CYBERARK®

SECURITY MATTERS

Identity Security

Threat Landscape EMEA Report 2024

Cyber debt builds with GenAI, rise of machine identities, third- and fourth-party risks.

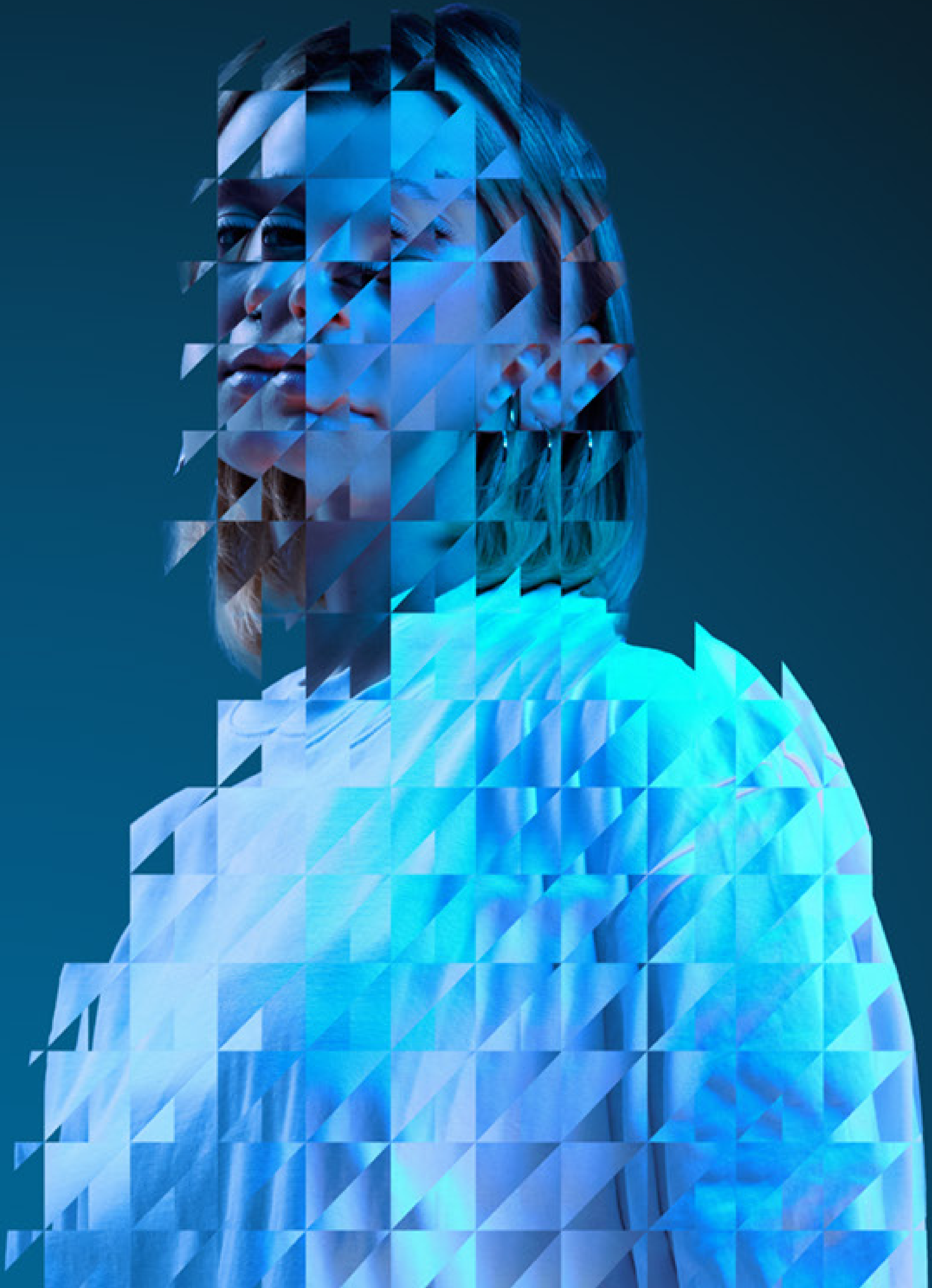
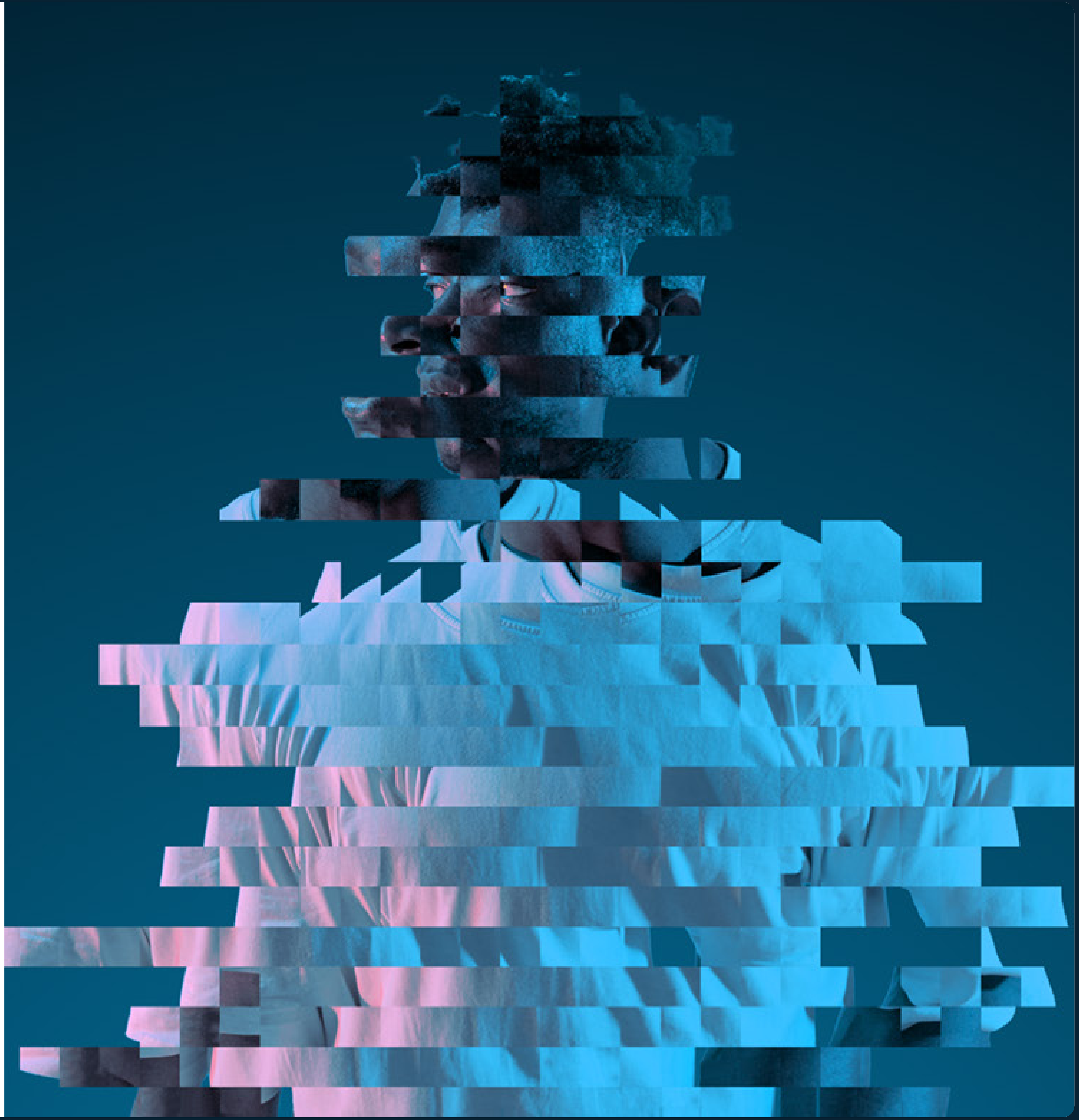


Table of Contents



Executive Summary

Executive Summary

CyberArk 2024 Identity Security Threat Landscape EMEA Report is a survey of 1,050 security decision-makers across 8 countries that examines how cyberattacks impact identity. This year we find that cyber debt continues to build with GenAI, rise of machine identities, and increasing third- and fourth-party risks.

We kick off this year's findings with a metaphor: if innovation is water, a glass is fine, a faucet is divine, but a firehose is a very bad time. We wax poetic not to torture you but to drive home the absolute tsunami of new identities, new environments and new attack methods that are pummeling and muddying the threat landscape in 2024.

Nearly half of organisations anticipate a threefold increase in the total number of identities, with machine identities squarely in the driver's seat (but largely under-secured and over-privileged). This growth in vulnerable identities, boosted by the widespread use of multi-cloud strategies, is a here-and-now threat ready to be exploited by bad actors with the AI-powered ability to execute at scale.

Of course, this is nobody's first rodeo with Generative AI. Nearly all surveyed organisations (and their adversaries) are using it. What is new is the rise in the volume of identity-related attacks, the increasing sophistication of election-year deepfakes — and a disturbing confidence among C-level leaders that their employees can identify realistic fake video or audio of their leaders. Our report also uncovered a lack of rigorous focus on vendor risk management, despite the growing web of our digital ecosystems. Third- and fourth-party breaches can easily cascade to your organization, creating a multiplier effect on risk.

Under a deluge of digital transformation, AI and identity-related attacks, it's tempting to adopt that shiny new tech to solve a unique use case or simply for fear of missing out on the market buzz — and incur hefty cyber debt. But with eyes on that shiny new tech, beware of the blind spot: phishing and vishing attacks. While far less interesting, these tried-and-true attack methods remain highly effective and lead to breaches and significant financial loss for 9 out of 10 organisations.

> In the last 12 months, 93% of organisations suffered two or more identity-related breaches.

In the last 12 months, 93% of organisations suffered two or more identity-related breaches. And, with 94% of our respondents using more than 10 vendors for identity-related cybersecurity initiatives, organisations find themselves tangled in a fishing line of multiple systems, applications, and services across different platforms and locations. While the attack vector is vast-bordering-on-dystopian, the slow and steady **consolidation of trust** (consolidation of tools with experienced, expert, innovative and trusted partners) could very well win this race.

Finally, we believe the imperative to establish a robust cybersecurity posture starts with securing every identity across the enterprise. Getting there requires a new cybersecurity model centered on identity security. Siloed, legacy solutions were built to solve yesterday's problems. The future of security starts with identity.

Key Findings

IDENTITY-RELATED BREACHES

94%

experienced an identity-related breach at least once in the last 12 months.

93%

experienced two or more identity-related breaches in the last 12 months.

NEW IDENTITIES

47%

Nearly half (47%) expect identities to grow at least 3x in the next 12 months (the average is 2.3x).

62%

of organisations define a privileged user as human-only.

#1

Machine identities are the #1 driver of identity growth.

#1

Machine identities and third-party are the #1 riskiest identity types.

NEW ENVIRONMENTS

83%

In the next 12 months, 83% of organisations will use three or more CSPs.

88%

The number of SaaS applications will grow by 88%.

92%

are concerned about third-party risks.

83%

are concerned about fourth-party risks.

NEW ATTACK METHODS

90%

were targeted by ransomware at least once.

74%

affected by ransomware paid the ransom but did not recover their data.

99%

have adopted AI-powered tools.

95%

expect a variety of negative impacts on cybersecurity due to AI-powered tools.

70%+

are confident that their employees can identify deepfakes of their leaders.

● ● ● ● ● ● ● ● ● ○ **9/10**

9 out of 10 organisations have been a victim of a successful identity-related breach due to a phishing or vishing attack.

CYBER DEBT LEADS TO CONSOLIDATION OF TRUST

99%

suffered negative business impact from a breach.

94%

use more than 10 vendors for identity-related cybersecurity initiatives.

61%

of organisations have or will prioritize Zero Standing Privileges (ZSP) and passwordless authentication.

GenAI: Promise, Potential – And Peril

GenAI: Promise, Potential – And Peril

We begin our 2024 Threat Landscape report with the technology we hate to love and love to hate: Generative AI. Wherever you stand on it — friend, foe or the future — two trends are undeniable. First, AI-powered tools aren't going away (surprise, surprise). Our 2023 report indicated that 98% of EMEA organisations were leveraging AI in their identity-related cybersecurity initiatives. In 2024 all respondents (100%) report that they are leveraging GenAI in their identity-related cybersecurity initiatives. Unfortunately, so are the bad guys.

In EMEA, we predict an unparalleled increase in the volume and sophistication of identity-related attacks as skilled and unskilled bad actors leverage GenAI to intensify their assaults. Like our global findings, in the last 12 months, 9 of 10 organisations in EMEA were victims of a breach due to a phishing/vishing attack. These types of attacks will be harder to detect as AI will automate and personalize the attack process . Looking to the year ahead, organisations can expect to be affected by data leakage from compromised AI models, AI-powered malware, and phishing. And, with GenAI, even previously unaffected organisations will find themselves in the crosshairs — and will have to do damage control.

In EMEA, 94% expect a negative impact from AI-powered tools in the next 12 months.

Buckle up and Brace for Impact

Our respondents are bracing for a myriad of incoming GenAI-enabled threats, particularly deepfakes that will spawn an increasing number of successful phishing and/or vishing attacks.

This year, we find the top three reasons causing identity-related attacks are:

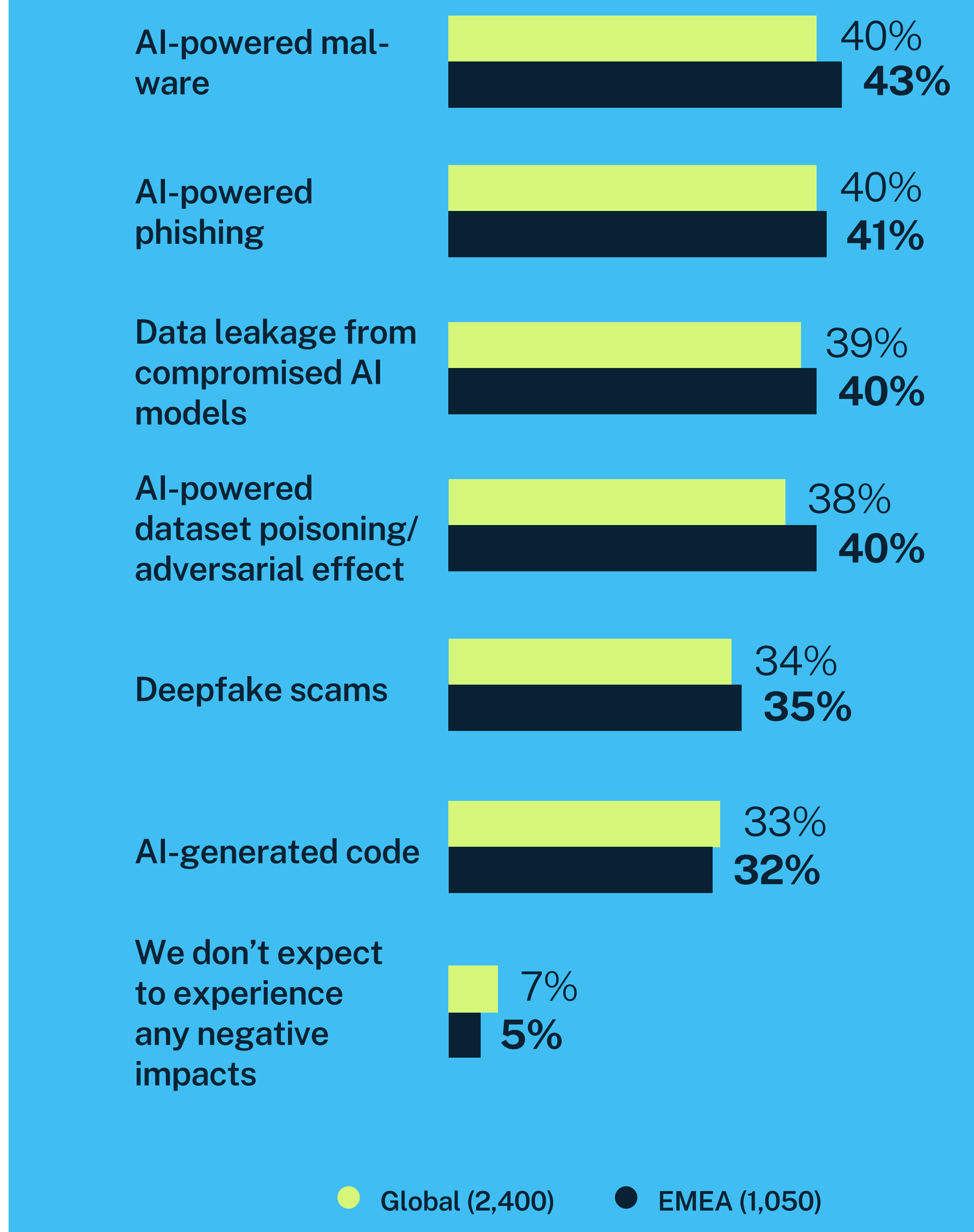
1. Digital transformation (EMEA 23%, Global 22%)
2. Vulnerable IAM infrastructure (EMEA 22%, Global 21%)
3. Volume & sophistication of cyberattacks (EMEA 19%, Global 20%)

What we asked:

What negative impacts, if any, do you expect from AI tools in the next year?

What we learned:

94% of EMEA organisations expect AI-related cybersecurity challenges, with malware and phishing topping the list.

