, two in five (42%) professionals engage third-party experts, highlighting a lack of internal expertise by needing to leverage external expertise for managing their cloud environments.

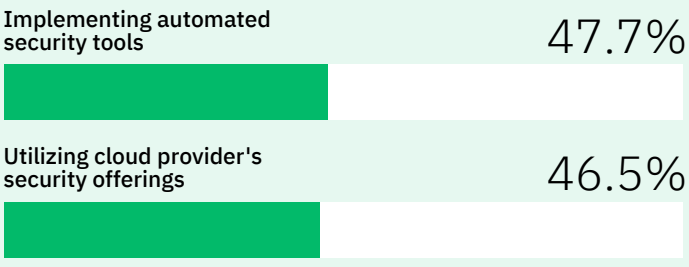
The fact that less than half of organizations are using automated tooling points to a significant gap in routine security practices . The cloud landscape is continuously evolving with business teams deploying multiple times a month, some even daily, making yearly or quarterly audits obsolete before they are even complete. Attackers are scanning cloud infrastructure 24x7, without automated tooling, attackers will discover exposures in your infrastructure before you do.

** Data can be found on page 8*

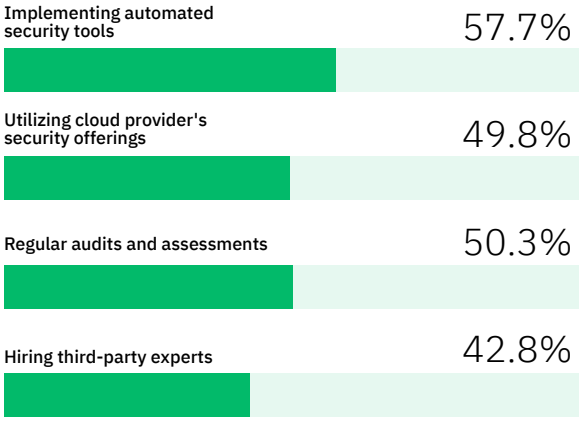
Question

How, if at all, are you monitoring risk across your cloud infrastructure?

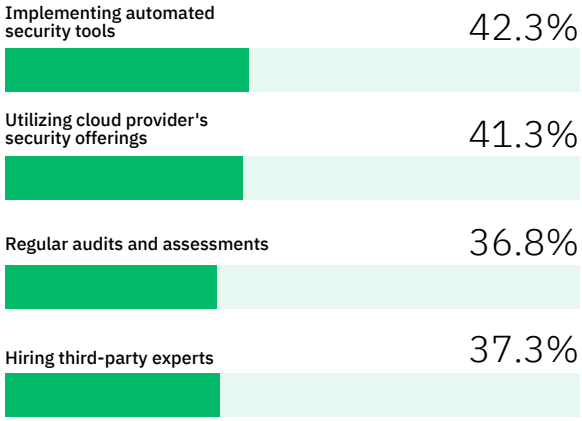
Overall



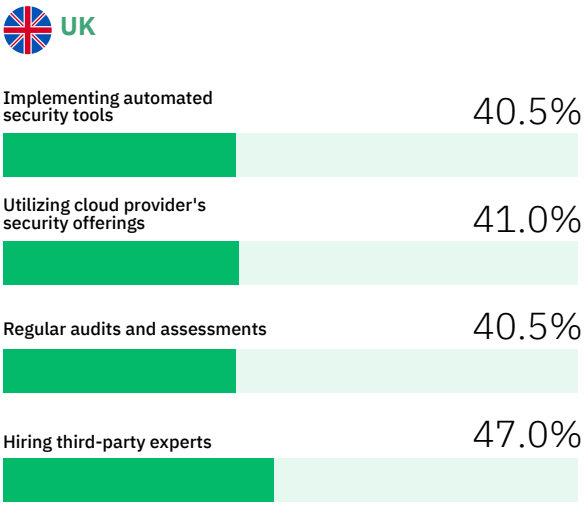
USA



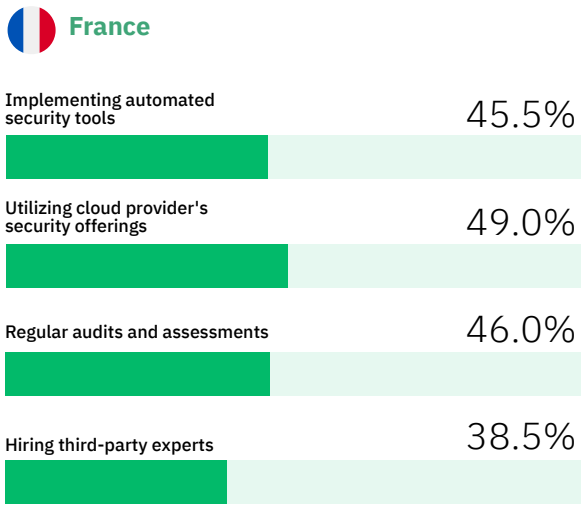
Germany



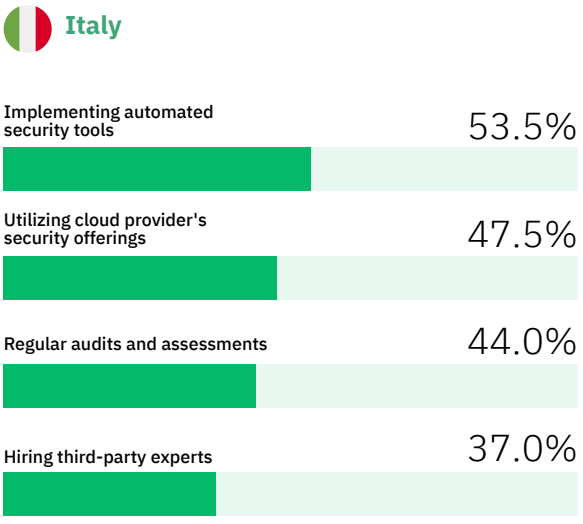
UK



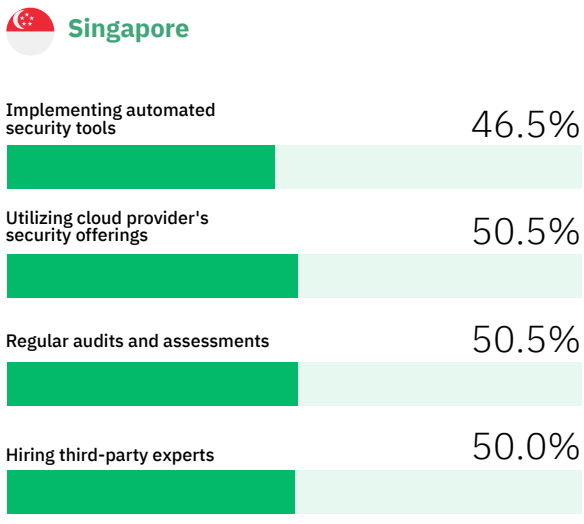
France



Italy



Singapore



Bitdefender

Mastering the Cloud: Strategies to Overcome Human Error

Visibility extends beyond merely detecting threats to organizational infrastructure; it also involves observing and comprehending the configuration. One of the core aspects of mitigating risk in the cloud is to start with a good foundation. Accomplishing this requires understanding your assets' configuration to ensure they align with best practices.

In our survey, significant concerns align with this challenge, with nearly a third (32%) of respondents worrying about human error. Similarly, others were more specific, with 39% concerned about Identity and Access Management and 34% about the risk of misconfigurations. Much of this is driven by the lack of cloud security skills, a concern for 32% of respondents.

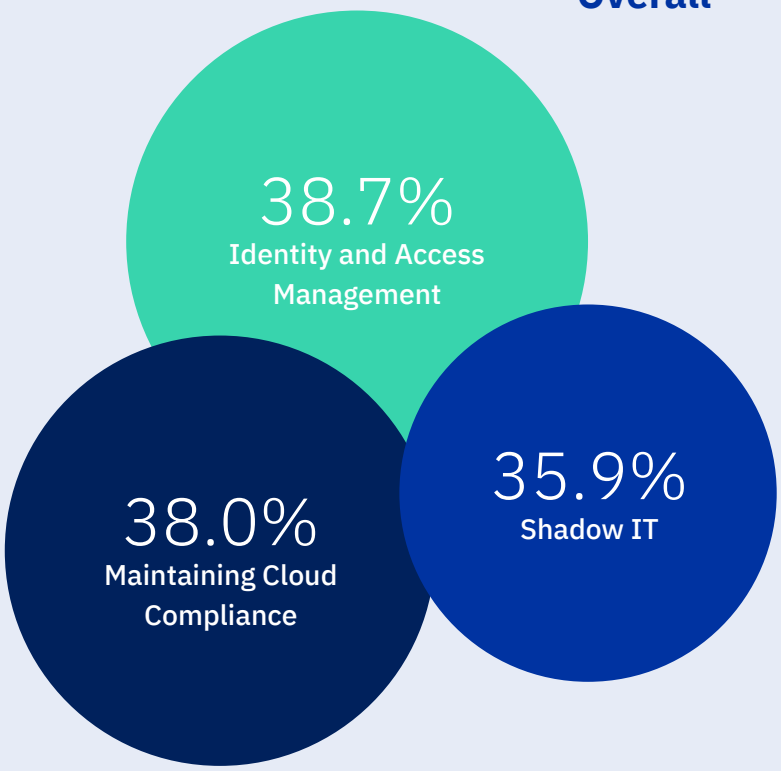
These concerns are well founded as human error accounts for many vulnerabilities in infrastructure that attackers take advantage of, resulting in what are reportedly a majority of breaches. Many companies could have avoided such breaches if they had used tools such as Cloud Security Posture Management (CSPM) to detect misconfiguration and Cloud Infrastructure Entitlement Management (CIEM) to monitor data access privileges.