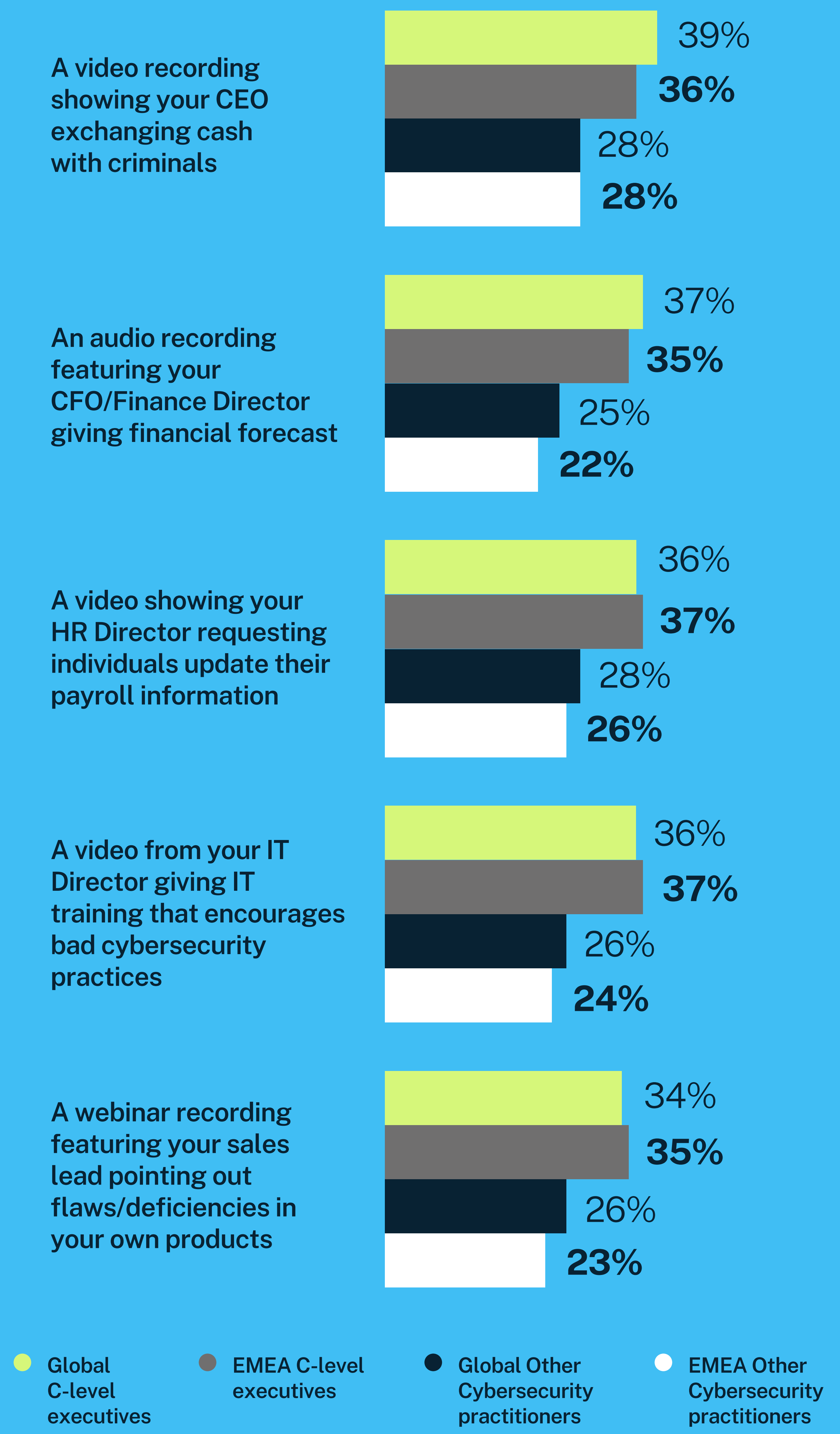


What we asked:

How confident are you that your employees can correctly identify the following deepfakes?

What we learned:

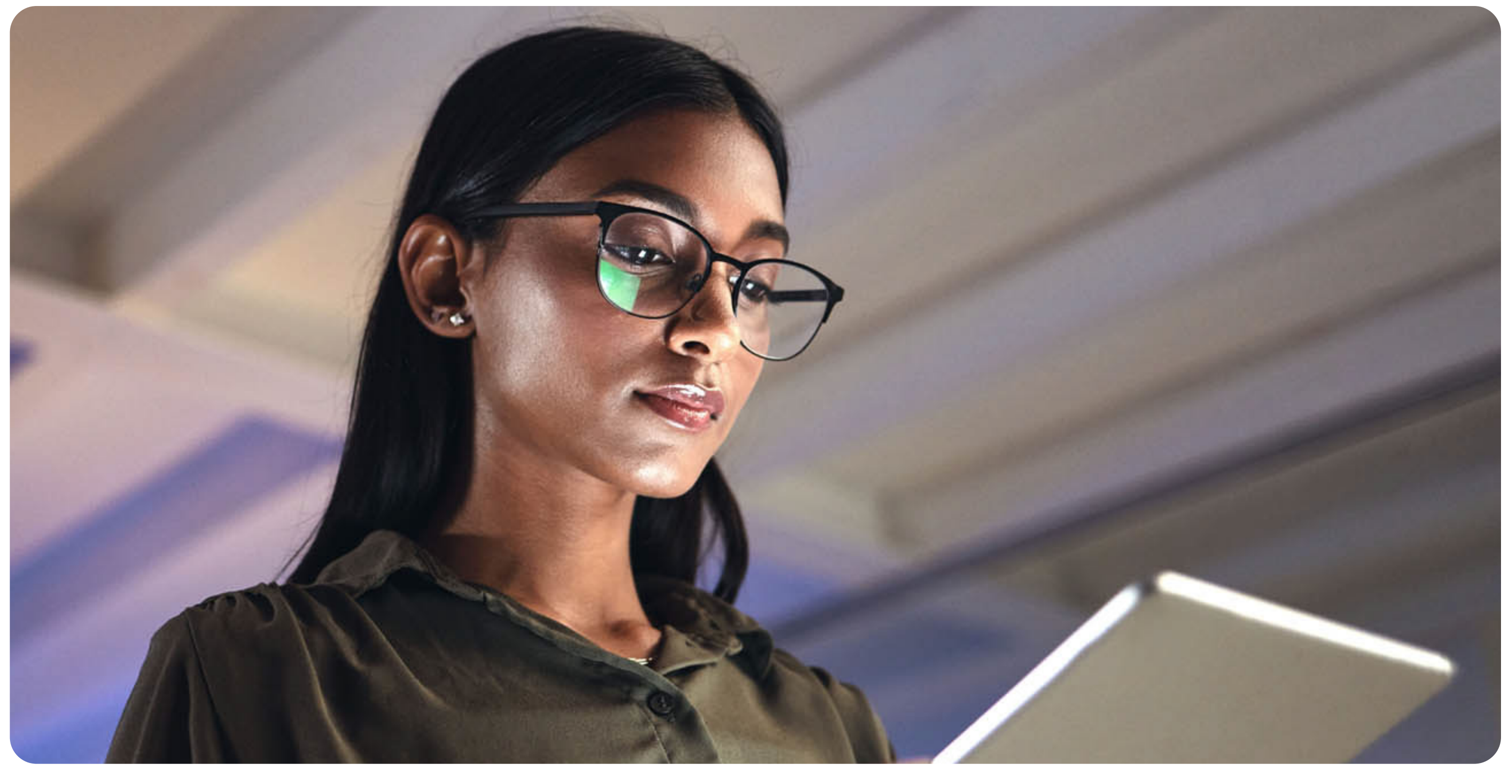
Compared to other cybersecurity leaders and practitioners, a majority of executives are **completely confident** that employees can spot deepfakes of their leaders.



This year, another up-and-comer joins the pain party: deepfakes. Perhaps the only thing more disturbing than the emergence of deepfake videos is our collective overconfidence that we won't be fooled by them. Nearly three-quarters of organisations are confident that their employees can identify B2B deepfake videos.

Are You Smarter Than a Deepfake?

The truth is, GenAI tools will produce increasingly realistic deepfake videos that will be hard for employees to identify and harder for cybersecurity teams to get in front of. Until we have tools sophisticated enough to detect and prevent deepfake scams, CISOs must focus on educating and building awareness with support and services teams on the frontlines of incoming technical help calls and emails.



Overconfidence: The Mother of All Biases

Our persona-level insights paint an interesting picture. We find that C-level executives in EMEA are entirely confident that their employees can identify these deepfakes compared to other cybersecurity leaders and practitioners surveyed in this report. This trend is consistent with our global findings.

Whether we chalk it up to the illusion of control, planning fallacy, or just plain human optimism, this level of systemic confidence is misguided. The full destructive potential of GenAI remains unknown, and we may not quite grasp how vulnerable we are.

CyberArk Insights

The rapid adoption of GenAI harkens back to another global phenomenon with a similar path of destruction: unregulated social media. To that end, we see significant urgency from governments around the world, eager to not repeat the same mistakes with GenAI.

In March 2023, the European Union passed the Artificial Intelligence Act, and eight months later, the United States issued an executive order 14110 or EO for Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. In EMEA, the message is clear: the responsibility for the safe usage of AI-powered tools lies squarely on the provider and users — with hefty penalties for misuse.

The providers are responding in kind. OpenAI is delaying the release of Sora AI to ensure content provenance and to enable users to identify real vs. increasingly real-looking but fake videos. Deepfakes put us all at increasing risk of widespread mis- and disinformation, phishing and vishing attacks, breaches, data loss, regulatory fines, and reputational damage at scales previously unknown to us.

What This Means for You

A deepfake video emerges of your CEO exchanging cash with a known criminal. Will your employees know what they're really seeing? It all depends on who you ask. According to our research, C-level executives have much more faith in their employees' deepfake detection abilities than cybersecurity experts.

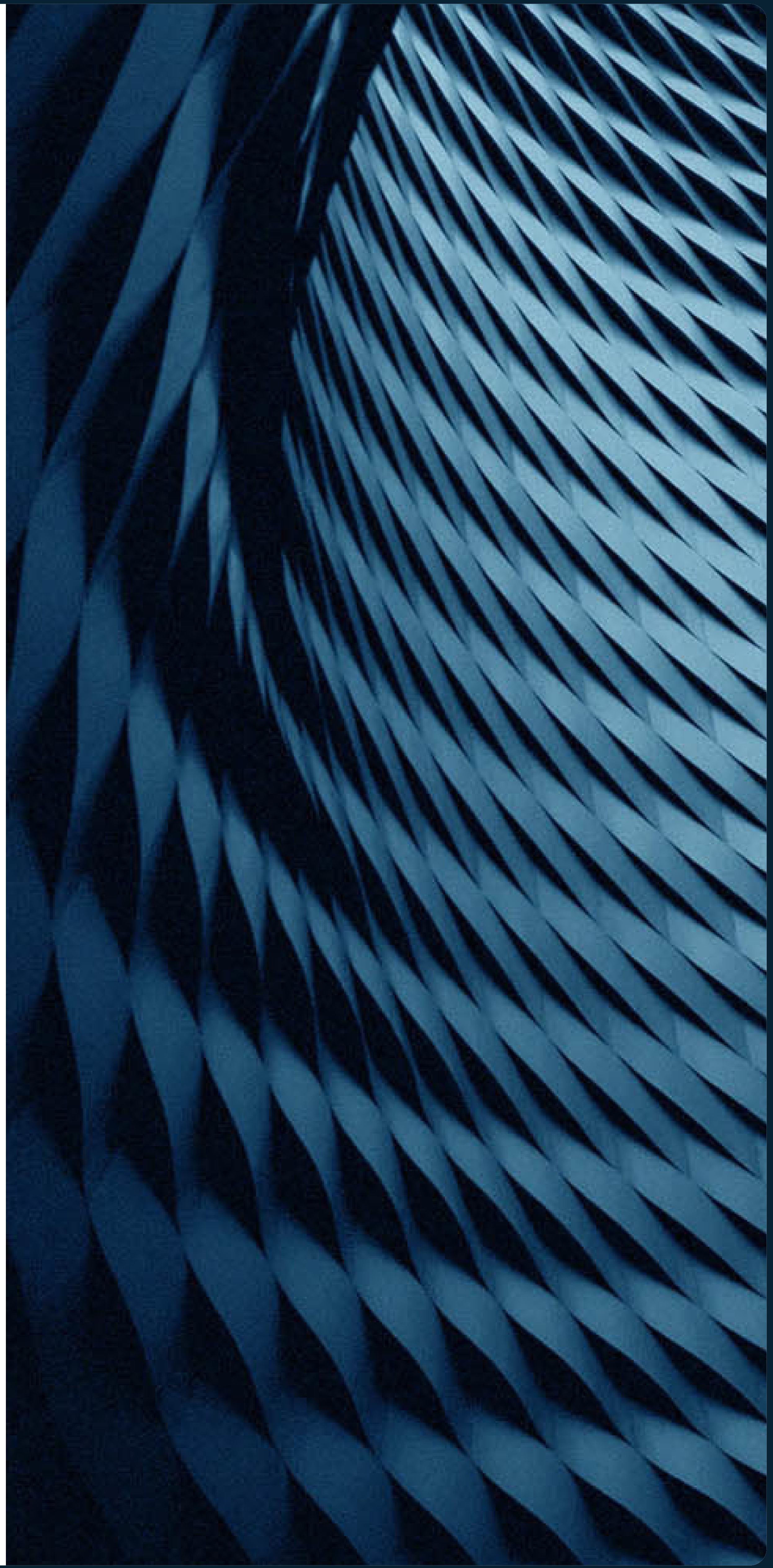
Our advice: Discuss this perception gap with stakeholders in your organization and identify why it might exist. Only when executives and cybersecurity teams are aligned can there be a path to resolution.

With 99% of organisations already adopting AI-powered tools in their identity-related cybersecurity initiatives, we urge you to consider scenarios where the AI that protects your organization is also under attack. Here are a few quick rules of thumb for introducing AI tools.

1. **Run It by Legal:**
   It's wise to include legal language in your contracts that lets you review their capabilities. This ensures the tool delivers exactly what it promised and meets your expectations.

2. **Handle (Data) With Care:**
   Take a close look at what types of data the AI tool accesses and retains. Think about how you can isolate and segregate tools to prevent any data tampering or leakage – especially if the data models get compromised.

3. **Awareness is Everything:**
   Don't cut corners on cybersecurity training for your service and support teams. They hold the front lines with customers and, potentially, bad actors.



New Era: Rise of the Machines

New Era: Rise of the Machines

By now, organisations understand that any human identity with access to sensitive data is a privileged user. But what about the non-human (machine) identities? Not to get too dystopian, but the classic human tendency to underestimate machines leads to our Bladerunner-esque downfall. Similarly, in a B2B setting, underestimating machines contributes to cybersecurity risk and makes them the most dangerous identities of all.

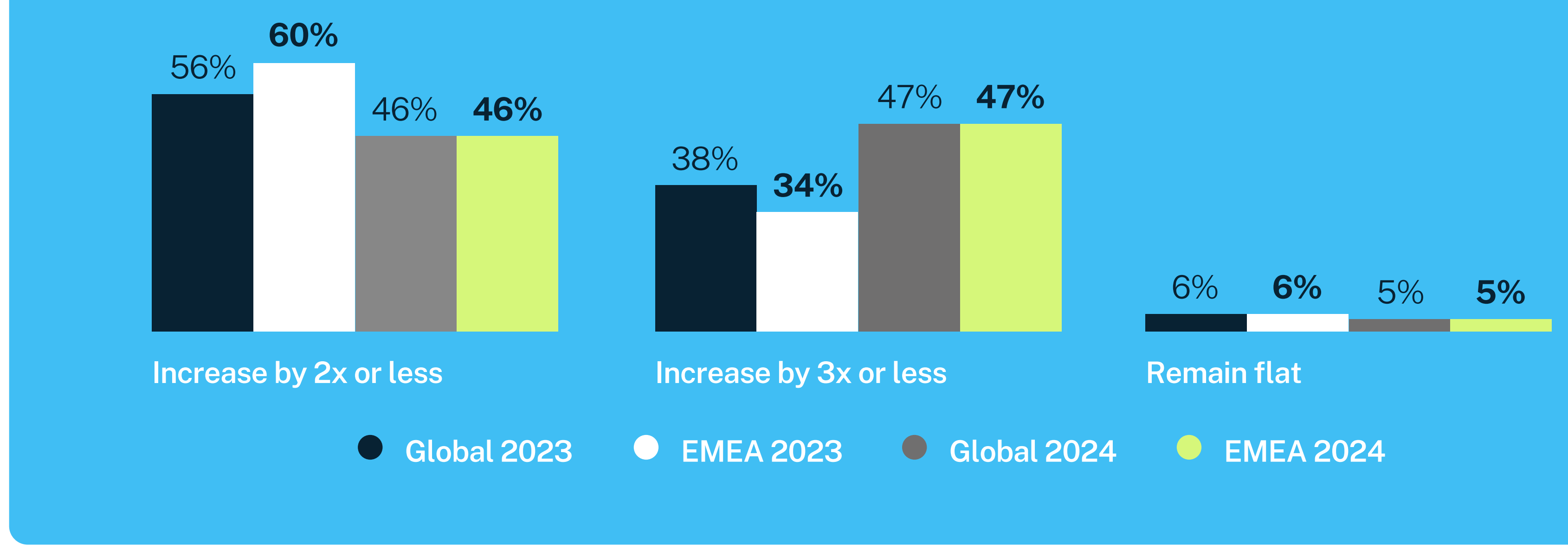
Over the next 12 months, we predict the number of identities to more than double (2.4x) in EMEA, following the same pattern we saw in our global responses in 2023 and 2024. Similar to our global findings, nearly half of this year's EMEA respondents expect an increase of three times or more in 2024 — a 24% increase from last year.

What we asked:

Over the next 12 months, how much do you expect the total number of human and machine identities within your organisation to increase?

What we learned:

Nearly 50% expect the total number to grow by 3x or more.



Sci-Fi 101: Don't Overlook the Machines

The growth of the total number of identities is neither new nor surprising. What is surprising is that nearly two-thirds of the organisations we surveyed have a very narrow definition of 'privileged user'. Access is power, and machine identities have more than we realize.

In 62% of EMEA organisations, the definition of a 'privileged user' applies solely to human identities.

The security controls we implement in our IT environments are only as good as the risks we define. With 9 out of 10 EMEA organisations naming phishing and vishing as the number one reason for an identity-related breach, we naturally focus all our security resources on the weakest link: human identities. However, according to our research, machine identities are the primary driving force behind the exponential growth of the total number of identities in EMEA. Humans are only one corner of a million-piece puzzle. After all, have you considered that it won't be long before chatbots or virtual assistants will be phished?

Repeat After Me: Machines Are Privileged Users Too

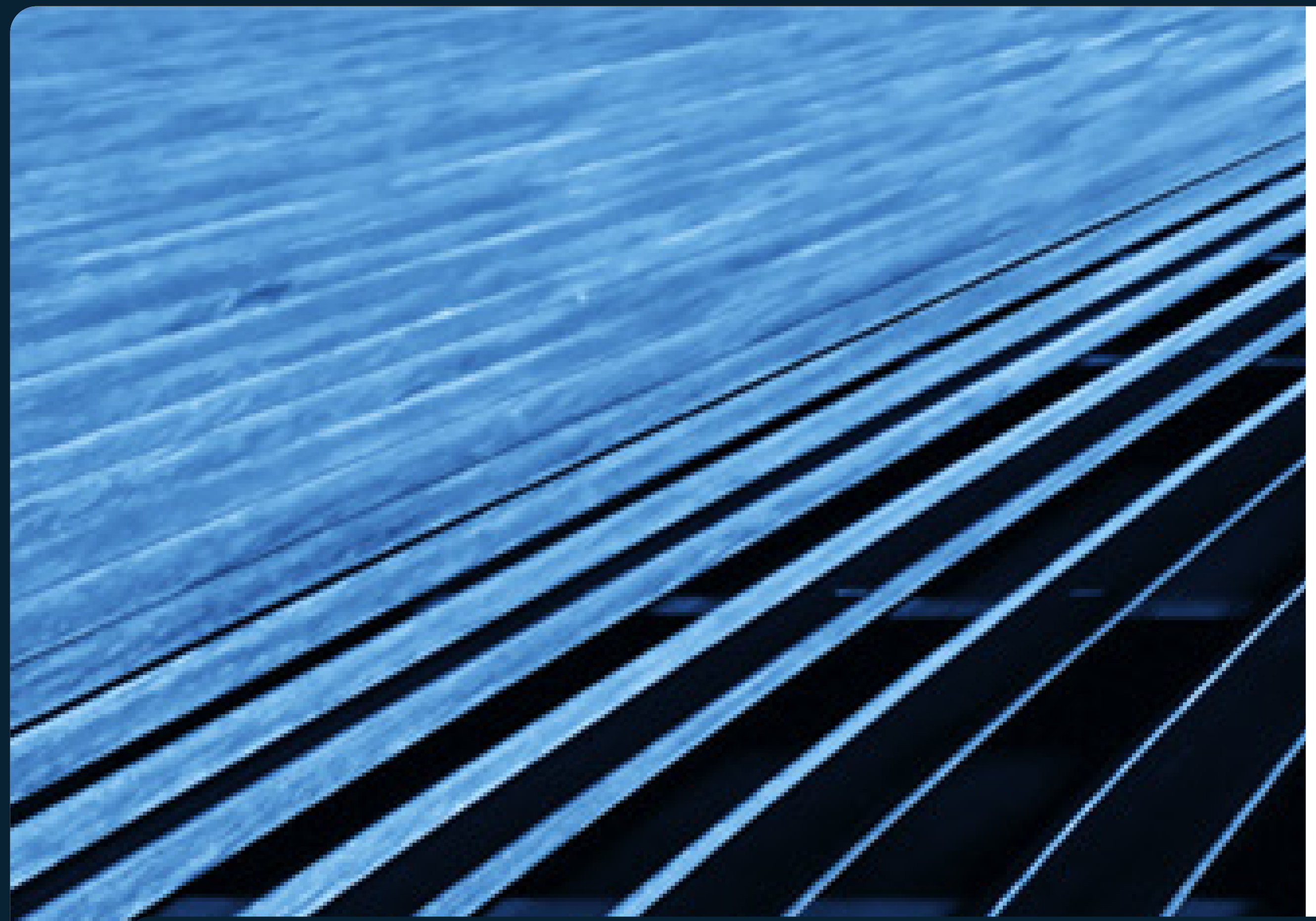
Nearly three-quarters (68%) of respondents indicate that up to 50% of all machine identities have access to sensitive data, compared to 64% who report that about half of human identities have access to sensitive data. With an increasing number of machine identities gaining access to sensitive data, 49% of our respondents identify them as the riskiest identity type.

And because of the lack of focus on securing machine identities, organisations report that their next biggest concern is a machine identity-related security incident that would require significant manual effort to address or remediate.

Manage Your Non-Humans Here

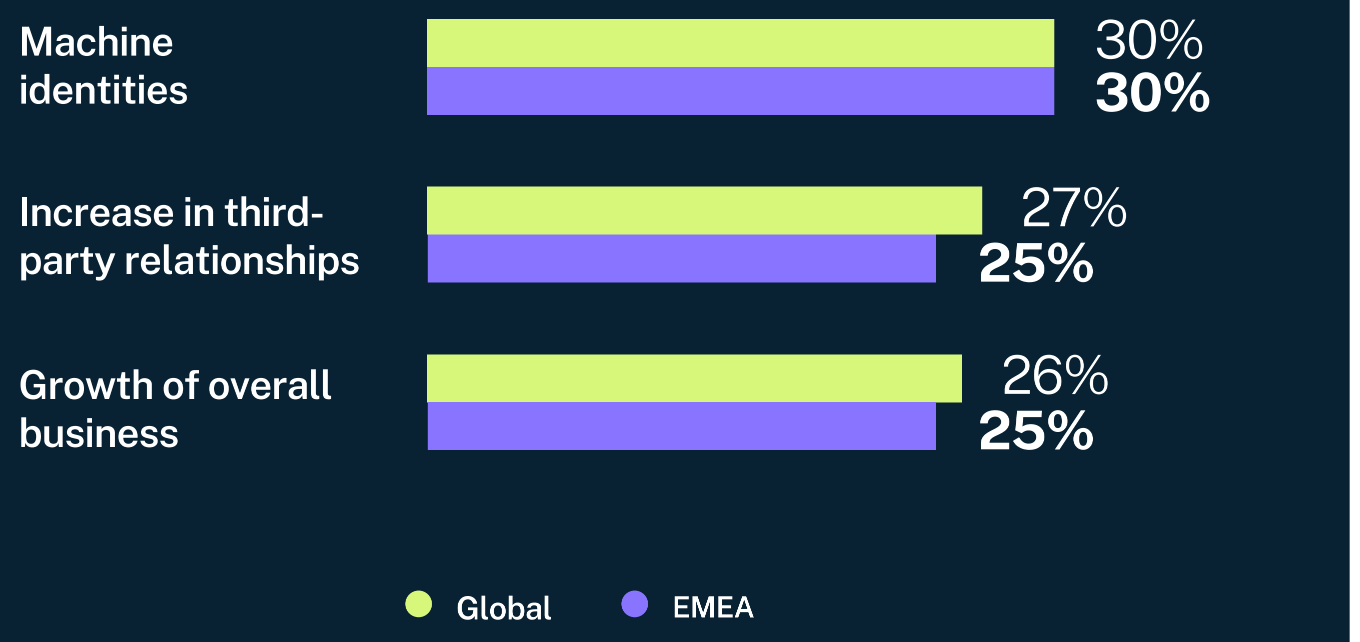
You need to secure risky, unknown and unmanaged machine identities. Where exactly should you start?

According to our respondents, the risk landscape has shifted away from business-critical applications (2023) to DevOps, CI/CD pipelines and development environments — followed by user machines and service accounts used by applications.



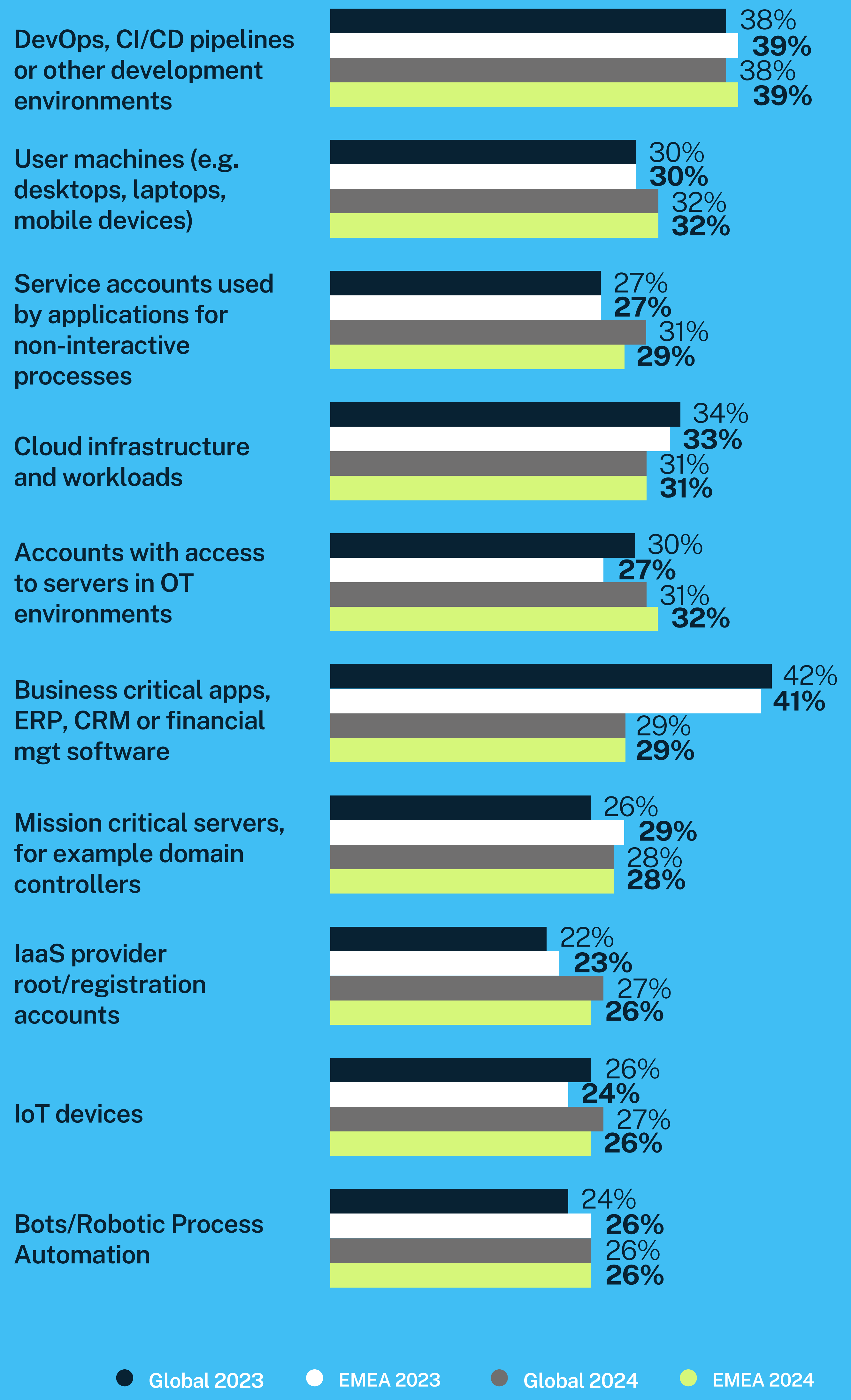
What we asked:
What is driving the increase in the number of identities under management at your organisation?

What we learned:
Machine identities are the #1 driver for overall identity growth in EMEA.



What we asked:
Where do the riskiest unknown, unmanaged identities live in your organization's IT environment?

What we learned:
DevOps, CI/CD pipelines, user machines, and service accounts are perceived as leading attack vectors.



CyberArk Insights

The message is clear. Machine identities are on the rise, and they have access to your sensitive data. With GenAI, machine identities will proliferate at a much faster pace in the near future. Your organization must reassess its definition of a privileged user to ensure every identity is secured. And (one more time for those in the back) this includes machine identities.

What This Means for You

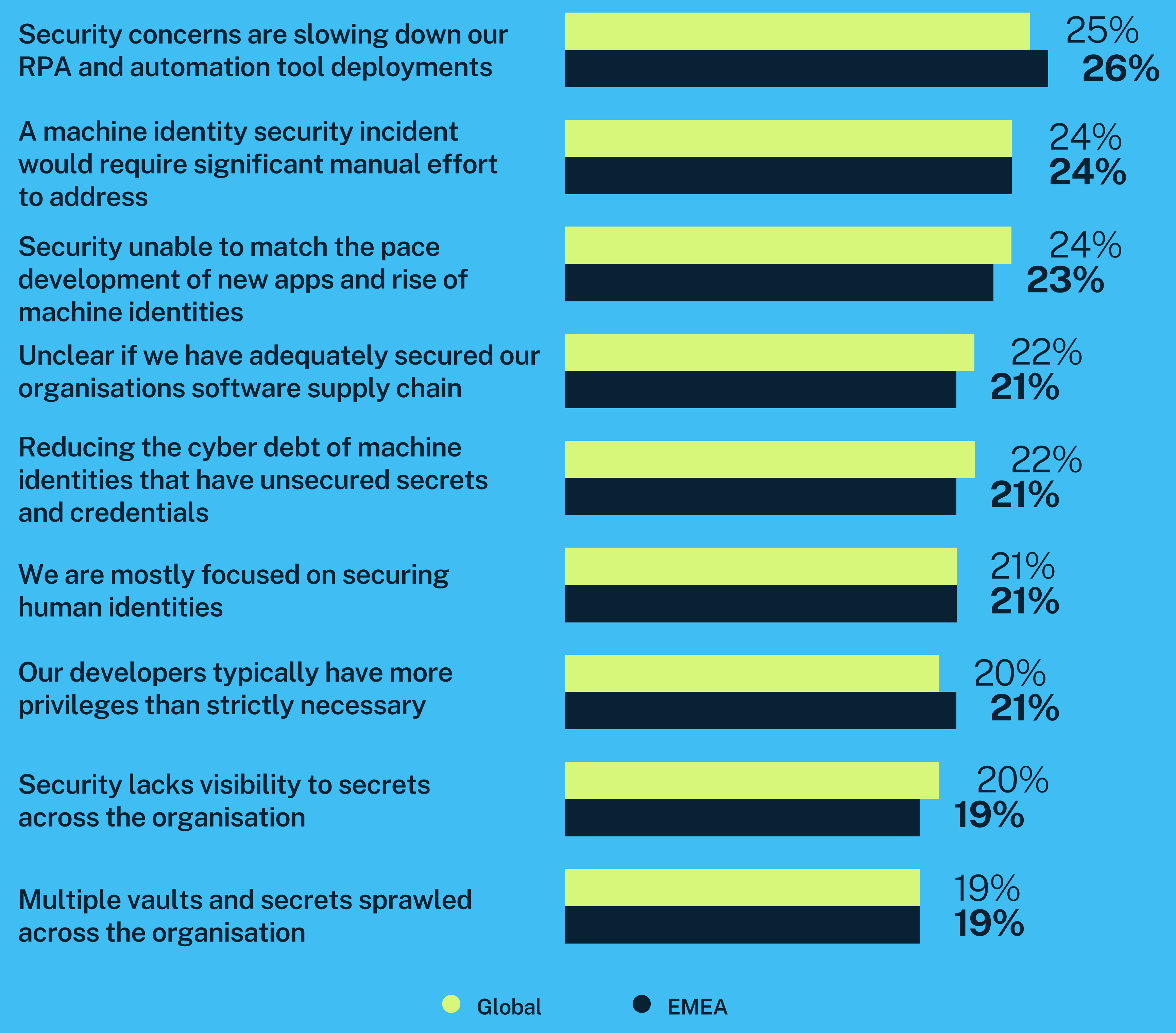
Once you define both human and machine identities as privileged users, it's important to assess every user machine, service account and workload to apply security controls where they were previously limited or missing due to an overly narrow definition.

It's been said a thousand times, but we'll say it again for good measure: Developers and engineering teams must involve corporate cybersecurity teams from day one of their projects. Both parties need to agree on how to strike a balance between productivity and security.

If you lack visibility of secrets within your environment, consider eliminating (or at last reducing) multiple vaults and secrets sprawl.

What we asked:
What are your organization's top concerns when securing machine identities (e.g., applications, cloud workloads, RPA)?

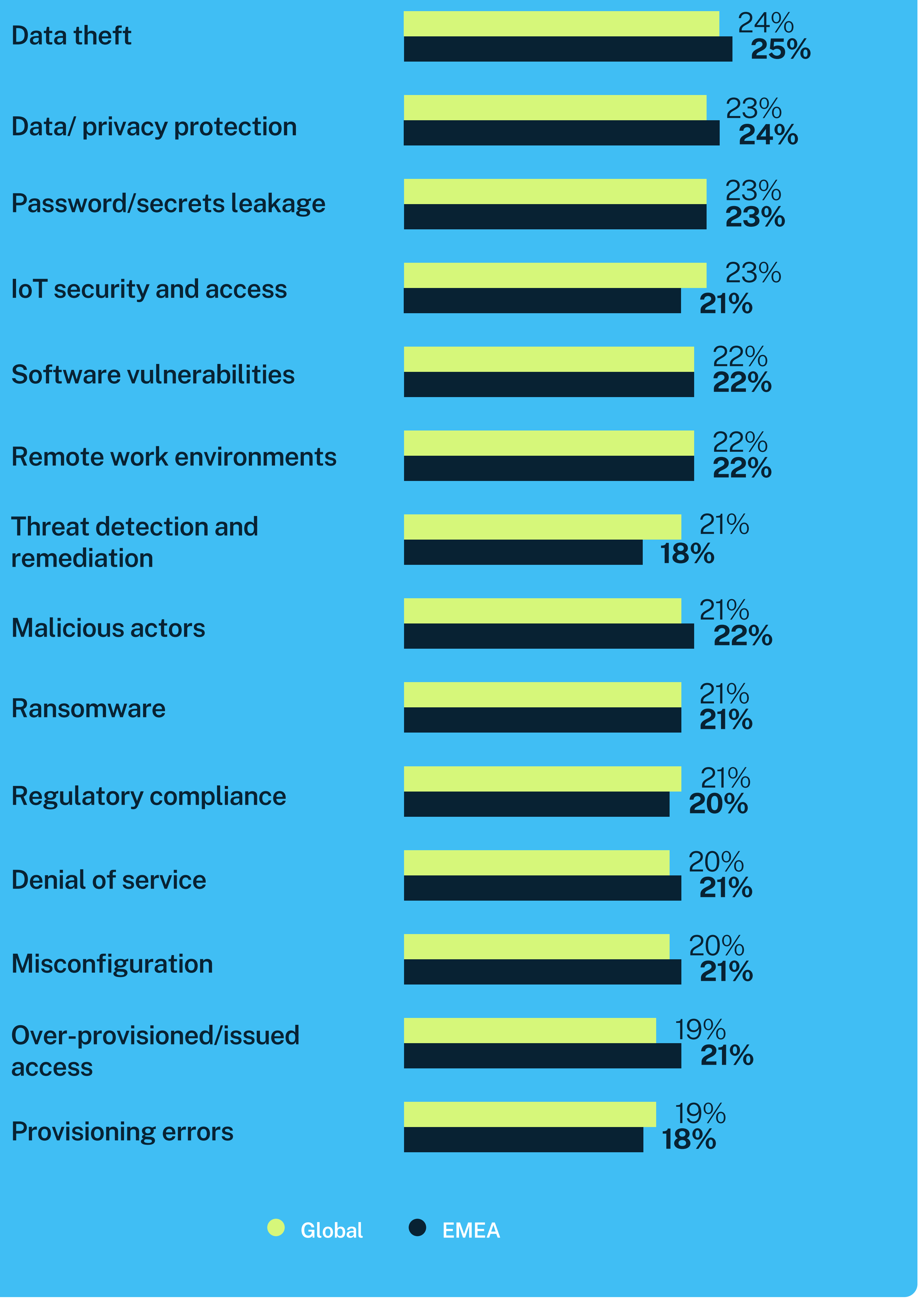
What we learned:
Security concerns are slowing down automation. Also, the threat of a machine identity-related security incidents could cause significant manual effort to remediate.



Chain Reaction: Third- and Fourth-party Risks

What we asked:
What are your top two cloud security concerns?
(Select two)

What we learned:
All EMEA organisations have cloud security concerns.