Question

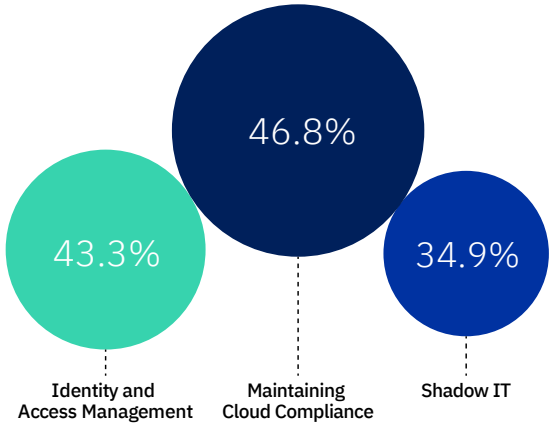
What are the top security concerns, if any, you/your organization have when it comes managing cloud environments?

Respondents selected up to three of their top choices.

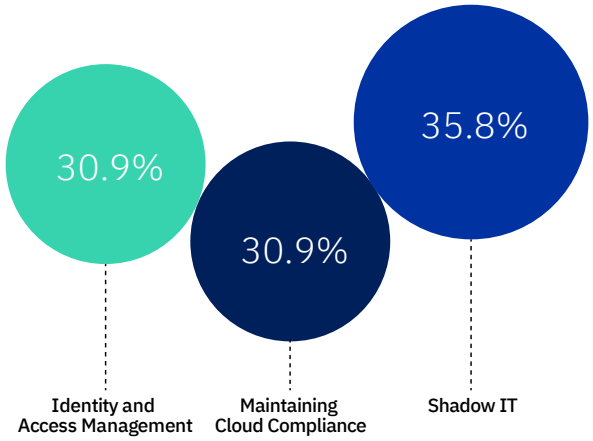
Overall



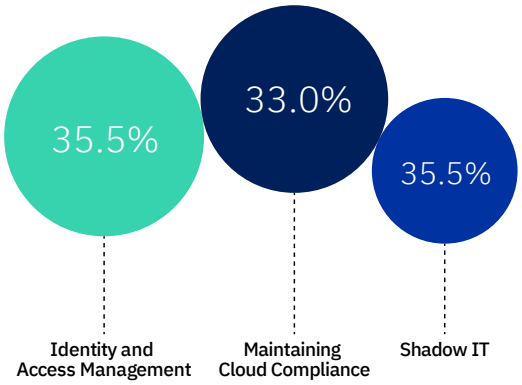
USA



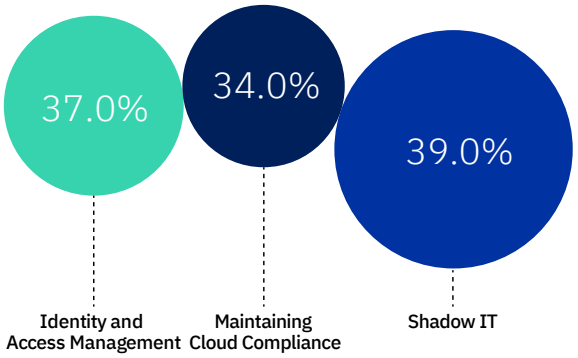
Germany



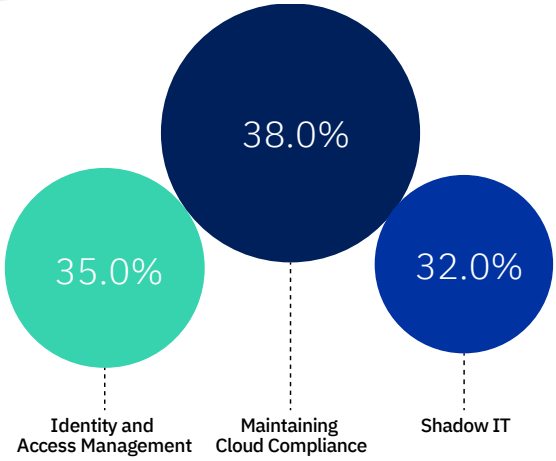
UK



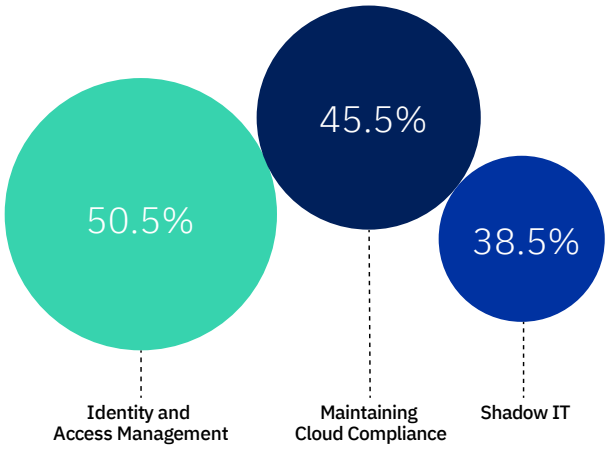
France



Italy



Singapore



AI: The New Vanguard in Cybersecurity

AI has been making headlines for its innovative applications and its growing role in cybersecurity threats, which is why it's no surprise that AI was also one of the top cybersecurity concerns for global survey respondents.

AI has shown benefits for businesses in decision-making, problem-solving, and automation. Attackers have keyed into this and are leveraging AI to enhance their operations' effectiveness and speed. Cybercriminals can automate complex tasks once manually executed, such as crafting phishing emails or generating malicious content that can bypass conventional security measures.

As AI continues to evolve, so does the sophistication of attacks, creating a dynamic where defensive measures must continually adapt to counter these enhanced capabilities. Organizations need innovative strategies to keep up with an escalating arms race between cyber defense and AI-powered threats.

Harnessing AI: Elevating Defenses, Escalating Challenges

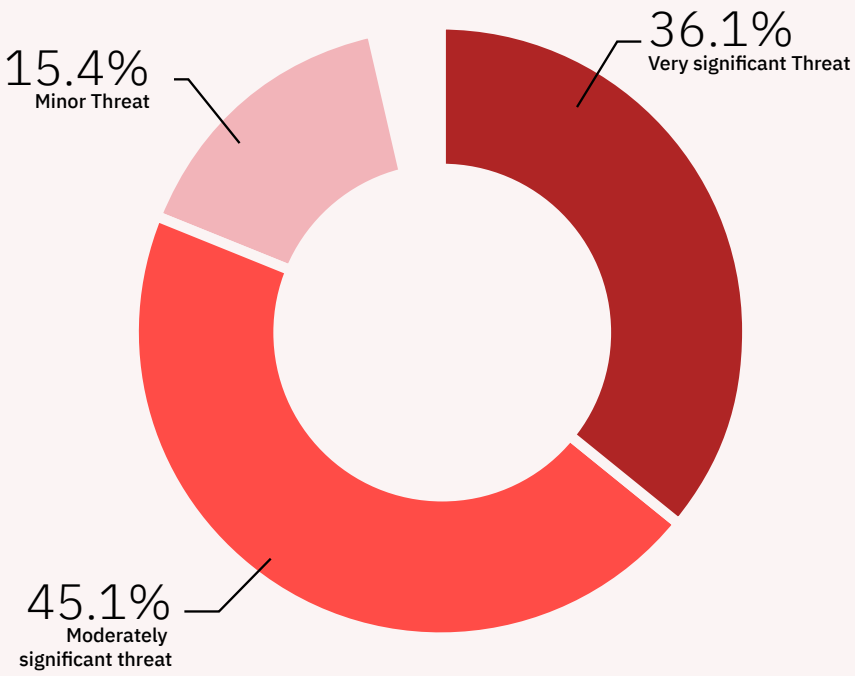
AI has transformed into an indispensable tool for modern phishers, significantly enhancing their attacks' believability and success rate. Generative AI (genAI), in particular, is a game-changer, enabling attackers to refine poorly crafted messages into compelling and convincing communications. This technology effectively eliminates the usual giveaways of phishing attempts, such as misspellings, poor grammar, and awkward phrasing, which were once clear indicators from cybercriminals who are non-native language speakers.