CHAIN REACTION: THIRD AND FOURTH-PARTY RISKS

Chain Reaction: Third and Fourth-party Risks

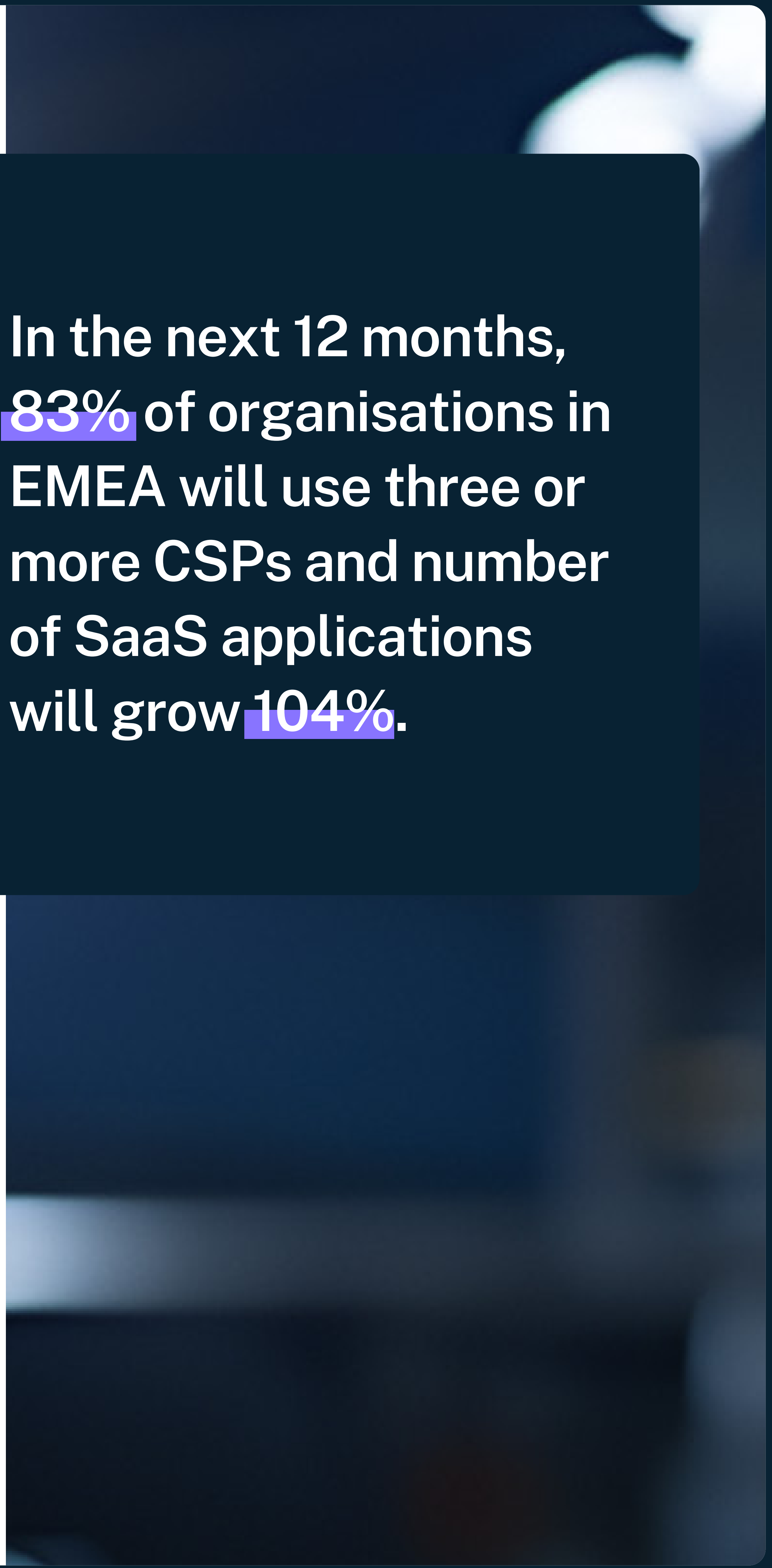
If you're already concerned about the state of cybersecurity at your third-party vendors, have you considered losing additional sleep over your partners' partners?

You've heard about third-party providers (product or service companies your organization engages with directly). Fourth parties contract with your third- parties and typically provide products or services to support your organization's digital business. Unfortunately, a compromise on one party leads to a compromise on all. Cry if you want to.

Third And Fourth Parties: Riskier Than Your Actual Extended Family

The growing constellation of business relationships can stretch an organization's reach, expertise, and budget. But every additional "nth" provider you bring into your digital ecosystem exponentially increases your risk. Our survey found that (84%) of organisations expect to leverage three or more cloud service providers (CSPs) in the next 12 months (on par with 85% last year). On the other hand, our 2024 respondents expect the number of Software as a Service (SaaS) providers to increase by 89% in the next 12 months, compared to 67% in the 2023 report.

Now, remember that your extended family indeed extends beyond CSPs and SaaS providers. Your third-party providers include your service providers, integrators, hardware and infrastructure suppliers, business partners, distributors, resellers, telecommunications and many others that are external to the organization that enable your digital business. Do you have visibility across all your third-party providers' security practices? How about your fourth-party providers?



In the next 12 months, 83% of organisations in EMEA will use three or more CSPs and number of SaaS applications will grow 104%.

A High-Stakes Trust Fall

The risks of a digital ecosystem are many — some severe and some minor. But overall, digital transformation continues to be the leading cause of an identity-related attack.

Our 2024 EMEA respondents indicate their multi-cloud environment currently consists of an average of 3 CSPs. Their key cloud security concerns are the following:

1. Data theft (EMEA 25%, Global 24%)
2. Data/privacy protection (EMEA 24%, Global 23%)
3. Password/secret leakage (EMEA 23%, Global 23%)

For EMEA, software vulnerabilities, malicious actors and remote work environments are tied at 4th sport for key cloud security concerns.

Our EMEA respondents also leverage an average of 88 SaaS providers. Every one of these providers is at risk of a cyberattack — and all of their customers stand in the blast radius. And yet vendor risk management remains a low priority in post-breach investments.

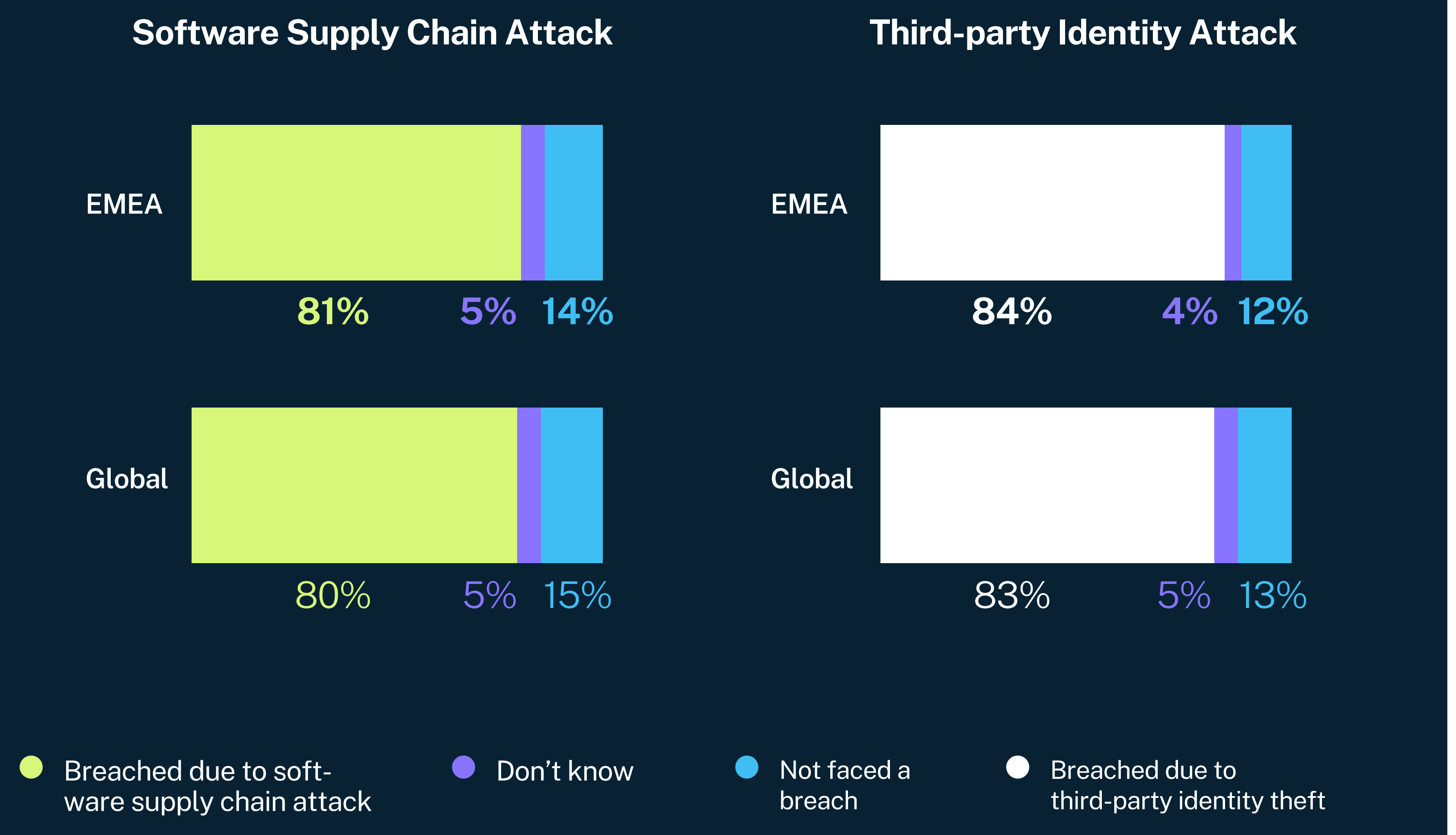
BOGO for Bad Guys

Some grim hypotheticals: Let's say one or more of your third-party providers were targeted and breached. They should notify you about the extent of the damage and its implications. But what happens to you if attackers infiltrate your fourth-party provider and impact your third party? Would you know the extent of the fallout on your organization? If you manage a multi-tenant environment, a bad actor needs to attack only one provider to gain access to multiple customer environments.

81% of organisations experienced an identity-related breach due to a software supply chain attack.

What we asked:
How often has your organisation faced a successful identity-related breach due to a software supply chain attack in the last 12 months?

What we learned:
Majority of organisations have suffered from a supply chain attack and third-party identity theft.

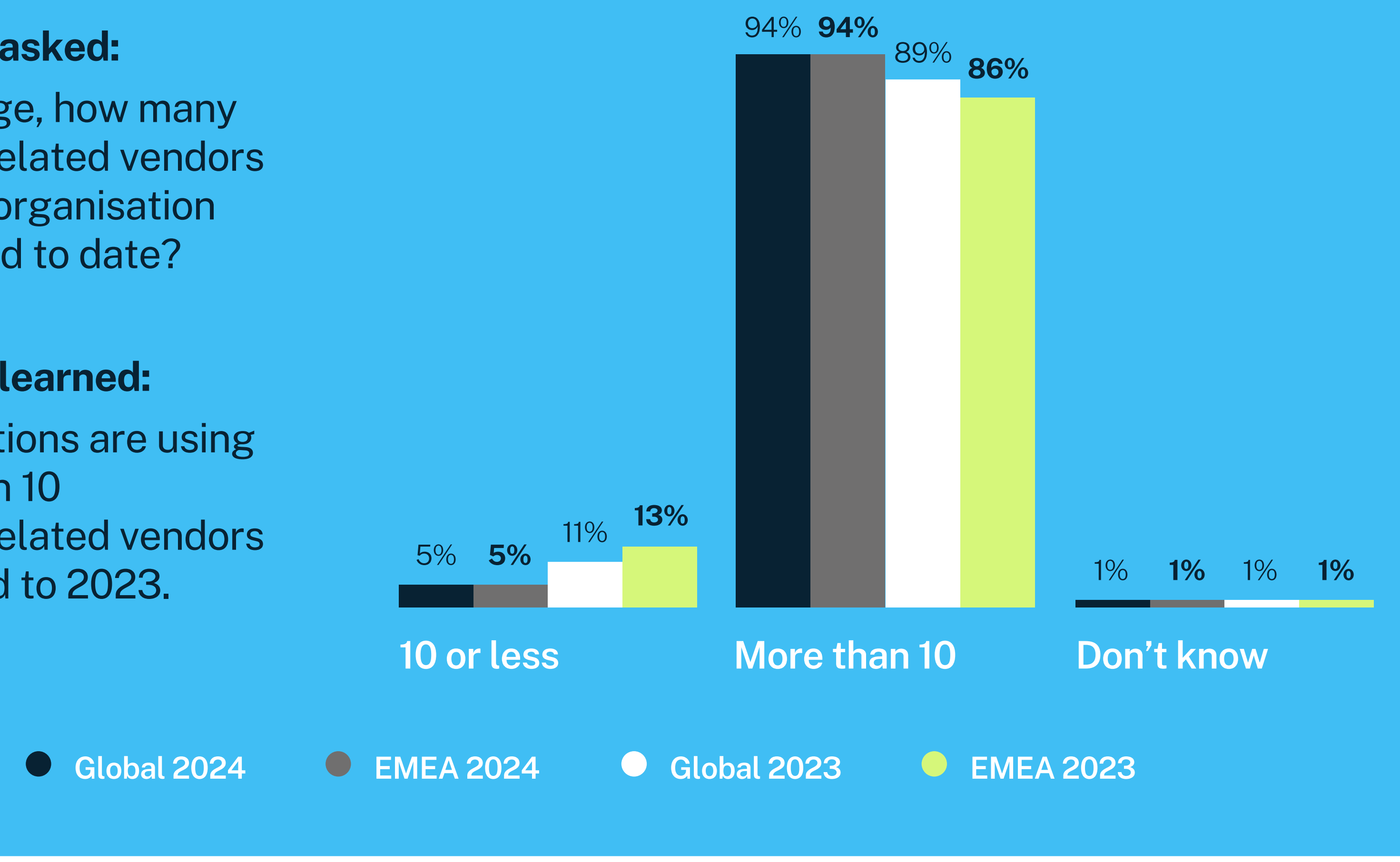


What we asked:

On average, how many identity-related vendors has your organisation onboarded to date?

What we learned:

Organisations are using more than 10 identity-related vendors compared to 2023.



Open Season on Sitting Ducks

Not so long ago, the industry experienced its first double software supply chain attack on 3CX that impacted over 600,000 customers. Fast forward to today, and we see hackers optimizing their efforts and maximizing potential financial gains with sophisticated AI-powered cyberattacks. Our 2024 findings indicate that 81% of EMEA organisations experienced an identity-related breach due to a supply chain attack, and 58% of these breached organisations reported that external bad actors were responsible.

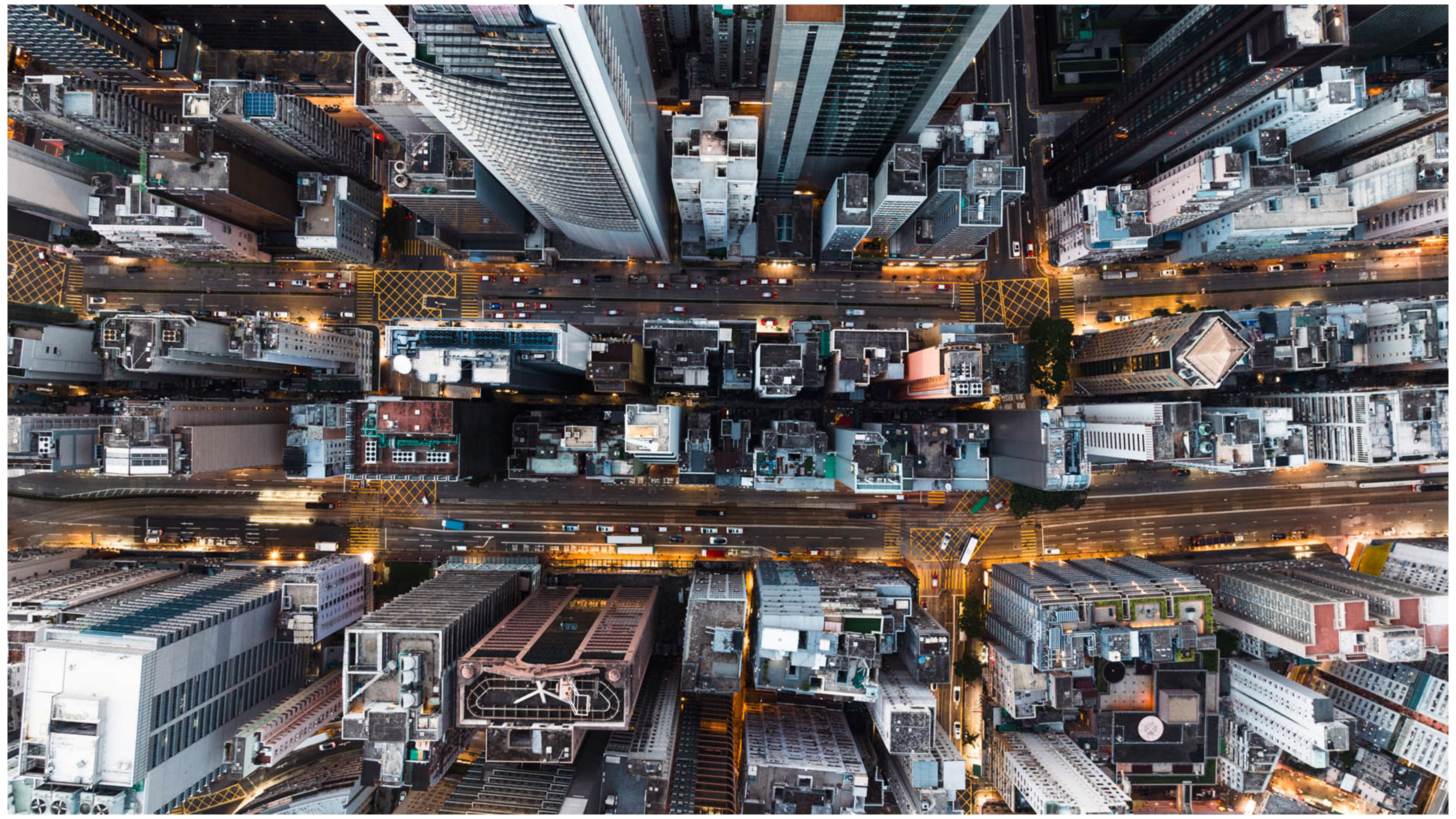
We are seeing a rising number of individuals, groups and nation-states actively targeting technology-critical infrastructure providers. In April 2024, hackers accessed hard-coded secrets in the GitLab repositories of Sisense, a business intelligence company. The subsequent breach of sensitive customer data prompted the leading US-based Cybersecurity and Infrastructure Security Agency (CISA) to issue alerts for customers to reset any shared credentials and secrets immediately.