AI empowers cybercriminals to swiftly generate and iterate new messages, allowing them to evade less sophisticated detection systems with more sophisticated and varied attack vectors. These AI-assisted social engineering attacks have been recognized as a substantial threat in the cybersecurity community; a striking 96% of professionals view it as a concern, with over 41% considering it a very significant threat.

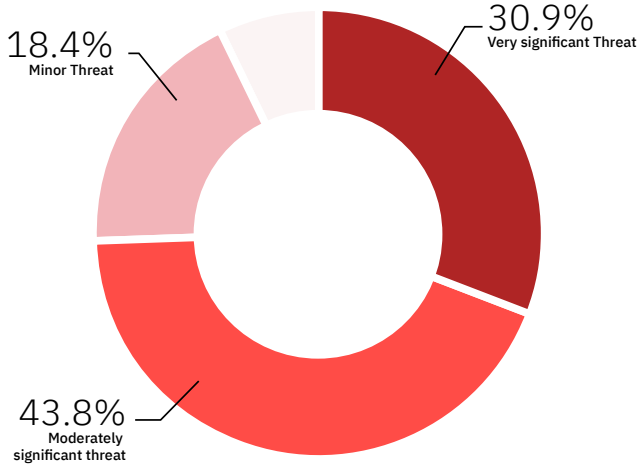
Question

How much of a threat, if at all, do you perceive Generative AI technology to be in the cybersecurity landscape when it comes to the manipulation or creation of deceptive content (e.g., deepfakes)?

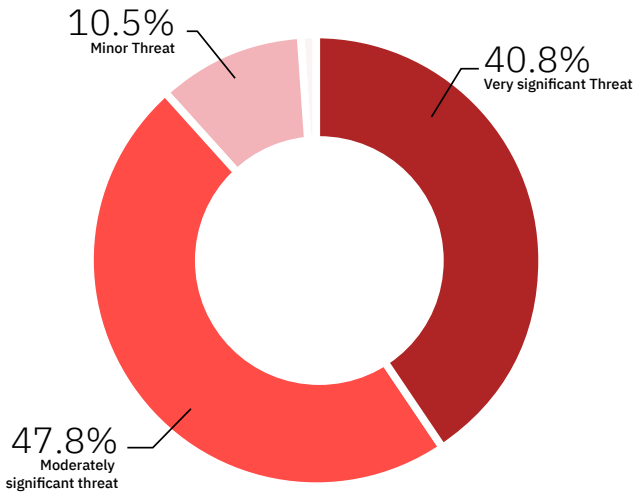
Overall



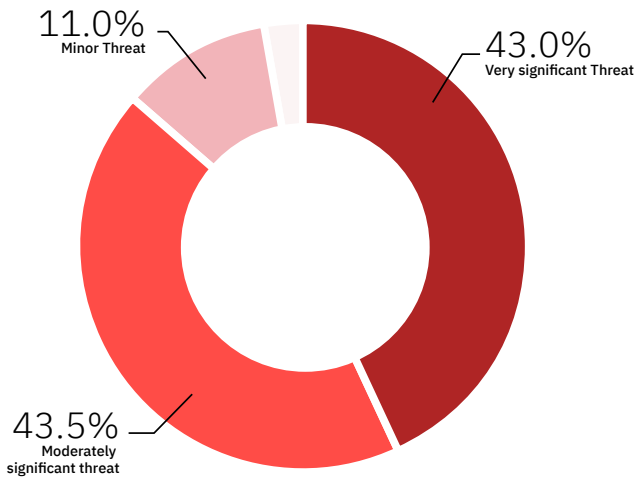
USA



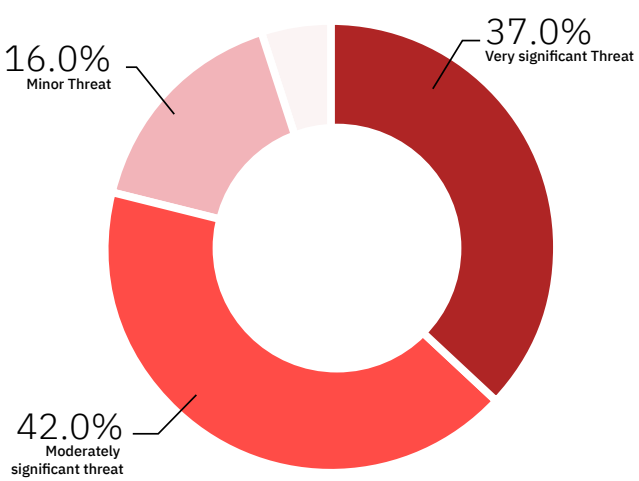
Germany



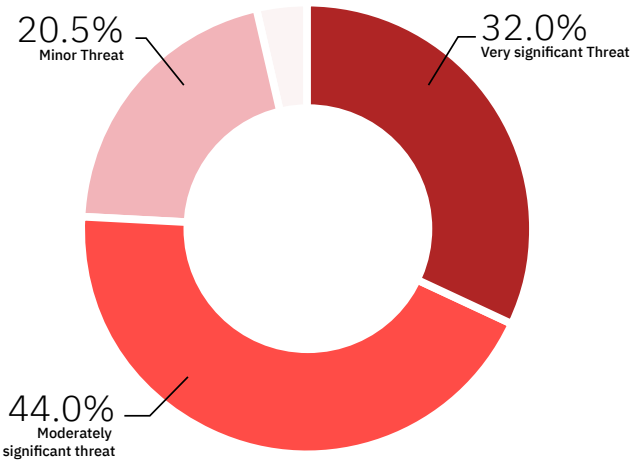
UK



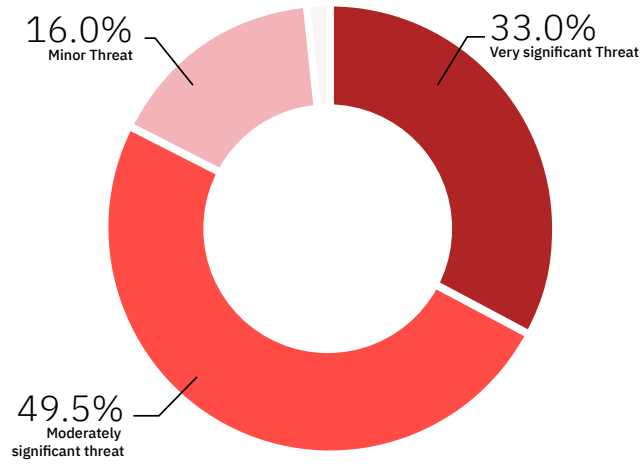
France



Italy



Singapore



Navigating the AI-Enhanced Cyber Threat Landscape

Despite attackers improving their game, most organizations feel confident responding to these security threats. Virtually all (94%) professionals surveyed say they are confident in their organization's ability to respond to security threats. However, when looking deeply at the infrastructure, approximately 2 in 5 respondents feel very confident (37%) that their organization has the tools, strategies, and people in place to respond to threats, and only 58% feel somewhat confident. The general feeling of confidence may be targeted toward existing threats, but possibly overly confident about emerging threats, lacking the tools and processes in place to address them.

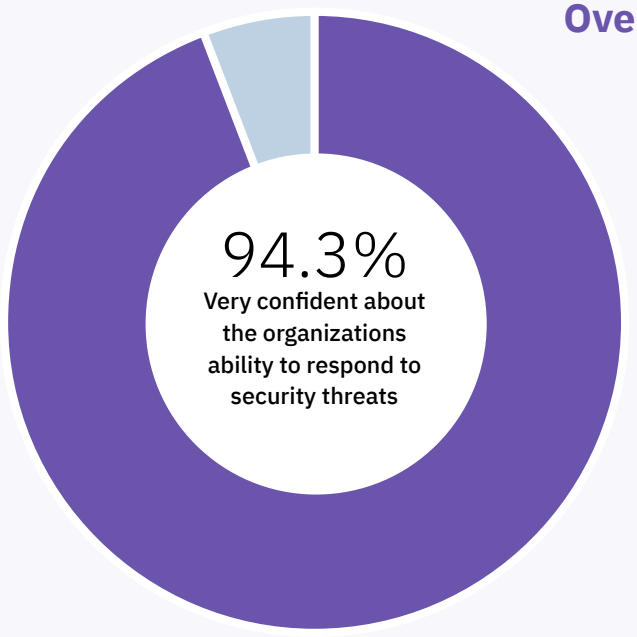
While many organizations feel confident they have the tools to effectively respond to attacks, once an incident occurs, some damage is done, which may include leaking PII or other sensitive data, resulting in compliance issues or even sensitive company data, allowing competitors a leg up.

Proactive strategies are vital to avoiding a breach. Hardened environments from patch management and IAM make it harder for attackers to succeed. Technologies like endpoint detection and response (EDR), extended detection and response (XDR) and managed detection and response (MDR) are essential for detecting and stopping threats before they take hold.

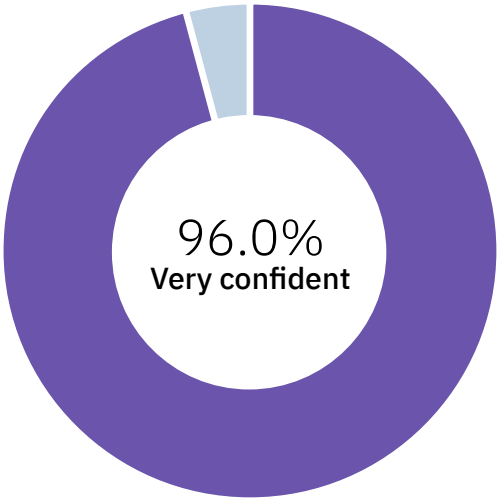
Question

How confident, if at all, are you about the current state of your organization's ability to respond to security threats (eg. Ransomware, phishing, zero-days, etc.)?

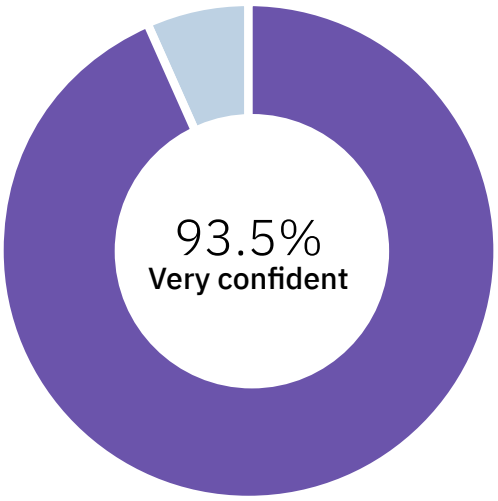
Overall



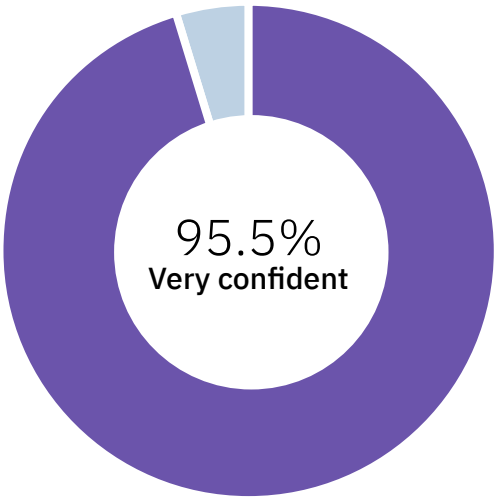
USA



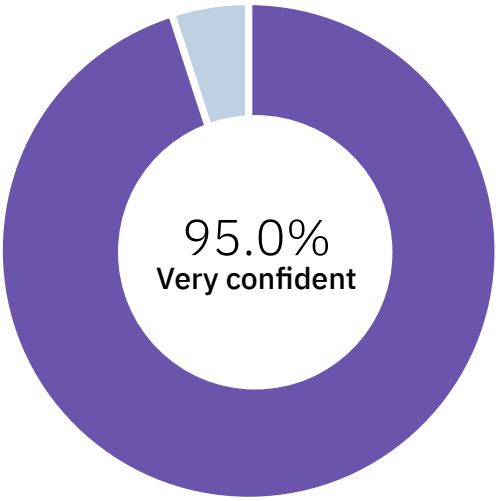
Germany



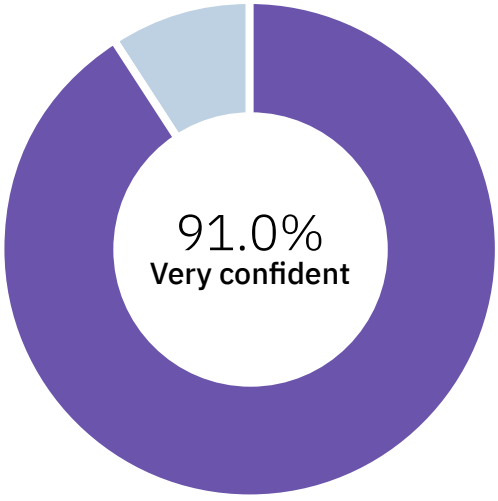
UK



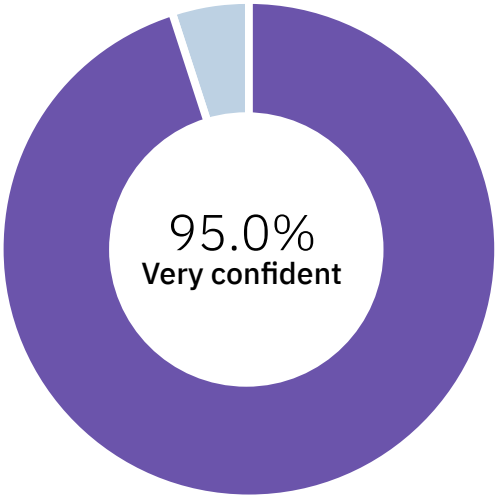
France



Italy



Singapore



Architecting the Future of Cyber Defense

AI is increasingly used to orchestrate "narrative attacks" or misinformation campaigns that can severely damage an organization's reputation. Such campaigns manipulate facts or fabricate stories, often using advanced techniques like deepfakes, to misrepresent reality convincingly. Nearly all (97%) of IT/Security professionals surveyed consider the manipulation or creation of deceptive content as a significant threat, with more than a third (36%) viewing it as very significant.

Deepfakes, in particular, can make fraudulent claims or damaging statements appear shockingly authentic, reinforcing false narratives with high-fidelity audio or video content. Despite a substantial majority (74%) expressing confidence in their colleague's ability to identify such deepfake attacks, about 21% are not confident, and 5% are unsure, indicating a significant vulnerability. In security, experience has shown that overconfidence in stopping a specific threat often leads to greater vulnerability, especially for rapidly evolving threats.

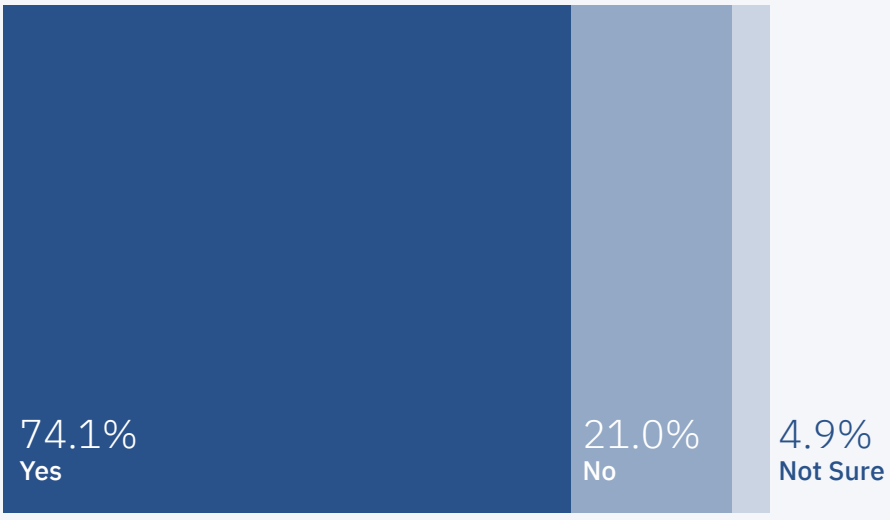
The manipulation from deepfakes is not just about spreading false information; it targets critical aspects of an organization, such as allegations of staff or customer mistreatment, fraudulent activities, or covered-up data breaches.

Depending on its nature, each narrative can erode customer trust dramatically—particularly in sensitive sectors like FinTech, where trust is a fundamental currency. The impact on an organization's reputation can be profound and long-lasting, which is why nearly all professionals (96%) acknowledge that disinformation and misinformation campaigns facilitated by AI pose substantial threats.

Question

Are you confident your colleagues from your department could spot a deepfake (audio/video) type of attack?