Some bad actors want to influence election outcomes, some are in it purely for financial gain, and others, well, they just want your emails. Earlier this year, nation-state-led bad actors spied on executives' emails at both Microsoft and HPE. Experts are still evaluating the extent of the impact. As more and more incendiaries pile into the tinderbox of a global election year, seismic breaches like SolarWinds could be just the starter kit.

Unified Visibility is a Big Blind Spot

A digital ecosystem is often made up of disparate tools that address unique requirements across on-premises, hybrid and multi-cloud environments. This applies to your cybersecurity technology stack too, including your identity portfolio. In fact, 27% of EMEA respondents chose "lack of visibility across multiple identity-related point tools, products and services" as the top two truest statements for their organisations. Lack of visibility across disparate (on-premises and cloud) environments was a close third.

This lack of visibility extends deep into the digital ecosystem where risk from third- and fourth-party providers are hard to evaluate regularly. It bears repeating that vendor risk evaluation is usually the last priority in post-breach investments. This needs to change.



CyberArk Insights

Digital business is a tangled web of ever-expanding partners and providers, each eager to adopt new technologies but often unable to divest from legacy environments. For identity security professionals, too many tools for too many use cases are the bane of their existence. Research tells us that 94% of organisations leverage more than 10 vendors for their identity-related cybersecurity initiatives — up from 89% last year. If this is true for you, allow us to gently nag:

1. **Audit and evaluate** all legacy and new technologies across your environment.
2. **Assess the risks** of these disparate tools address vs. the time and effort required to maintain them.
3. **Create a plan** to consolidate your technology stack based on the right balance for your organisation. Do this slowly but surely.

Granted, this may be a long-term project. But we believe the light at the end of this particular tunnel is well worth the effort.

What This Means for You

Again, consolidating your vendor stack and deprecating those legacy tools is not an easy task. But there are few ways to make the process less painful.

Start with a simple question: What does "trusted third party" really mean? When qualifying a vendor, get a consensus with your stakeholders on why and how to stack and rank their experience, expertise, track record for innovation, and customer service capabilities. Look at analyst and earnings reports, market assessments and consider word-of-mouth recommendations. And while the shiniest and most talked-about product or service might be tempting, sometimes the less glamorous tools are the best fit for your unique environment.

Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Shiny Object Syndrome: we've all had it. After all, new technologies are attractive, exciting and capture our imaginations — and often a chunk of our organizational time and money (lookin' at you, GenAI). But as we focus on adopting and implementing transformational technologies and addressing the Threats of the Future, cybersecurity teams cannot — even for a moment — afford to take their eyes off the prize of the existing and age-old threat landscape. This is a recipe for disaster.

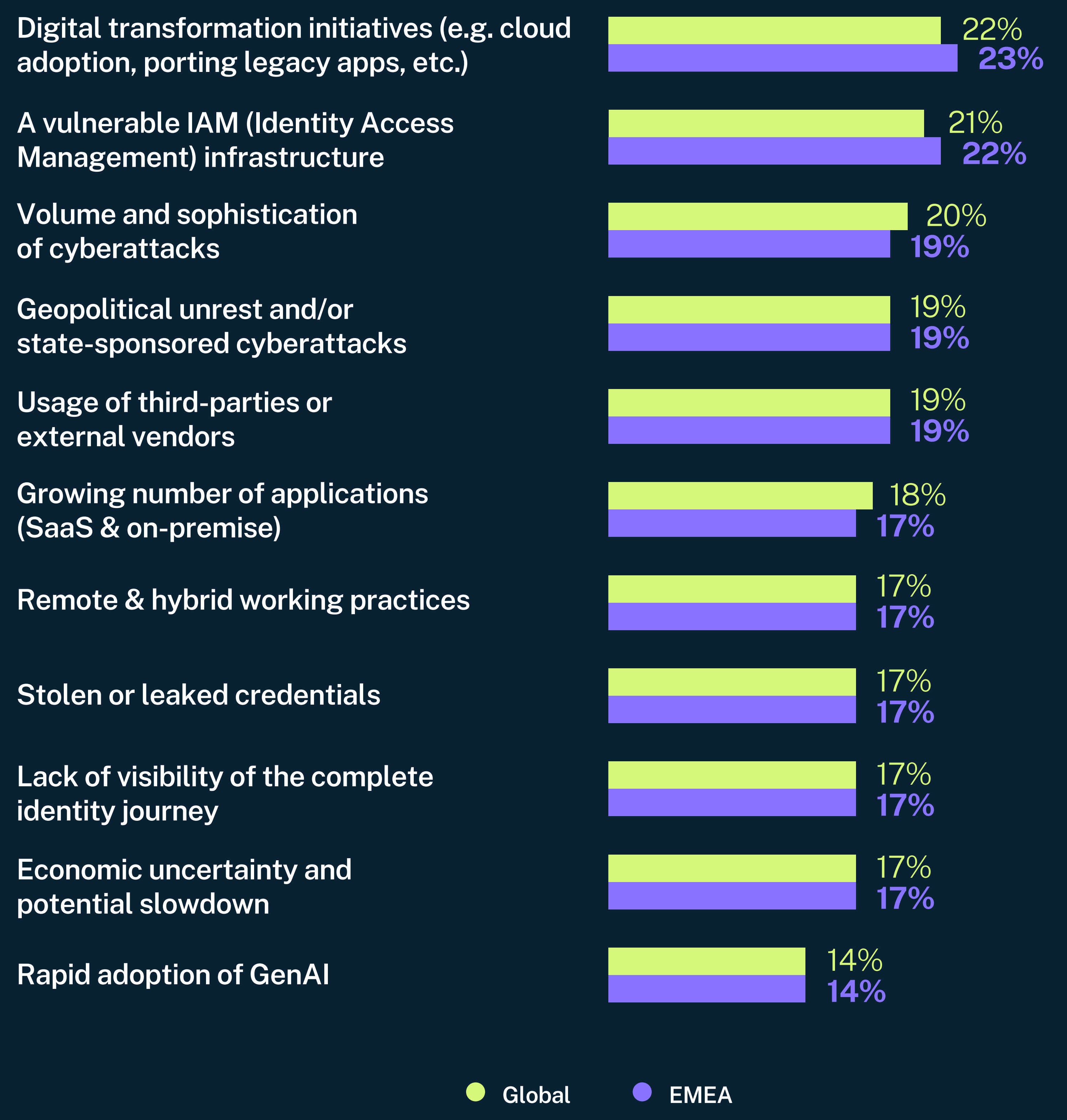
The More Things Change, the More They Stay Insane

Digital transformation continues to be the top cause of identity-related attacks. Similar to global findings, breaches due to phishing and vishing attacks have impacted 9 of 10 EMEA organisations. Nearly the same number of EMEA organisations were targeted by ransomware in 2024 (90%) as compared to 2023 (88% vs.) with a higher number of organisations reporting damage (irretrievable loss of data).

> In the last 12 months, 90% were targeted by ransomware and 74% paid ransom but did not recover the data.

What we asked:
Which two factors are most likely to cause an identity-related attack in your organisation?

What we learned:
Digital transformation fueled by cloud adoption is the #1 reason to likely cause an identity-related attack.



Any Identity with Sensitive Access is a Gateway

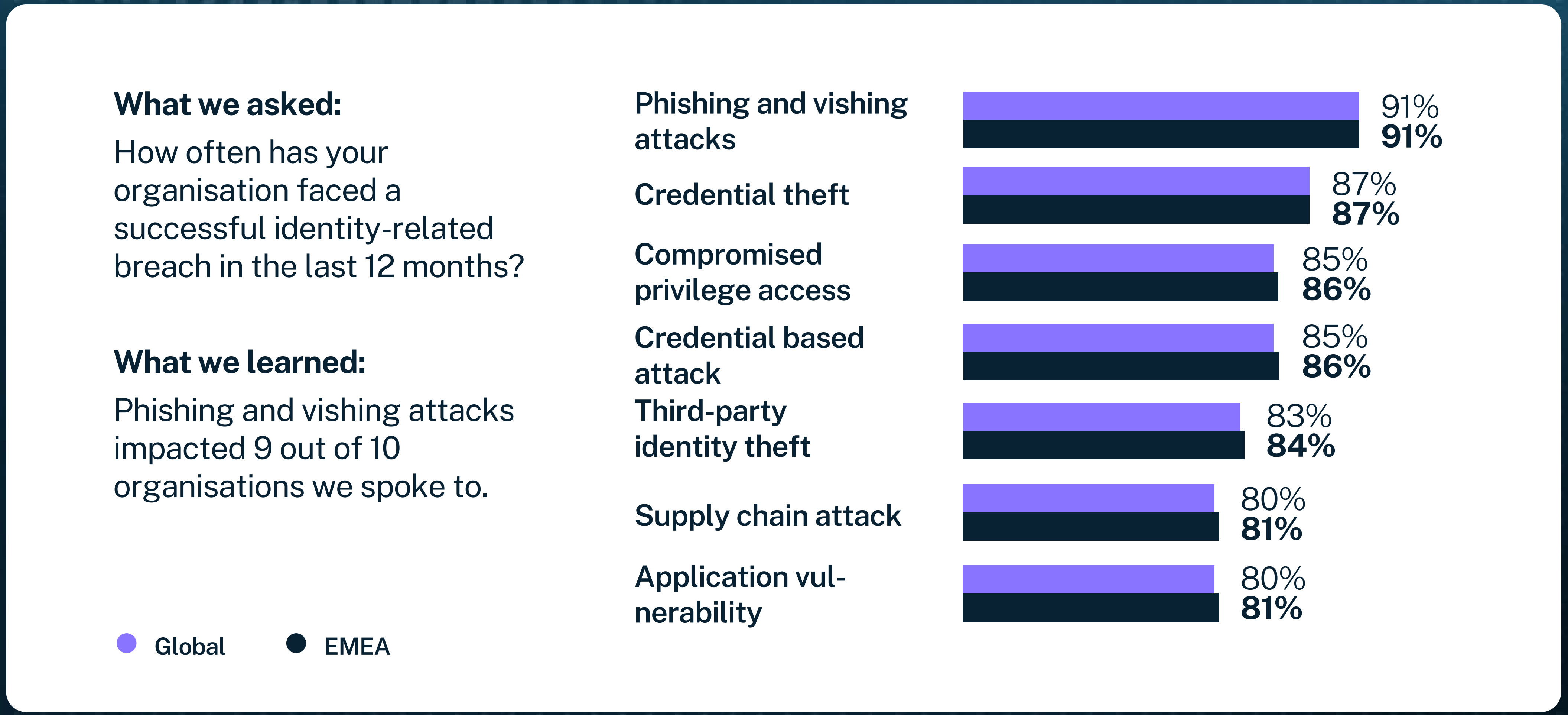
It's important to note that unauthorized or compromised access of any business user (employee or third-party contractors) is equally harmful to that of a compromised privileged user. We found that 70% of EMEA organisations report up to 50% of human identities have access to sensitive data, compared to 65% in 2023.

In our 2024 survey, 36% of EMEA respondents believe that more than half of their human identities have access to sensitive data. That's up 10% from 2023. In other words, every identity that has access to sensitive data is a privileged identity and must be secured appropriately.

How Do I Hack Thee? Let Me Count the Ways

Our respondents indicated that they were the victim of a data breach due to one of the following types of attack:

1. **Phishing and vishing** happen when a user is contacted by email, telephone or text message by someone posing as a close personal contact or on behalf of a legitimate institution. Ransomware is a common example of phishing and vishing attacks.
2. **Credential theft** is a type of cybercrime that involves stealing a user's credentials that prove their identity. Once in, the bad actor(s) gains the same account privileges as the user. Stealing credentials is the first stage in a credential-based attack.
3. **Compromised privilege access** is when a bad actor gains access to a user's login credentials to a firewall, server or other administrative account with the highest sensitive access.
4. **Credential-based attacks** occur when criminals steal credentials to gain access, bypass your organization's security measures, and steal critical data.
5. **Third-party identity theft** is when bad actor(s) gain access to your organization's contractors, consultants, or other people needing access to your IT resources. These third-party identities (users) are not permanent in the corporate user base.



What we asked:

How often has your organisation faced a successful identity-related breach in the last 12 months?

What we learned:

Phishing and vishing attacks impacted 9 out of 10 organisations we spoke to.

6. **Supply chain attack** uses third-party tools or services (collectively referred to as a "supply chain") to infiltrate a target's system or network. These attacks via your digital ecosystem are sometimes called "value-chain attacks" or "third-party attacks."
7. **Application vulnerability** is a system flaw or weakness in an application's code that can be exploited by a malicious actor, potentially leading to a security breach. Organisations must patch critically vulnerable software and systems across their digital footprint. Attackers will actively target those who have not yet applied the patch.

Seriously, Yes, Ransomware Is Still a Thing

We mentioned that 9 out of 10 respondents were breached due to a phishing or vishing attack. Phishing or vishing attacks often lead to some form of ransomware.

While many of us imagine a world free of ransomware, the truth is: old is gold, and humans are the weakest link. Ransomware is here to stay and, in fact, will increase in volume and sophistication with AI-enabled deepfakes. And no matter how much cybersecurity awareness training is in place, bad actors will get that one innocent user to click a link or share that OTP which can compromise their identity and the organization's data.

No Honor Among Thieves

Ninety-percent of organisations suffered a ransomware attack that wreaked havoc in a variety of ways. But perhaps the most disturbing trend is that 75% of these victims paid the ransom but no data was recovered — up 7% from 2023. We also found that organisations in the financial, healthcare and life sciences sectors have a significantly higher rate of this twofold injury: paying ransom without recovering data.

Any Breach Is a Bad Breach

Nearly all (99%) of organisations who were victims of an identity-related breach faced a direct impact to their business in the last 12 months. So how, you might ask, did that 1% sliver escape any negative fallout?

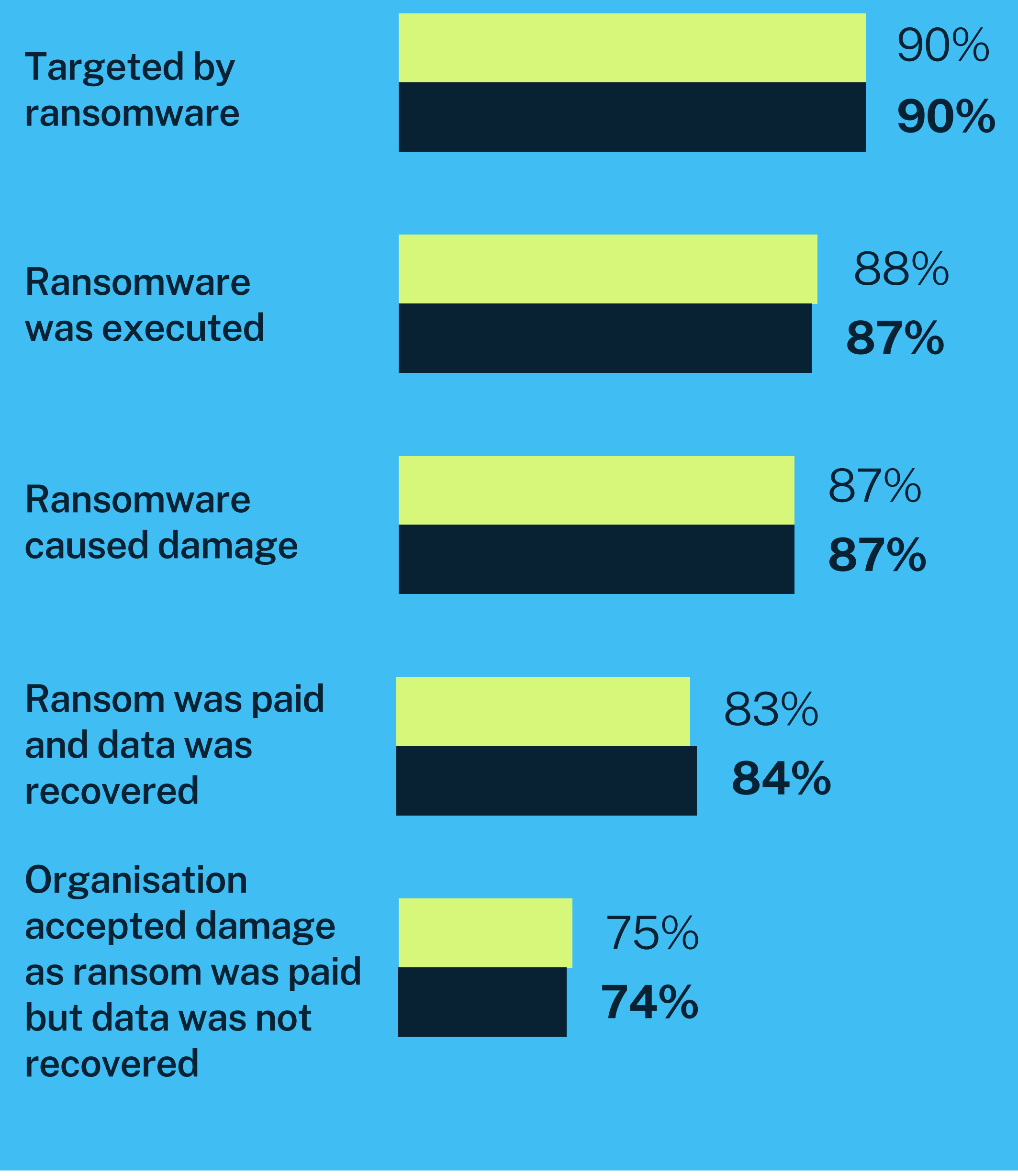
In looking at additional insights, we discovered that 3% of EMEA organisations from the technology sector reported no negative breach-related repercussions. Consider for a moment all the high-tech providers you leverage — how many of them made headlines last year with a high-profile breach? Have you stopped doing business with them? Could it be that your digital business is so intertwined with their technology that the time and effort of moving to a new provider is worth the risk of staying with them?

What we asked:

How often has your organisation faced a successful ransomware attack in the last 12 months?

What we learned:

Ransomware is a real threat that is actively causing harm and loss of data as well as finances more than once for most organisations in the last 12 months.



We know. It's not an easy choice.

This takes us back to the lessons learned in the risky third- and fourth-party sections of this report. Organisations are concerned with these vendor risks, but the only thing they can do (which most report they don't) is increase investments and the frequency of vendor risk assessment.