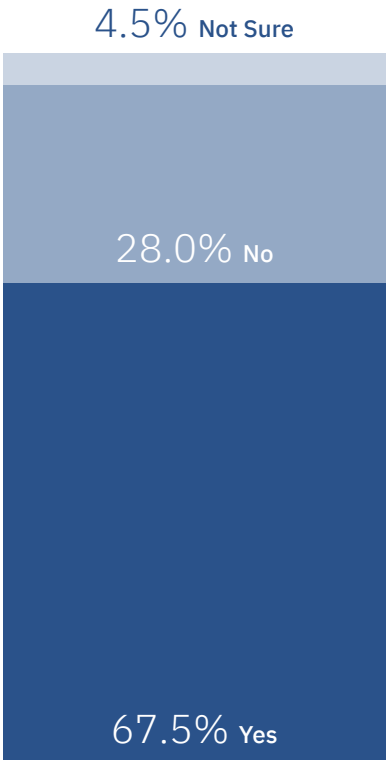
Overall



USA

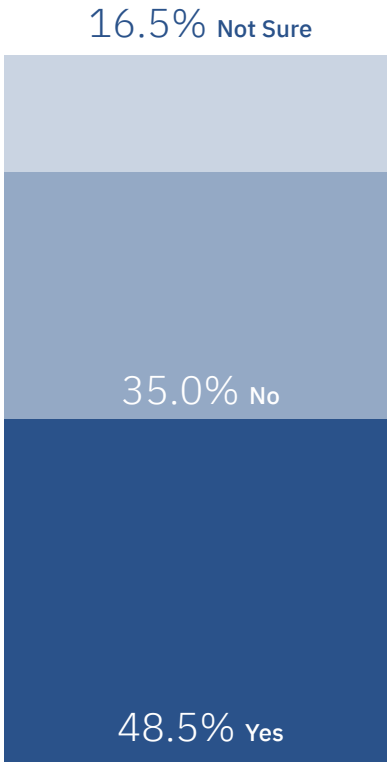
Germany

UK



France

Italy



Singapore

The Human Factor: Strengthening the Frontlines of Cyber Defense

AI-related data privacy breaches are seen as a significant threat by 97% of surveyed professionals, with nearly two in five (37%) considering them very significant. This is partially because of AI's potential to influence various aspects of society, including political processes. As we approach the upcoming US election, there is a growing expectation that AI will play a significant role, possibly impacting outcomes through the amplification of narrative attacks or misinformation campaigns. These breaches, facilitated by AI, can come in various forms—from creating and spreading deceptive content to manipulating public opinion.

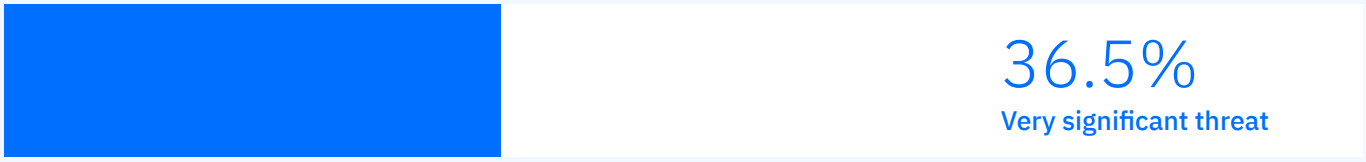
Using AI, attackers can improve their phishing tactics, leading to more successful malware dissemination. Attackers can also utilize AI to assess volumes of vulnerability data, helping sort through the chaff to find likely targets and strategies. While platforms like ChatGPT are designed with controls to prevent misuse, savvy attackers often find ways to circumvent these measures or even develop their own AI tools tailored for malicious purposes. This evolving threat landscape underscores the need for continuous advancements in cybersecurity defenses to counteract AI-powered attacks.

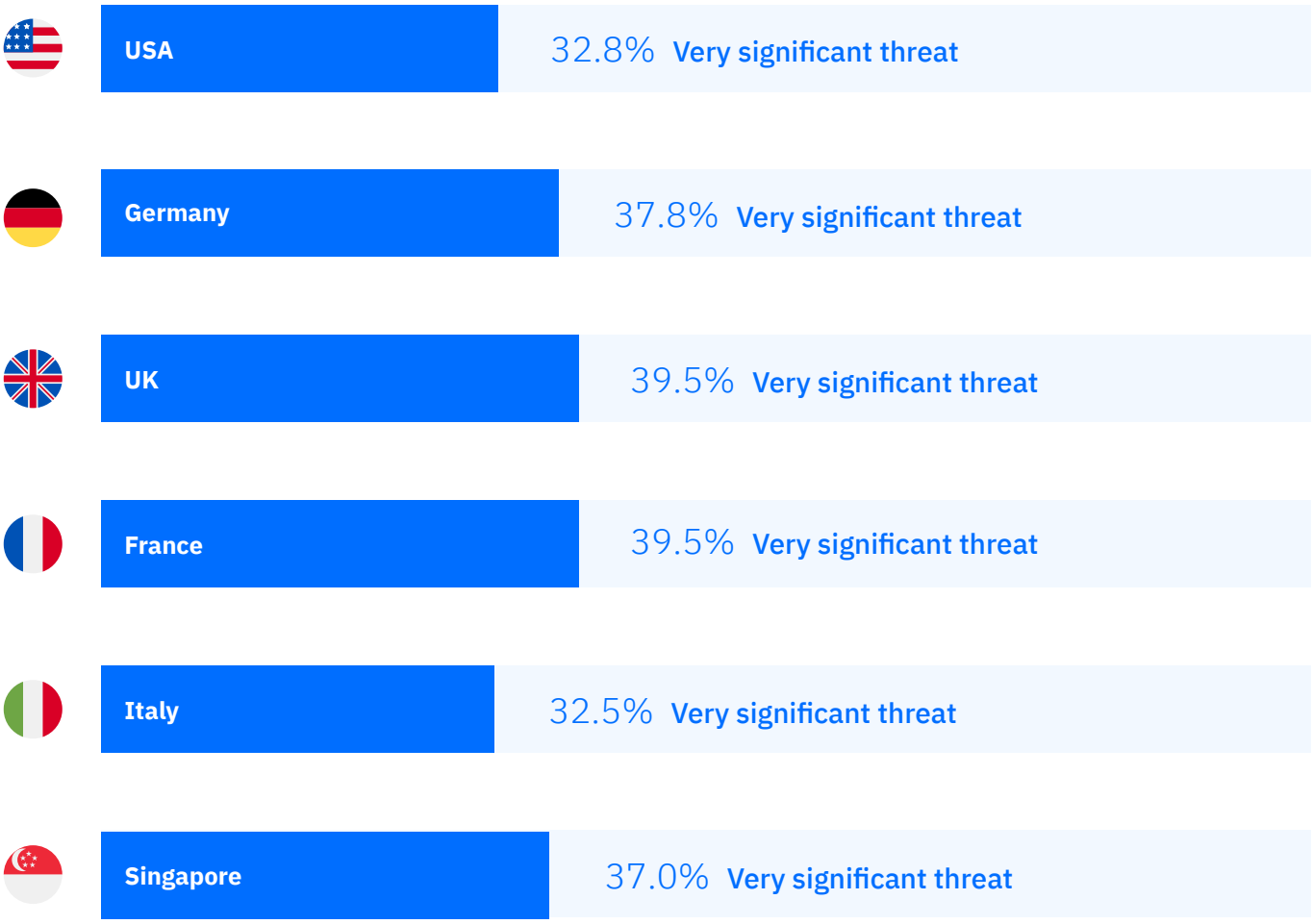
Large Language Models (LLMs) like ChatGPT are constructed using vast amounts of data, sometimes including sensitive information. Many organizations extensively use these models as part of their internal AI toolsets. However, breaches can occur despite robust security measures like sandboxing to isolate and protect such data. Innovative attacks are increasingly capable of breaking out of these protective sandboxes, gaining access to data that should be securely out of reach.

Question

How much of a threat, if at all, do you perceive Generative AI technology to be in the cybersecurity landscape when it comes to data privacy breaches as a result of AI?

Overall





Pioneering Proactive Cybersecurity: A Vision for Preemption

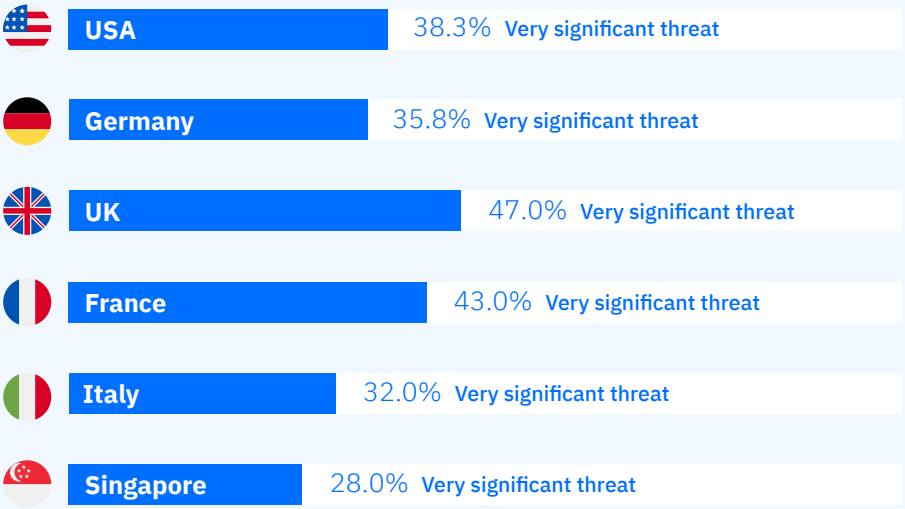
While attackers can exploit AI tools, corporations also harness AI to enhance their defensive capabilities. Many organizations are now considering integrating AI into their security systems to potentially identify and address vulnerabilities proactively before they can be exploited. This integration often involves AI analyzing vast datasets to detect potential threats quickly and efficiently.