CyberArk Insights

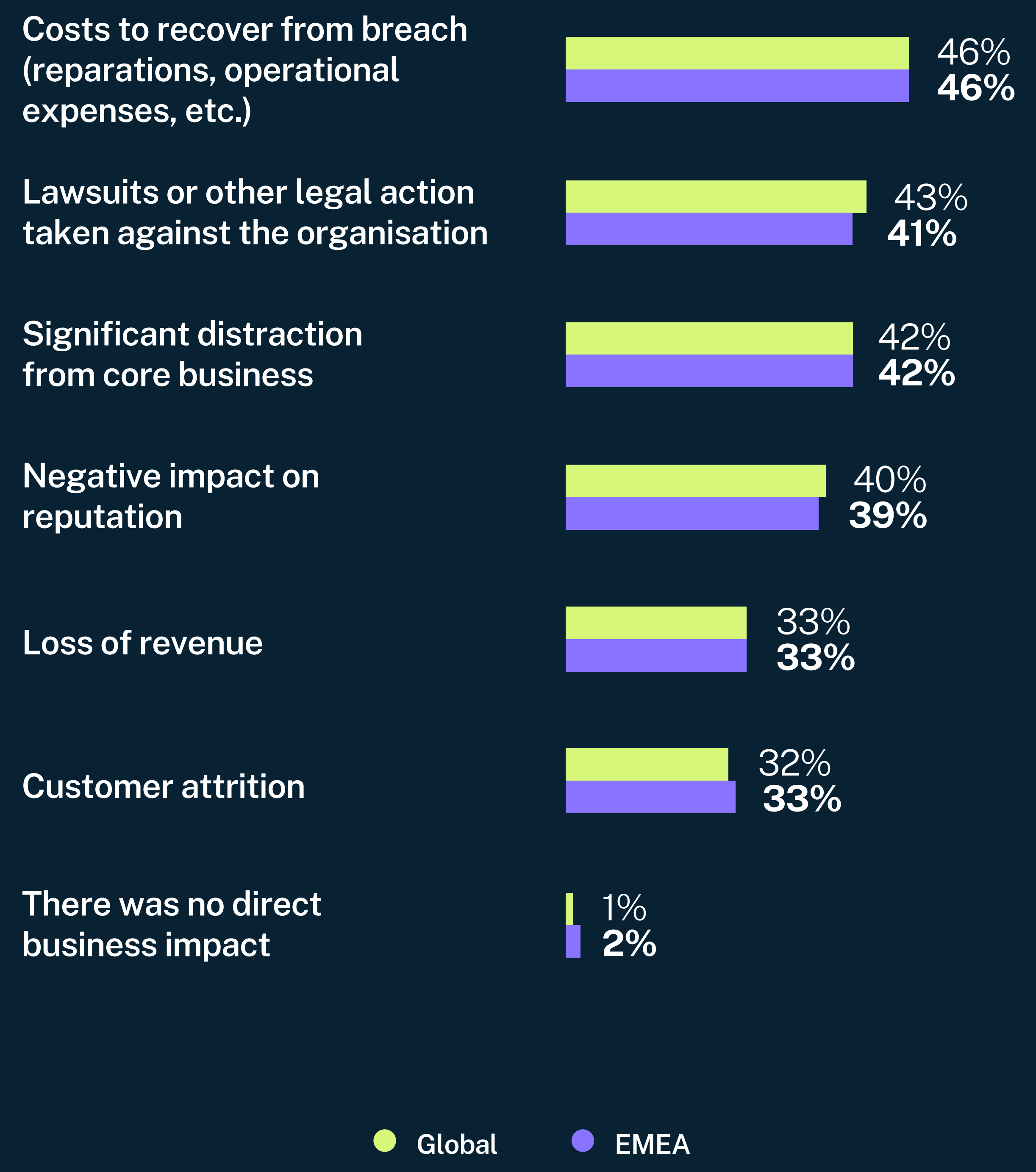
In its 2024 Global Risks Report[1], the World Economic Forum ranks misinformation and disinformation as #1 in its top ten risks for the next two years — and cybersecurity as #4. Given the political and economic landscape, these two technology threats (placing in the top 5 of 10) will create a new set of winners and losers in the digital landscape.

What we asked:

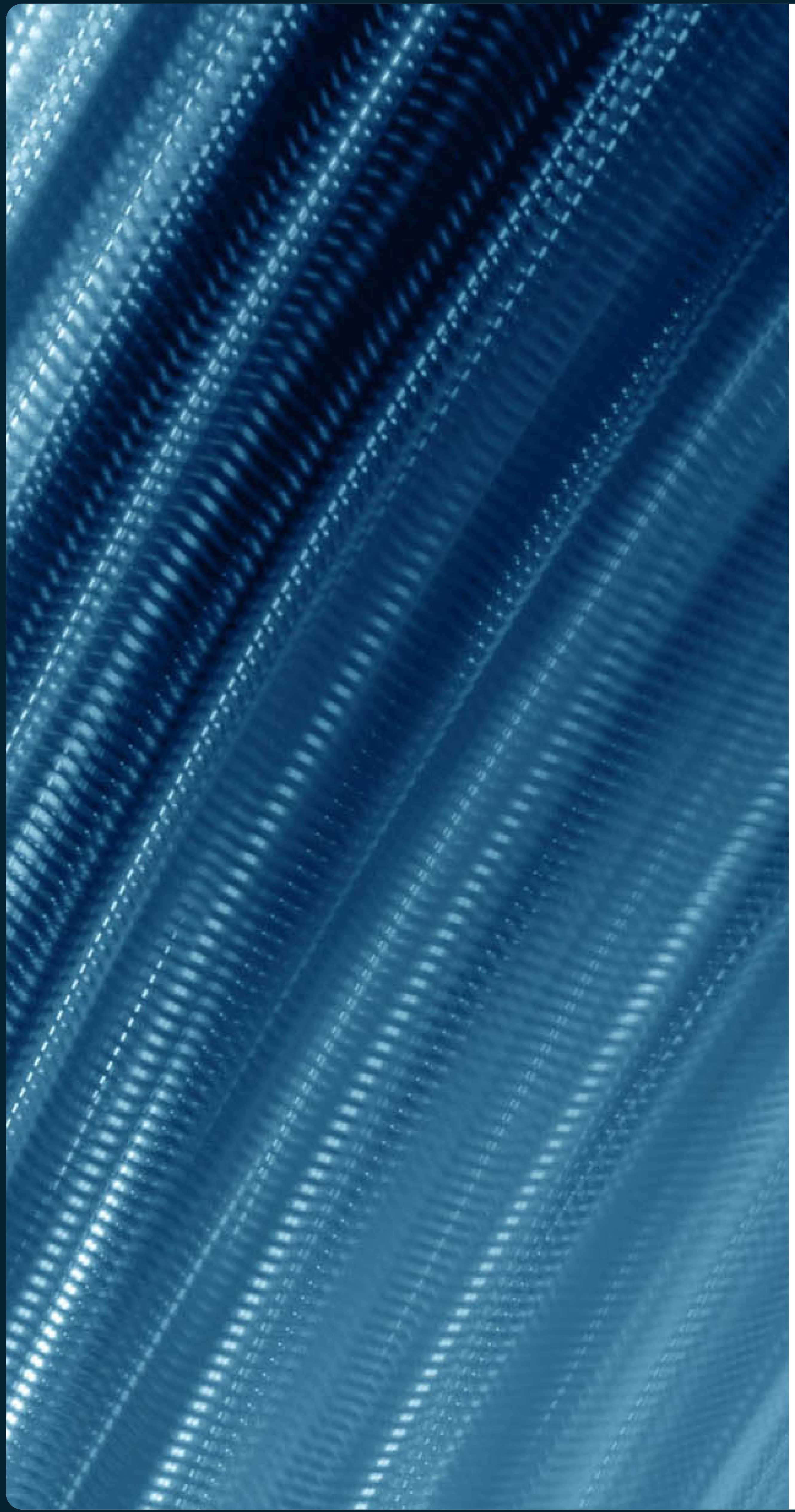
Did your organisation suffer any direct impact to business results due to the breaches in the last 12 months?

What we learned:

Nearly all organisations who were breached faced negative impact on their business



[1] WEF_The_Global_Risks_Report_2024.pdf (weforum.org)



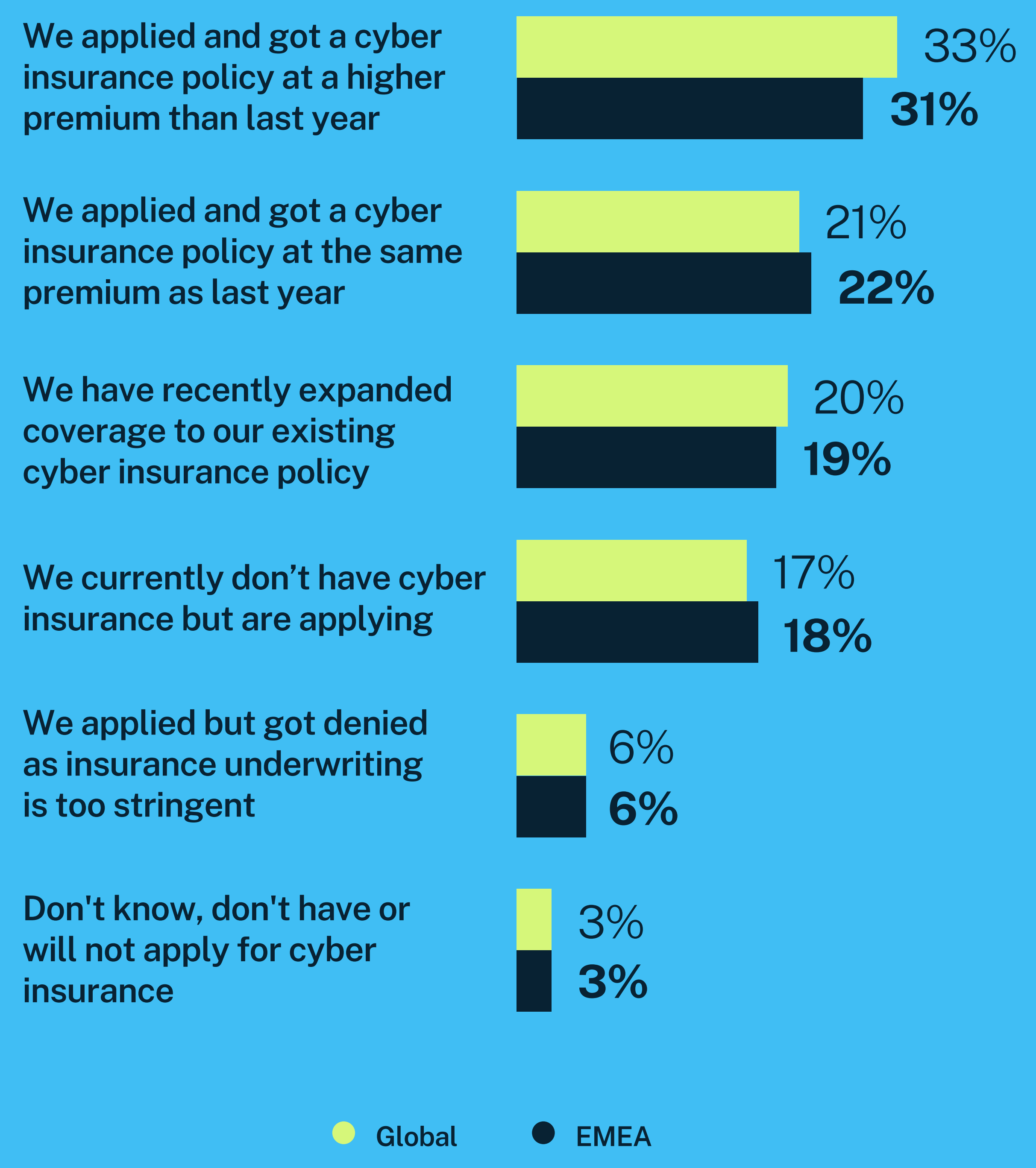
What This Means for You

While "peril" and "uncertainty" are two constants in cybersecurity, there are ways to ensure you not only avoid giant holes in the road but actually win the race.

1. **Zero Trust.** Your organization must start its Zero Trust journey — yesterday. If you're already implementing a Zero Trust strategy, congrats. Advance quickly to step 2.
2. **Secure every identity** across your entire environment. Leave no identity — human and machine — unmanaged or unsecured. This is the only way to ensure that identity remains a formidable defense.
3. **Training works.** Bad actors tend to prey on humans. After all, we're susceptible to a false sense of trust and can rather easily be coaxed into sharing sensitive information. Therefore, a cadenced and mandatory cybersecurity awareness training is a must to slowly build cyber hygiene practices amongst your employees.
4. **Plan for the worst.** No matter how much you invest in bolstering defenses, bad actors enjoy the challenge of finding that one overlooked vulnerability. Develop a contingency plan and practice tabletop exercises for key doomsday scenarios like ransomware, phishing, insider threats, software supply chain breaches, data breaches and privacy compliance attacks.
5. **Cyber insurance.** Yes, it's hard to get insured in cyberspace. Underwriters are increasingly tightening guidelines and requirements. But the fact is, following those guidelines means you've developed a path to a robust security posture and can attain some hard-won peace of mind.

What we asked:
Which of the following statements related to cyber insurance is true for your organisation?

What we learned:
One-fifth of organisations have expanded cyber insurance coverage for a higher premium



The Path Forward

The Path Forward

While there is no shortage of doom and gloom, significant silver linings do exist. Organisations are evolving their cybersecurity strategies with new capabilities and task automation. Identity security organisations are adopting identity threat detection and response (ITDR) and passwordless authentication capabilities. Respondents have told us that implementing just-in-time (JIT) access, IGA automation and advanced user behavioral analytics have increased their ability to mitigate identity-related risks and reduce cyber debt.

The State of Automation

All — 100% — EMEA organisations indicated that they will prioritize new tools or technologies in the next 12 months. Topping that list: ITDR. This emerging security discipline will help organisations like yours to address an all-too-familiar challenge: managing and securing the massive number of human and machine identities across the enterprise. ITDR enables Zero Trust initiatives, keeps identity as the central focus and protects what's most precious to your organization: data.

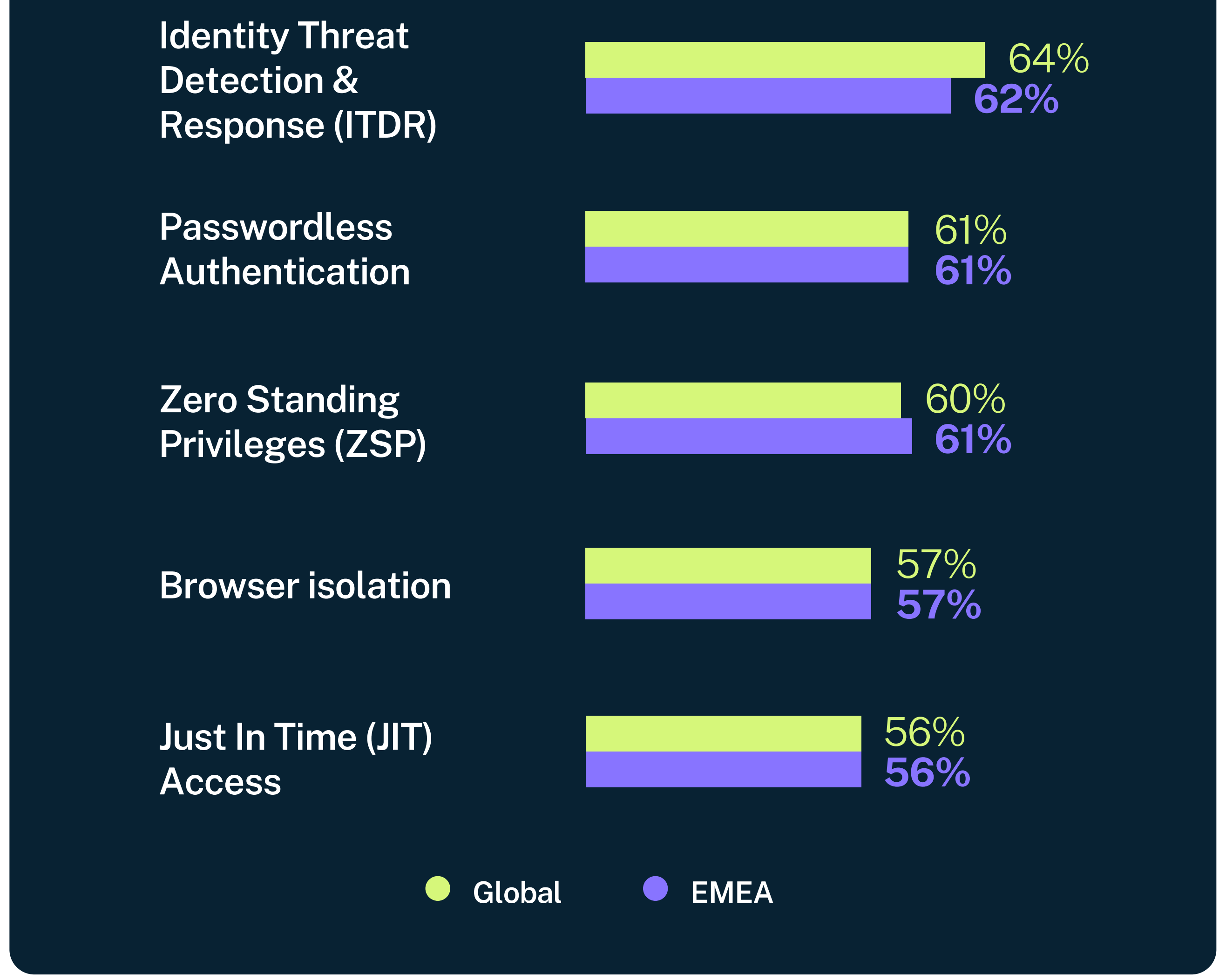
Our research finds that organisations are automating or partially automating threat-hunting tasks, phishing analysis, password resets, alert triage and threat intelligence management. AI-powered tools are also powering better breach detection and prevention and advanced analytics.

However, automation and AI are not one and the same.

Automation executes predefined tasks and reduces manual intervention. AI, on the other hand, incorporates machine learning from large datasets to ultimately make decisions without explicit programming. As your organization steers from automation towards rapid AI-powered decision-making, the key is to ensure the transparency and explainability of that fast and furious execution. It will be up to human counterparts to step in and figure out the why and how behind AI's decisions.

What we asked:
How has, or will, your organisation prioritize each of the following tools, technologies or capabilities in the next 12 months?

What we learned:
ITDR and passwordless authentication will see greater adoption in the next 12 months.



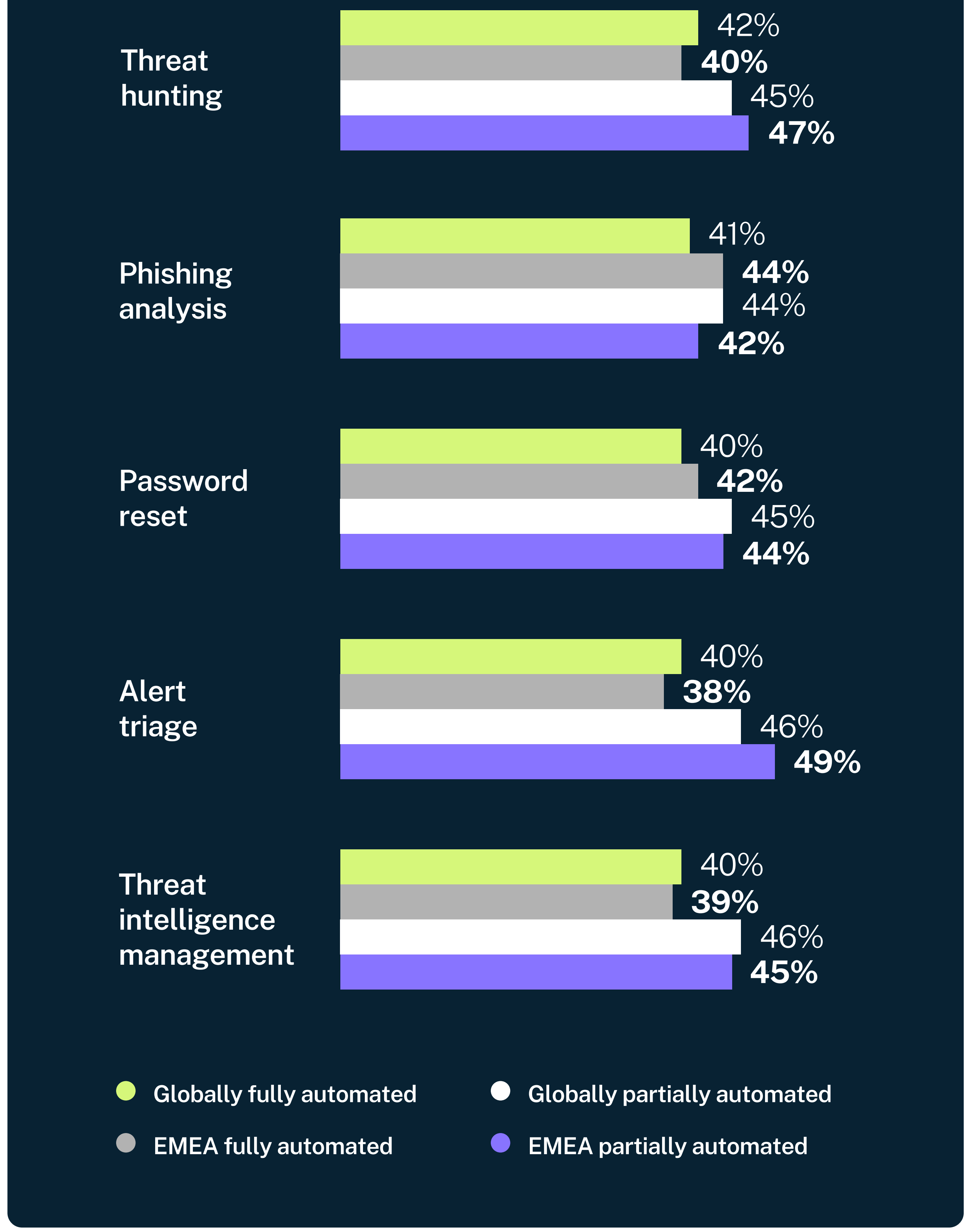
For the next 12 months, 62% of EMEA organisations have or will prioritize ITDR capabilities.

What we asked:

To what extent are the following cybersecurity processes/use cases automated in your organisation?

What we learned:

Most cybersecurity processes are only partially automated.



Start Here

We get it: You're adrift in a sea of issues that can or need to be addressed. Where do you begin?

Our respondents weighed in on the best practices that helped them have the most impact against identity-related threats.

Headlining that list (tied for the #1 spot): adopt JIT access to improve cloud security and automated identity governance and administration (IGA). Second, implement advanced AI/ML-based behavioral analysis and anomaly detection.

Put Your Money Here

Apart from the need for endpoint security, federated identity, cloud infrastructure entitlements manager (CIEM) and automating third-party identity management we'd like to draw your attention to the smartest bets for your post-breach investments.

Third- and fourth-party risks are cause for significant concern. But all too often, investing in vendor risk management remains at the bottom of the post-breach priority list. If you've suffered a breach related to a third- or fourth-party provider, don't be complacent. Incorporate a regular cadence for vendor risk assessment immediately.

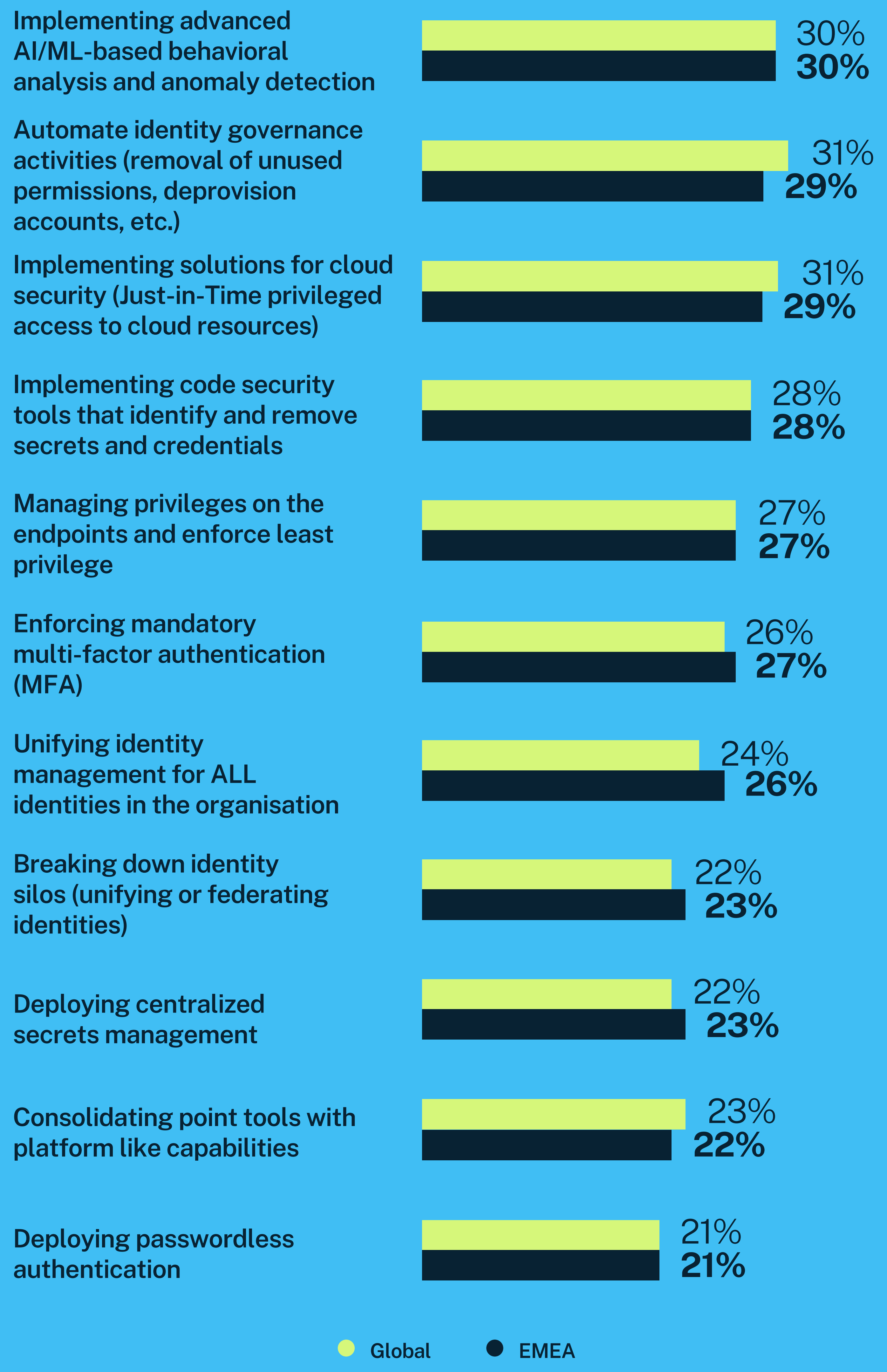
Similarly, while we know machine identities are among the riskiest, investments in secrets management and machine identities lag behind as well. These gaps must be addressed quickly to ensure a robust security posture.

What we asked:

Please select up to three actions your organisation has taken that have had the biggest positive impact on the ability to mitigate identity-related threats and reduce cybersecurity debt.

What we learned:

Implementing code security tools is rising to the top apart from securing human identities.

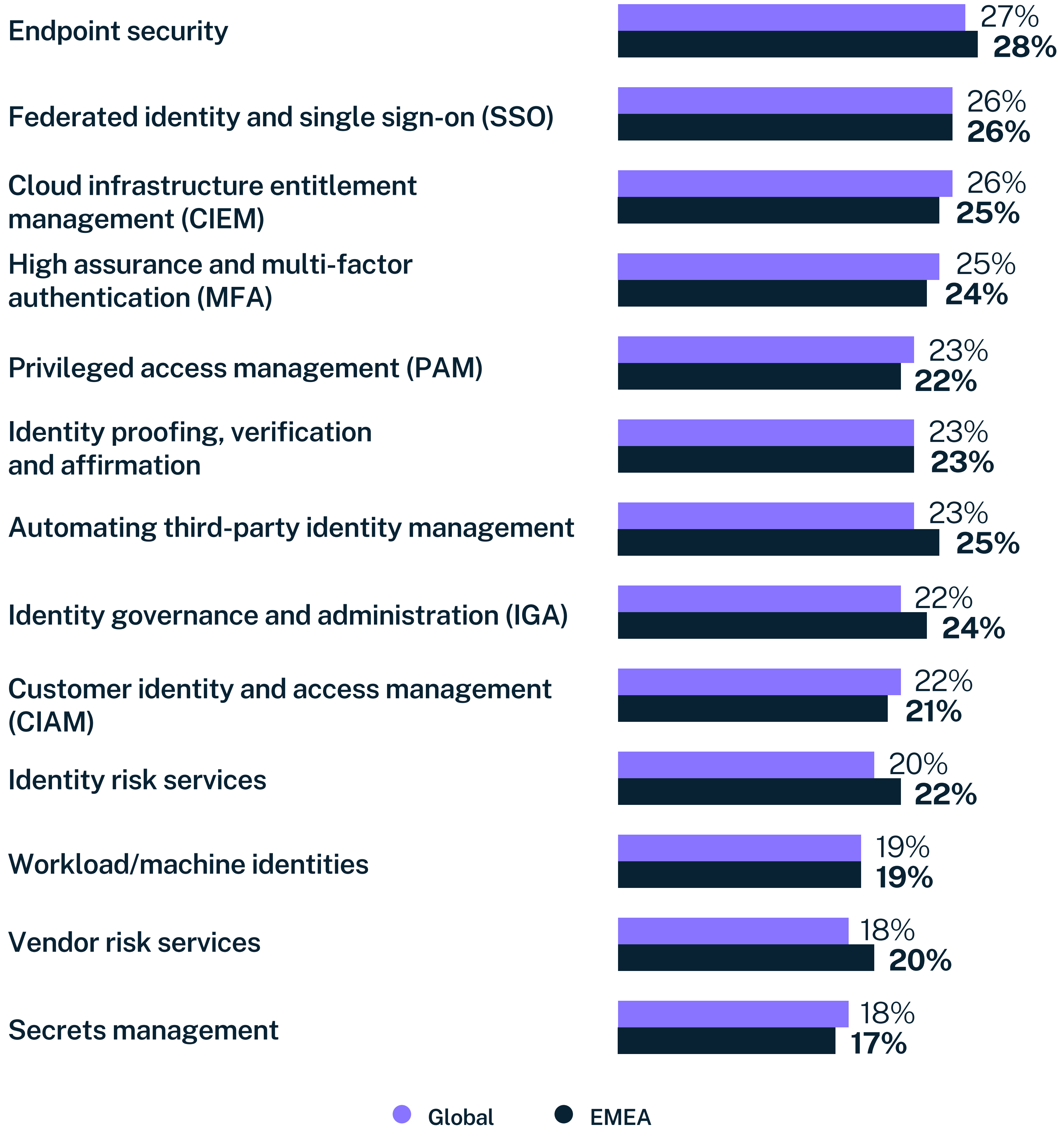


What we asked:

After the breach, which two identity-related technology investments did you increase or make net new investments in?

What we learned:

Similar to global findings, in EMEA machine identities, secrets management and vendor risk services scored lowest post-breach investments.



CyberArk Insights

When challenges become overwhelming, particularly given the advent of GenAI, there is strength in numbers. Cybersecurity experts can learn from their peers, assess their own unique environments, identify the most critical areas of risk and find a smooth path forward.

What This Means for You

There is constant pressure to buy new technologies to address the latest issues. We've seen the race to adopt GenAI for various use cases, including augmenting cybersecurity initiatives. It's important to pause and reflect on the known and unknown risks of any new technology and whether its adoption outweighs the risks it brings.

In a world where SEC can hold individual CISOs responsible for fraud and internal control failures, it's non-negotiable that you ensure transparency, accountability and good governance across your cybersecurity initiatives. Assess, evaluate and iterate any key performance indicators (KPIs) your organization has outlined.

You are undoubtedly in a fast-paced world with a long list of daily Sisyphean challenges. Every defense you put up becomes a game that bad actors love to win. And it only takes one misstep by anyone on your team to bring down the stack of cards.

The one advantage we have is each other.

"Talent wins games, but teamwork and intelligence win championships." That's not our quote (it's Michael Jordan's) but the advice is timeless. The team at your back isn't limited to your immediate colleagues. It spans your entire organization and even to your third- and fourth-party providers. This year's cybersecurity threats may be the storm of the century, but together, we can hold the fortress down.

EMEA Country Spotlight

EMEA Country Spotlight

The EMEA cybersecurity landscape is increasingly complex, influenced by stringent government policies and geopolitical dynamics. Cyber-attacks, including ransomware and data breaches, have profound impacts, disrupting businesses and economies, and highlighting the need for robust security measures in this diverse region.

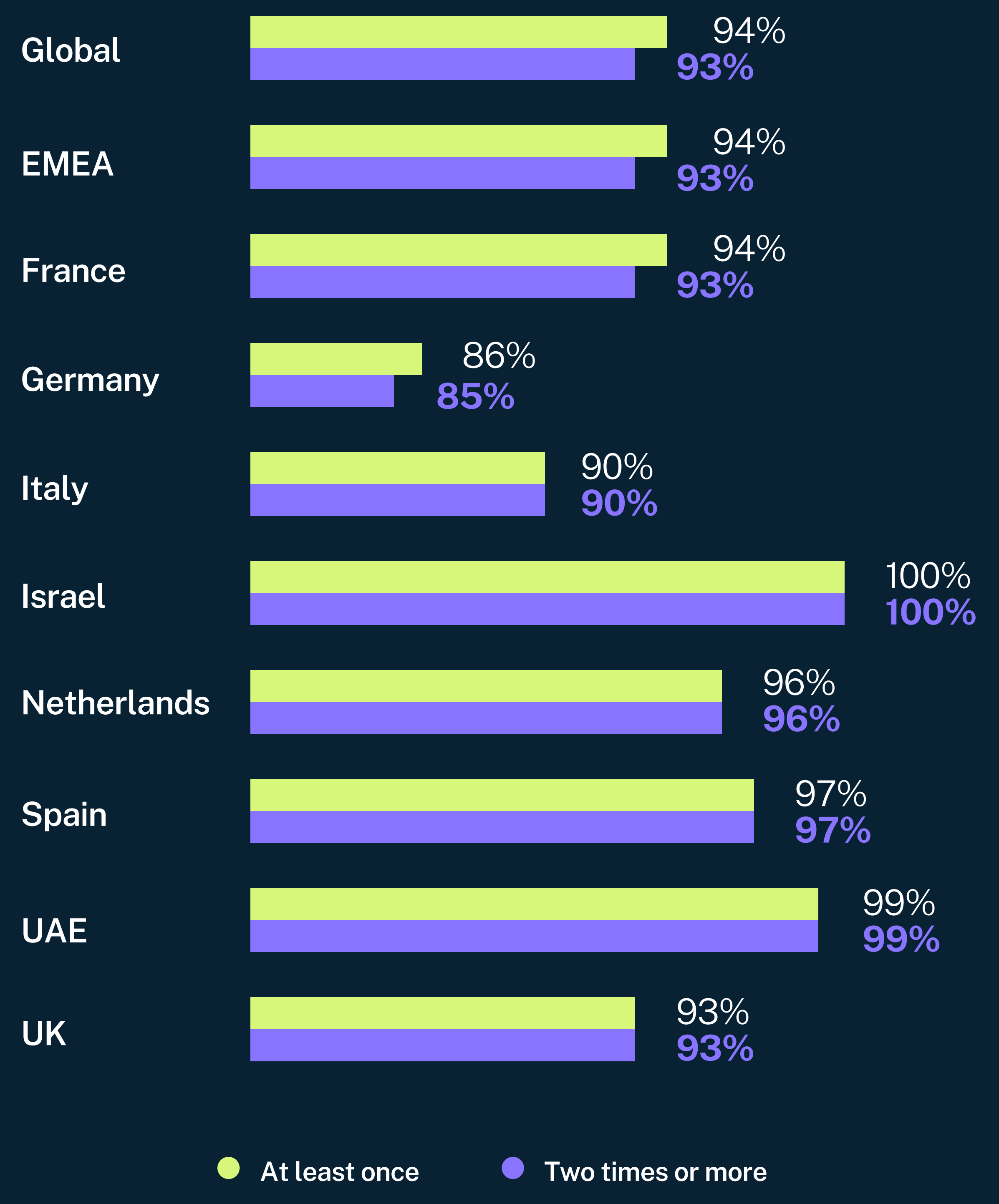
As a region, EMEA follows the global pattern of breaches we've seen in the last 12 months, with significant variation at the country level. Germany and Israel stand out as globally unique: 86% of German respondents reported an identity-related breach at least once in the last year, compared to 100% of Israeli respondents indicating the same. These two countries represent the lowest and highest rates of breaches, not just across the EMEA but also among the 18 countries we surveyed globally. In our country-level insights, we'll explore these contrasting findings.

In the next section, we'll explore specific country-level insights and compare them to pan-EMEA findings. At a higher level, we'll delve into the economic, geopolitical and technological landscape affecting every country and its impact on organisations facing identity-related threats or breaches.