However, as AI is not yet a standard component of security infrastructures, so concerns about over-reliance on these systems are starting to emerge. The fear is that excessive dependence on AI for security decision-making could lead to complacency, reduced human oversight, and a failure to catch anomalies that AI might miss. This concern is reflected in the sentiments of the cybersecurity community, where 96% of professionals view the over-reliance on AI as a potential threat, and nearly 2 in 5 (37%) consider it a very significant risk.

Question

How much of a threat, if at all, do you perceive Generative AI technology to be in the cybersecurity landscape when it comes to over-reliance on AI for security decision-making?

Overall



Navigating the Aftermath of Cyber Breaches

Despite the best efforts to maintain robust security protocols, incidents are inevitable. Unfortunately, incidents are not only common but can also be incredibly costly for organizations. The expenses associated with incidents stem from several sources, compounding their impact. Initially, there's the direct cost of addressing and rectifying the incident, which includes technical investigations and remediations. Beyond the immediate financial outlays, organizations often face significant losses in productivity as operations may need to pause or slow down to manage the breach response. Potential legal and regulatory fines exist, particularly if the breach involves sensitive customer data and violates compliance mandates. Perhaps most damaging in the long run is the impact on an organization's reputation, which can erode customer trust and loyalty, leading to a decline in business and future revenue. Numerous studies have shown that a significant percentage of businesses experience customer loss and reputational damage following a breach.

Overcoming Technological Complexity in Cybersecurity

Managing security becomes increasingly complex as technology advances and attack surfaces expand, often giving attackers the upper hand. This complexity is exacerbated when technology fails to meet expectations, a sentiment echoed by most professionals; 71% feel that their security solutions have not lived up to the promised hype, a significant increase from 54% last year. This is likely due to an abundance of products promising AI/ML integration but not delivering improved detection or accuracy.

These challenges are compounded by the sheer volume and diversity of solutions available, with nearly a quarter of respondents indicating that there are too many systems to manage effectively. This has led to calls for vendor consolidation, particularly noted as a top priority in the UK, where organizations seek to streamline their security operations. These organizations are not just looking for any solution; they demand proven, reliable systems that integrate seamlessly, simplifying the management and monitoring interfaces.

Other notable challenges include managing the complexity of systems (23%), enhancing reporting capabilities (23%), and reducing unnecessary features (20%), all of which contribute to the difficulty in maintaining a secure and efficient operational environment. Addressing these issues involves not only selecting the right tools but also ensuring that they work cohesively to enhance security without adding undue burden. This holistic approach to selecting and integrating security solutions is critical in reducing vulnerabilities and improving overall cybersecurity posture.

71% feel that their security solutions have not lived up to the promised hype, a significant increase from 54% last year.

Question

What, if anything, are the biggest challenges about your current security solutions?

Respondents selected up to three of their top choices.

Overall

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

USA

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

Germany

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

UK

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

France

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

Italy

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

Singapore

Adhering to data compliance and regulations

Extending capabilities across multiple environments (on-premises, cloud, hybrid).

Incompatibility with other security solutions

Addressing the Cybersecurity Talent Crunch

Staffing challenges are a significant and ongoing issue in security operations. The cybersecurity industry continues to grapple with a chronic shortage of almost 4 million skilled professionals, exacerbating an already tense situation within many organizations. This talent scarcity strains existing staff and contributes to a cycle of dissatisfaction and burnout among employees. As a result, when staff members leave—overwhelmed by the workload and underappreciated—they inadvertently increase the pressure on their remaining colleagues. This often leads to reduced effectiveness, as overburdened teams cannot maintain the same level of vigilance, potentially missing threats that could otherwise have been identified and mitigated.

Statistics reveal the depth of this issue, with more than 70% of security professionals working weekends, a clear indicator of burnout and overload. This intense workload correlates strongly with job dissatisfaction; notably, 64% or three out of five security professionals are considering new job opportunities within the next year.

To address these challenges, organizations urgently need solutions that alleviate the burden on their security teams. Such measures enhance the work environment and improve the overall efficacy of security operations, ensuring that critical threats are not overlooked.

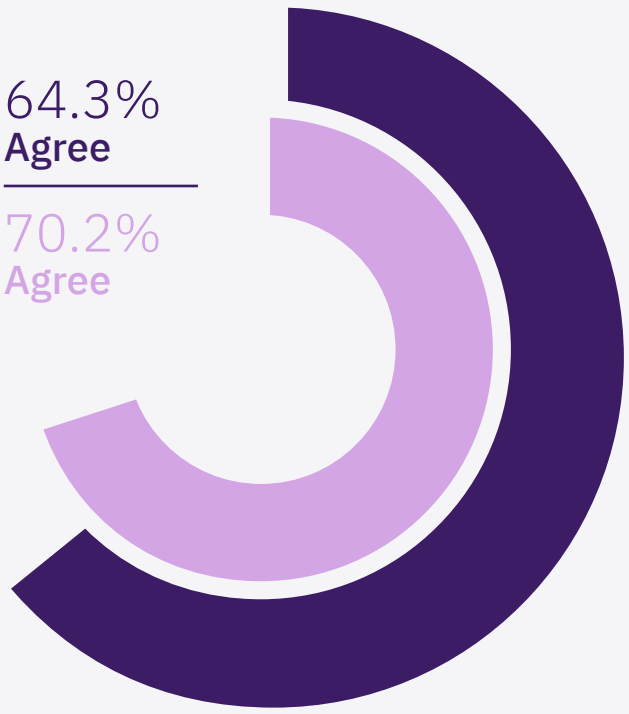
Question

How much do you agree or disagree with the following statements?

I am planning on looking for a new job in the next 12 months

I often have to work at weekends due to security concerns that my company faces

Overall



I am planning on looking for a new job in the next 12 months

I often have to work at weekends due to security concerns that my company faces

USA

62.2%
Agree

70.2%
Agree

Germany

76.6%
Agree

77.1%
Agree

UK

71.0%
Agree

81.0%
Agree

France

69.0%
Agree

70.5%
Agree

Italy

61.5%
Agree

64.0%
Agree

Singapore

45.5%
Agree

58.5%
Agree

Proactive and Reactive: Dual Forces in Cybersecurity

Organizations are increasingly focusing on mitigating threats before they escalate into significant breaches. The rationale is clear: while prevention is not a foolproof solution, it is invaluable in minimizing the impact of potential security incidents. By stopping threats early in their tracks, organizations can limit the extent and severity of damage.

However, despite the best preventive measures, the unpredictable nature of cyber threats means that incidents can still occur. Therefore, reactive capabilities remain essential components of a robust cybersecurity framework. The ability to respond swiftly and effectively when a breach occurs is critical, ensuring that organizations can quickly contain and remediate any damage. This dual approach, combining proactive prevention with prepared and responsive action, forms the cornerstone of modern cybersecurity strategies.

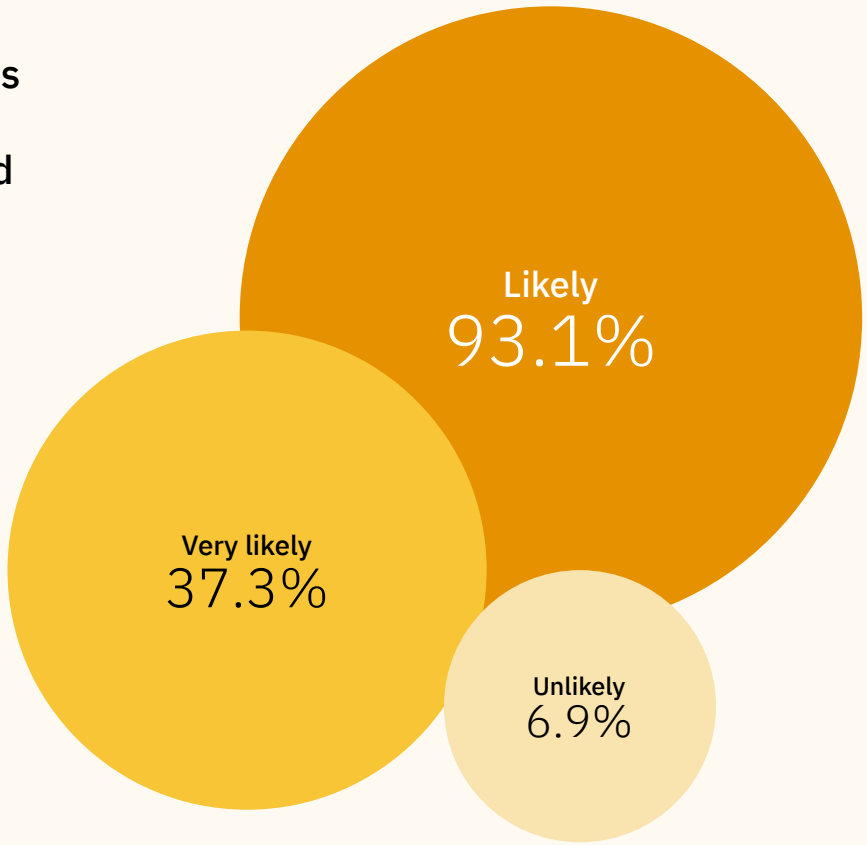
Fortifying Frontlines: Amplifying Investment in Proactive Cybersecurity

There is also a growing trend among IT and security professionals towards bolstering their defenses with proactive continuous security measures. A significant majority, over 93% of professionals surveyed, indicate a likelihood to increase their investment in critical proactive strategies such as risk assessments, penetration testing, and red team exercises. This data highlights a strong commitment within the industry to enhance security frameworks before issues arise. Specifically, more than half (56%) are likely to implement these measures soon, while nearly two in five (37%) are very likely to do so, demonstrating a robust inclination towards proactive security initiatives. Conversely, less than one in ten (7%) are unlikely to increase their investment in these areas, suggesting a broad consensus on the value of preemptive action.

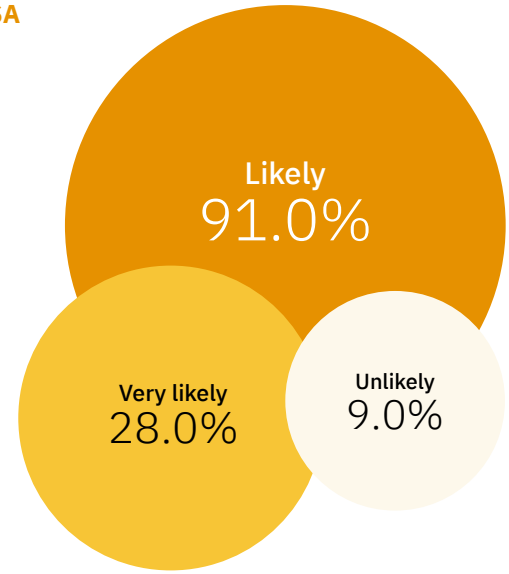
Question

How likely, if at all, are you to increase investment in proactive security measures such as risk assessment, penetration testing, and red team exercises soon?

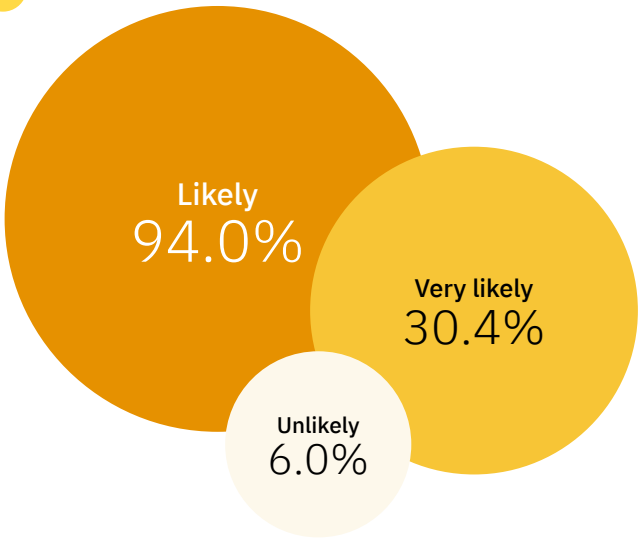
Overall



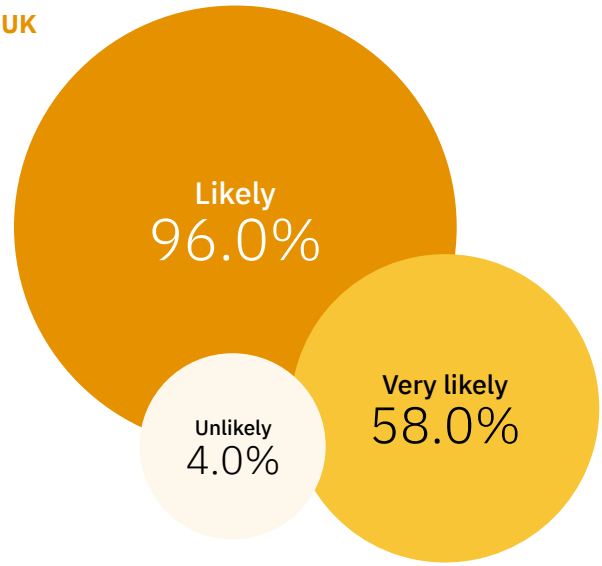
USA



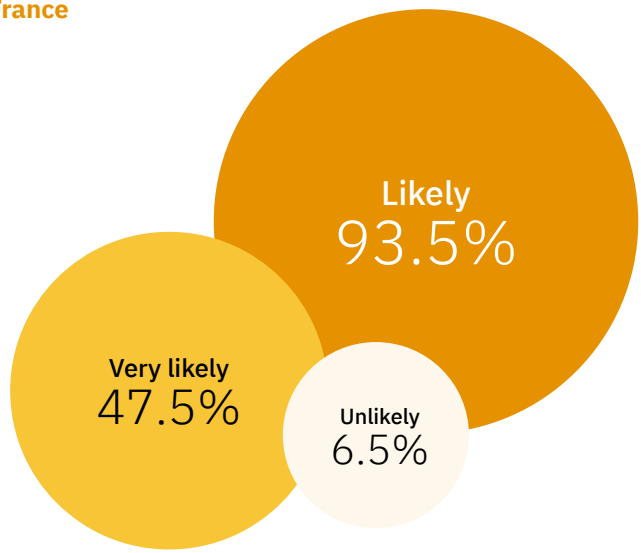
Germany



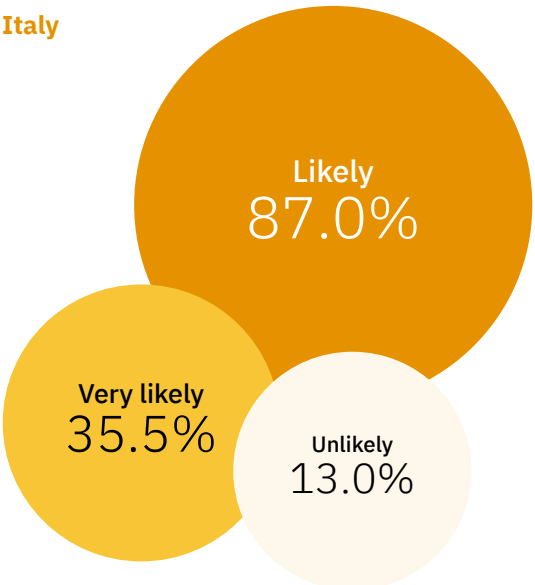
UK



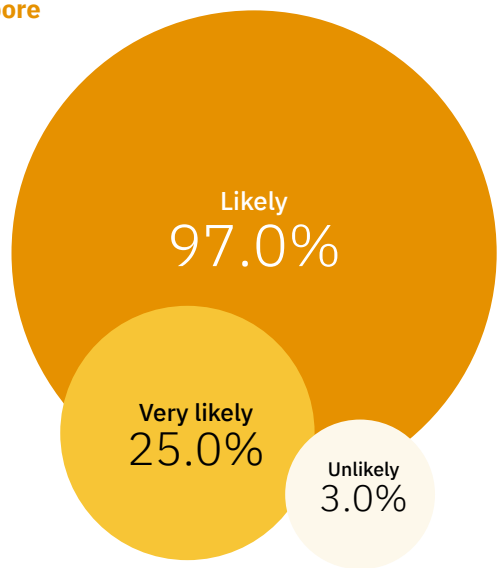
France



Italy



Singapore



Elevating Security: The Critical Role of Managed Detection and Response

Managed detection and response (MDR) is one of the top solutions for proactively managing security threats and is increasingly recognized as a vital component of a holistic security strategy. Organizations choose MDR for several key reasons. Among the primary drivers, 33% of IT/Security professionals emphasize the importance of 24x7 security coverage, ensuring that threats are identified and addressed promptly, day or night.

Similarly, 29% value access to security analyst expertise, which MDR provides without requiring extensive in-house capabilities. This expertise is especially critical for proactive threat hunting, which was highlighted by 29% of respondents. It helps identify potential vulnerabilities before they can be exploited.

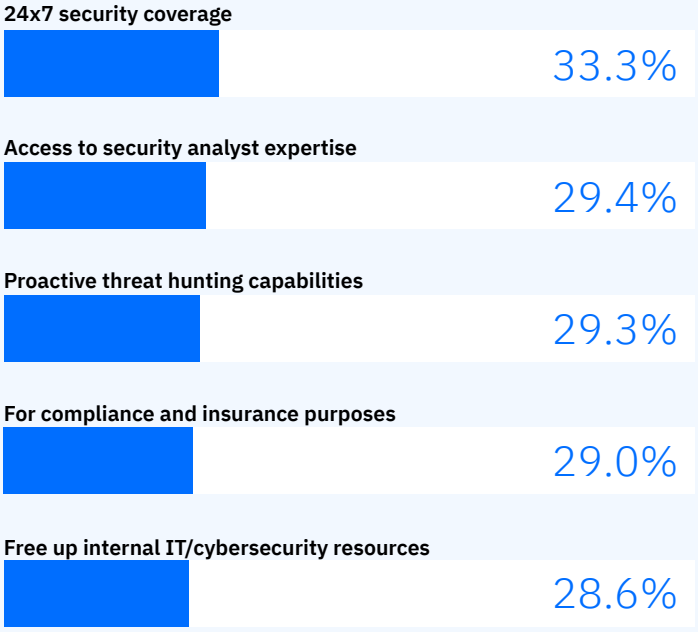
Compliance and insurance purposes, as well as the need to free up internal IT and cybersecurity resources were also of importance—each cited by 29% of professionals—highlighting MDR's role in enhancing security and optimizing organizational efficiency. Additionally, 28% of respondents pointed to acquiring actionable intelligence, rather than just a flood of alerts, as a significant benefit, providing clarity and focus in security operations. Peace of mind, mentioned by 27%, and the fact that a quarter of professionals feel overwhelmed by the complexity of the threat landscape further validate the growing reliance on MDR services.

Question

If you currently utilize, or are contemplating the use of a managed detection and response (MDR) provider, what personnel-related factors, if any, primarily drive this decision?

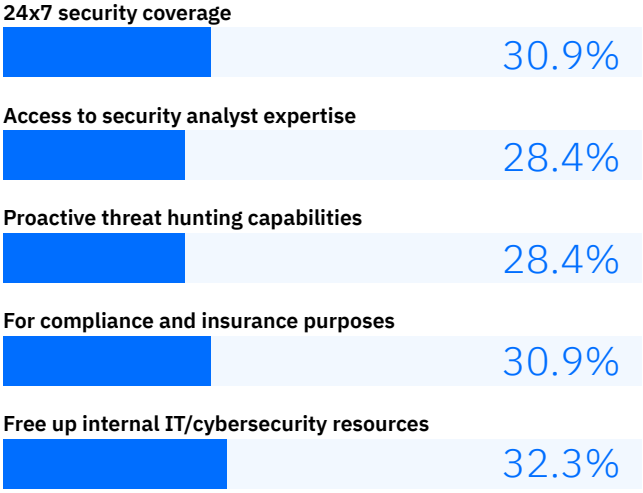
Respondents selected up to three of their top choices.

Overall



USA

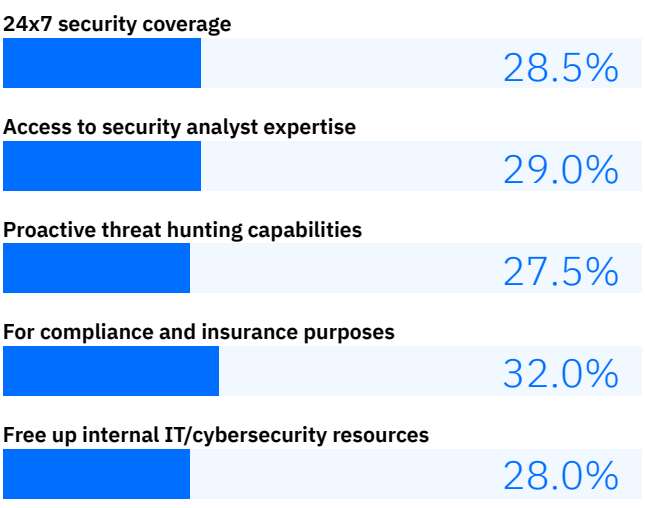
Germany



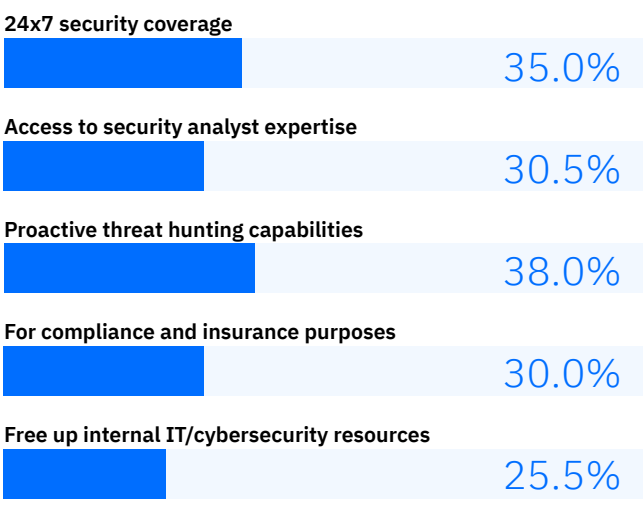
UK

France

Italy



Singapore



Bitdefender

Building a Fortress: Defense in Depth Strategies for Today's Cyber Threats

Organizations are increasingly adopting cloud technologies to boost efficiency and agility. However, the rapid embrace of these technologies often outpaces the implementation of adequate security measures. This discrepancy leaves significant vulnerabilities, with 44% of organizations worried about data breaches or leaks, 43% concerned about unauthorized access, and another 43% troubled by misconfigured cloud storage. Consequently, the cloud presents as much risk as it does benefit.

As these organizations look to further enhance their operations, many see artificial intelligence (AI) as the next evolutionary step beyond the cloud. Yet, this advancement introduces complex challenges. AI not only offers opportunities to strengthen security protocols but also equips attackers with more sophisticated tools. Notably, 96% of cybersecurity professionals recognize AI-enhanced social engineering attacks as a substantial threat, illustrating AI's dual role in both augmenting defenses and expanding attack vectors.

Amid these technological advancements, the human element remains a critical vulnerability. Approximately 48% of teams report significant skill gaps that hamper their ability to manage security effectively. This chronic shortage of skilled cybersecurity professionals not only puts additional pressure on existing staff but also compromises vigilance and overall security posture.

To address the myriad of cybersecurity threats effectively, a defense-in-depth strategy is essential. This approach begins with establishing a secure foundation for cloud environments, primarily through Cloud Security Posture Management (CSPM). CSPM tools play a pivotal role by automating the identification and remediation of risks associated with misconfigured cloud resources. By ensuring a robust baseline of cloud security, these tools help prevent potential breaches, setting the stage for a comprehensive, layered defense strategy that adapts to both current and emerging threats.

Building upon this foundation, organizations should integrate extended detection and response (XDR) and MDR to fortify defenses further. XDR enhances security by offering holistic visibility and correlation across all data points—endpoints, networks, cloud services, and applications.

This comprehensive view is crucial for detecting abnormal behaviors and potential threats to AI systems, allowing for the identification of sophisticated attacks, such as zero-day exploits and AI-specific threats like model poisoning. Advanced analytics and machine learning enable XDR to predict and prevent incidents before they escalate.

MDR complements these capabilities by providing 24/7 monitoring and threat hunting, ensuring continuous oversight of the IT environment, including AI systems. MDR teams are adept at navigating complex and evolving threat landscapes, providing an invaluable layer of expertise that helps identify early signs of targeted AI attacks. Additionally, in the event of a security breach, MDR's rapid incident response and remediation efforts are critical to minimizing downtime and restoring operations swiftly.

45%

Less than half of organizations are conducting regular audits/ assessments across their cloud infrastructure.

57%

More than half of organizations experienced a data breach or leak in the last 12 months (up 6% from previous year).

Together, CSPM, XDR, and MDR form a multi-layered security strategy that allows organizations to preemptively identify and mitigate threats, ensuring a proactive stance against the challenges posed by modern attack surfaces. This integrated approach secures existing infrastructure and adapts to the evolving nature of threats.

96%

Nearly all respondents are concerned about AI's impact on the threat landscape.

Bitdefender Business Solutions

Bitdefender delivers solutions that enhance an organization's ability to withstand cyber-attacks by providing comprehensive threat prevention, detection, investigation, and response across their entire environment, including identity, email, cloud, network, and endpoints.

The Bitdefender Labs serves as a research institute and a source for engineering innovations and threat intelligence. Its deep ties with academia enable cutting-edge developments in ML/AI, neural networks, and quantum security, while Bitdefender's extended collaboration with Global law enforcement agencies plays a pivotal role in disrupting cybercriminal activities.

Bitdefender's proprietary technologies, trusted by hundreds of cybersecurity vendors, ensure robust protection for our customers against even the most severe threats. With the GravityZone unified security platform, organizations can boost their operational efficiency and enhance security effectiveness, providing more core features out-of-the-box than other security technology providers.

Organizations choose Bitdefender to optimize their cybersecurity investments and safeguard their operations.

bitdefender.com/business