Let's begin.

What we asked:
How often has your organization faced a successful identity-related breach in the last 12 months?

What we learned:
Almost all EMEA organisations faced identity-related breaches with alarming frequency.



EMEA COUNTRY SPOTLIGHT: FRANCE

France

In this report, we surveyed 150 respondents in France. 80% of French respondents indicated that their organization had over 1,000 employees. Our respondent base includes 41% C-level executives.

France follows a similar EMEA-wide pattern with identity-related attacks. We find that in the last 12 months in France:

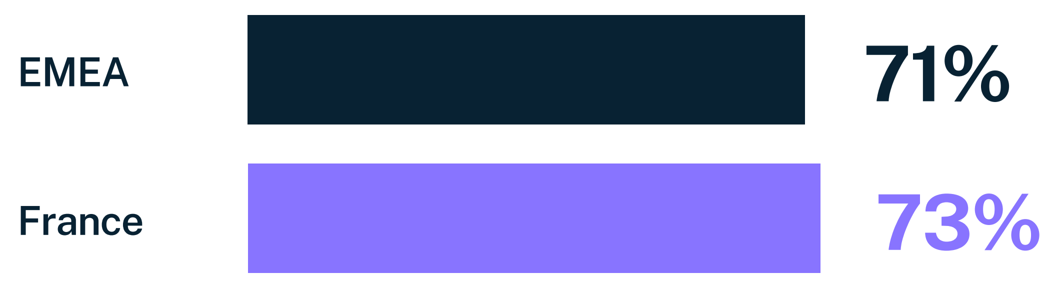
1. 94% faced an identity-related attack at least once compared to 94% in EMEA and
2. 93% faced two or more identity-related attacks compared to 94% in EMEA.

Amid the GenAI revolution, France faces cyber threats from a rising number of machine and third-party identities. The country is set to host Olympics and Paralympics games this summer and expects unprecedented cyber threats ranging from phishing, vishing, ransomware, deepfakes, and attacks on third- and fourth-party providers.

Let's look at how France compares to EMEA in the four key areas highlighted in this report.

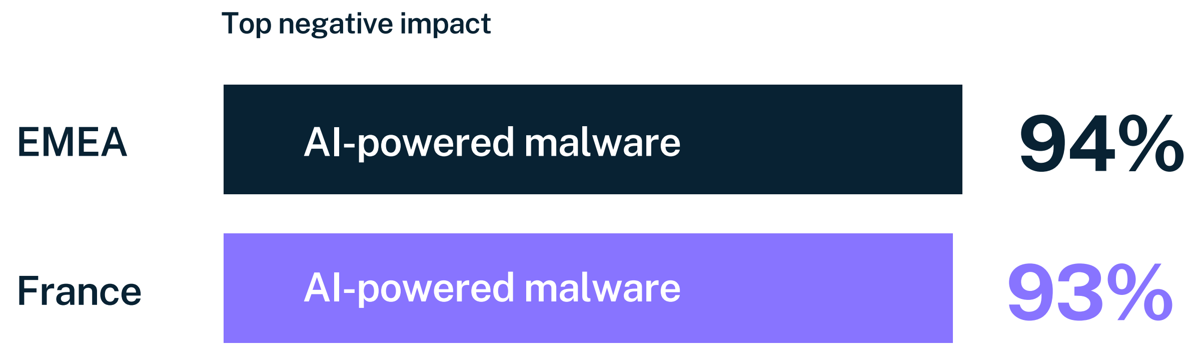
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders.



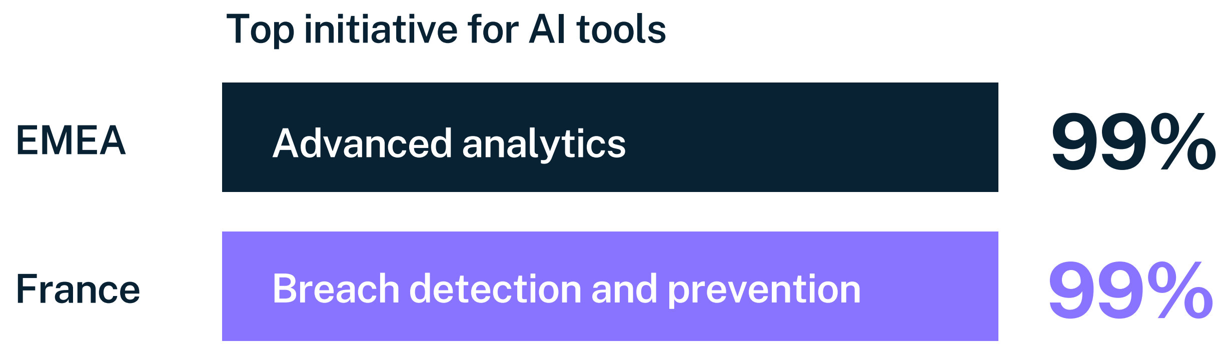
French C-Suite leaders are slightly more confident than their EMEA peers that employees can identify deepfakes of their leaders.

Expect negative impact from AI tools in 12 months



Only 10% of French organisations with less than 5,000 employees either don't know or don't expect any negative impact from AI tools.

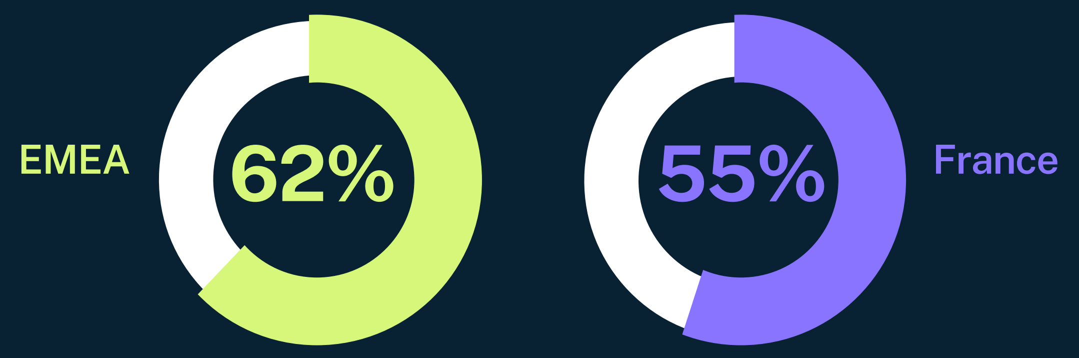
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



Leveraging AI tools for automation and flexibility is least priority for French organisations in the next 12 months.

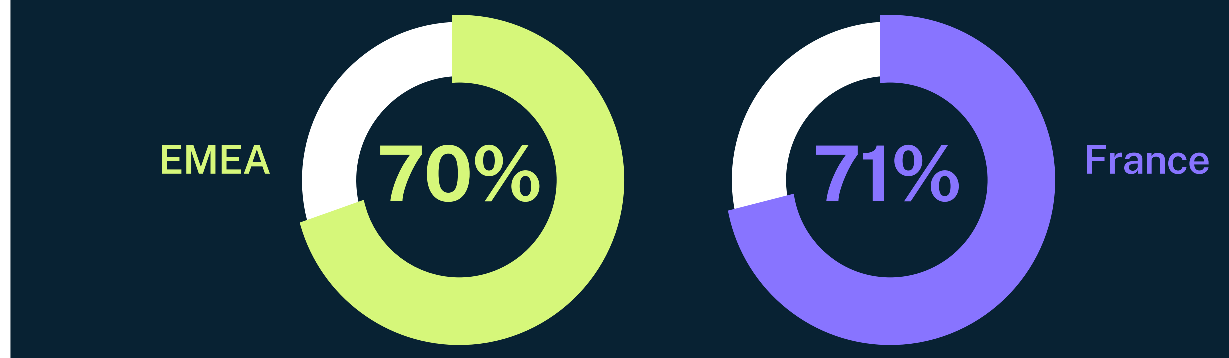
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



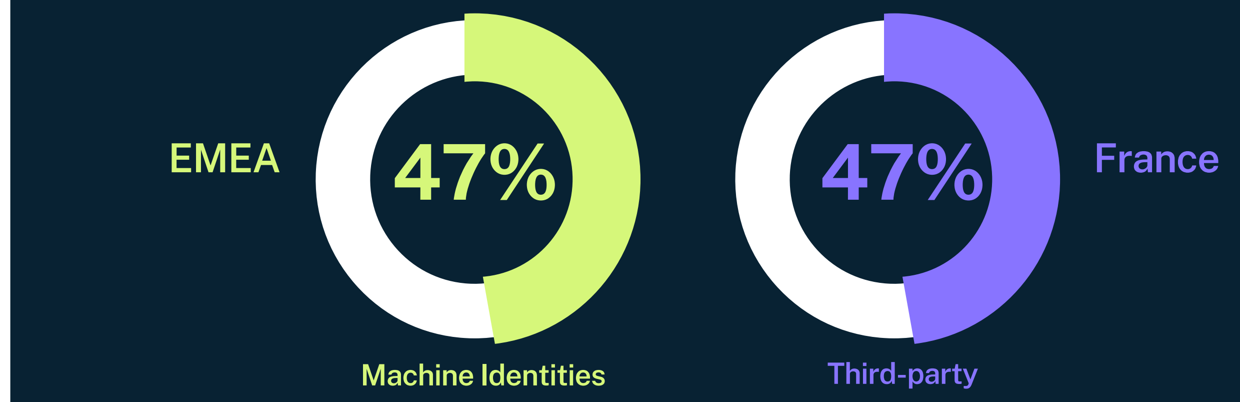
This 13% difference is because a higher percentage (49%) of C-level executives in France accurately define privileged users as both human and machine identities.

Respondents indicate up to 50% of machine identities have access to sensitive data



In France, over 70% of respondents indicate that up to half of human and machine identities can access sensitive data. The definition of 'privileged user' must expand to include machines.

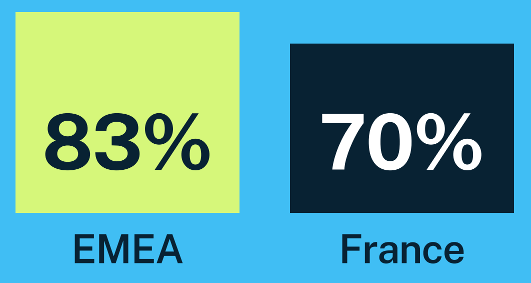
Riskiest identity types



French organisations report that overlooked risk posed by machine identities is among their top 3 security concerns.

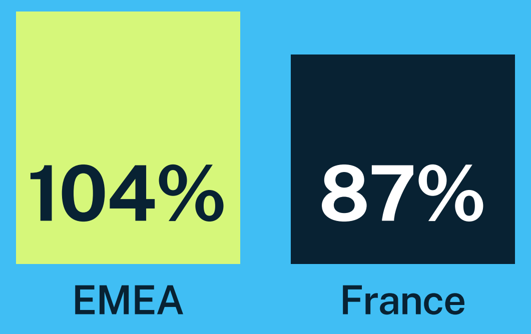
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



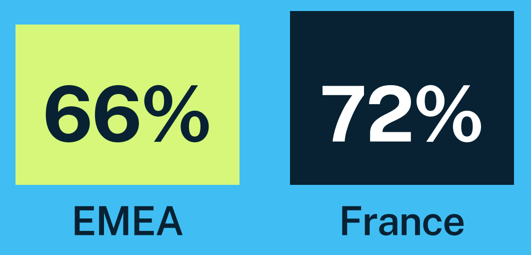
In EMEA, French organisations (41%) represent the lowest adoption of CSPs. In the next 12 months, France remains one of the two slowest adopters (next to Israel).

Expected annual growth of SaaS providers in the next 12 months



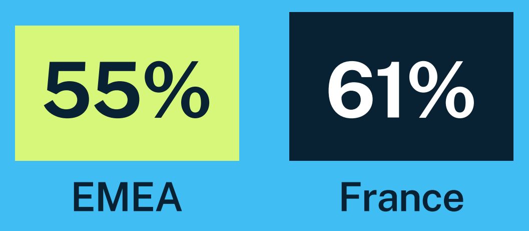
French respondents cite a growing number of applications (SaaS & on-premises) as among the top five reasons for an identity-related breach.

Are concerned about third-party risks



Last year, French organisations made the least investments in automating third-party identity management.

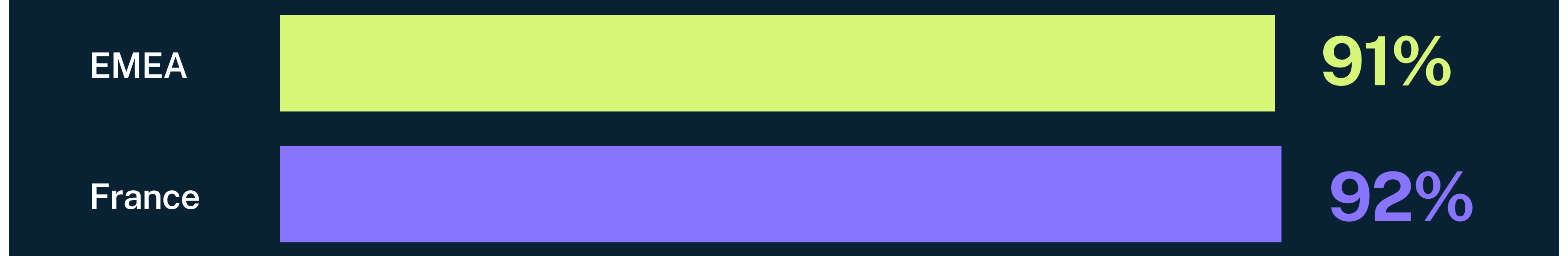
Are concerned about fourth-party risks



C-level French executives and similar cybersecurity experts are more concerned about third-party than fourth-party risks — indicating a gap in recognizing the growing threat of double supply chain attacks.

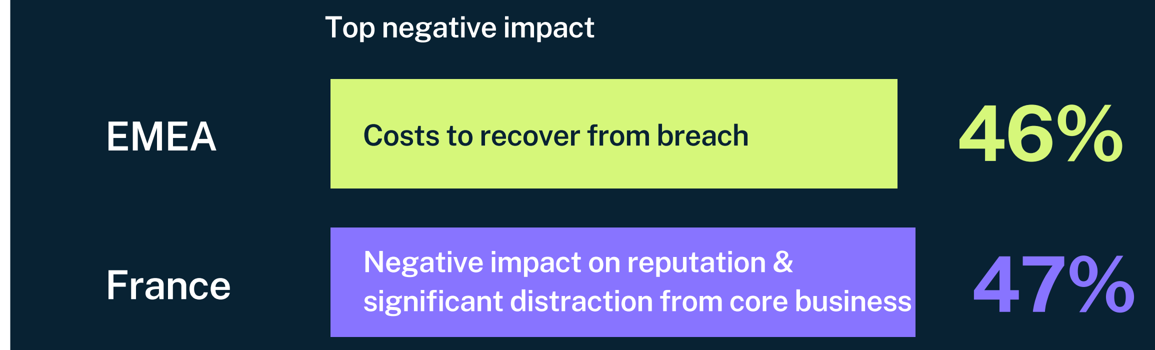
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



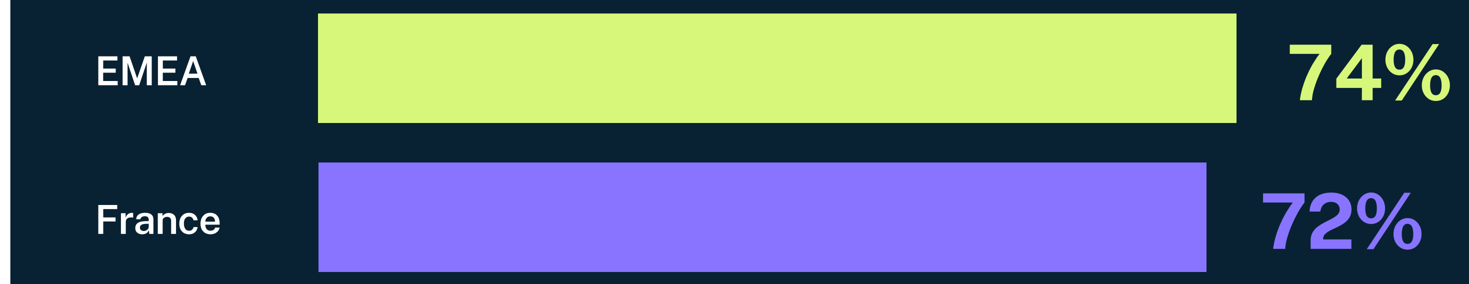
In response to increased attacks, 91% of French organisations have automated phishing analysis.

Organisations faced negative impacts on business results due to breach



71% of French organisations have subscribed to a cyber insurance policy. Only 1% of (vs. 6% in EMEA) indicated that they applied for cybersecurity insurance and were denied.

Organisations paid ransom but did not recover data



In the last 12 months, only 42% of French organisations (compared to 51% in EMEA) increased post-breach investments in identity-related products and services by 10% or more. This indicates a need for greater focus on identity-related cybersecurity initiatives.

Germany

In this report, we surveyed 150 respondents in Germany, with 91% from an organization with over 1,000 employees. Our respondent base includes 51% C-level executives.

Compared to EMEA, insights from Germany show fewer organisations faced an identity-related attack. We find that in the last 12 months in France:

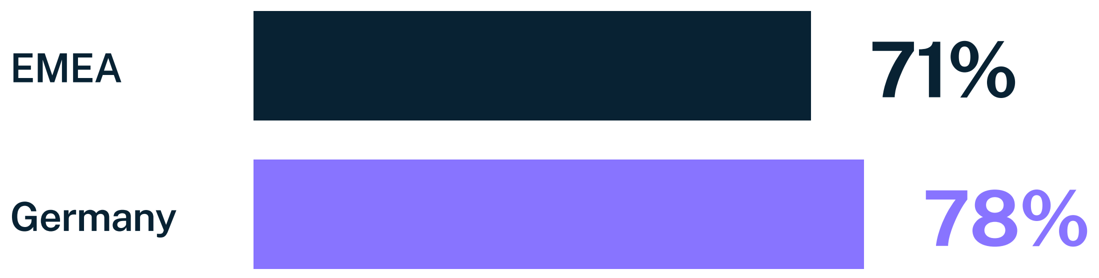
1. 86% faced an identity-related attack at least once compared to 94% in EMEA and
2. 85% faced two or more identity-related attack compared to 94% in EMEA.

Insights from Germany responses indicate an unmatched sense of forward thinking wherein organisations are increasing investments in securing machine identities in post breach environments and are concerned about AI-powered data poising and adversarial effects.

Let's look at how Germany compares to EMEA in the four key areas highlighted in this report.

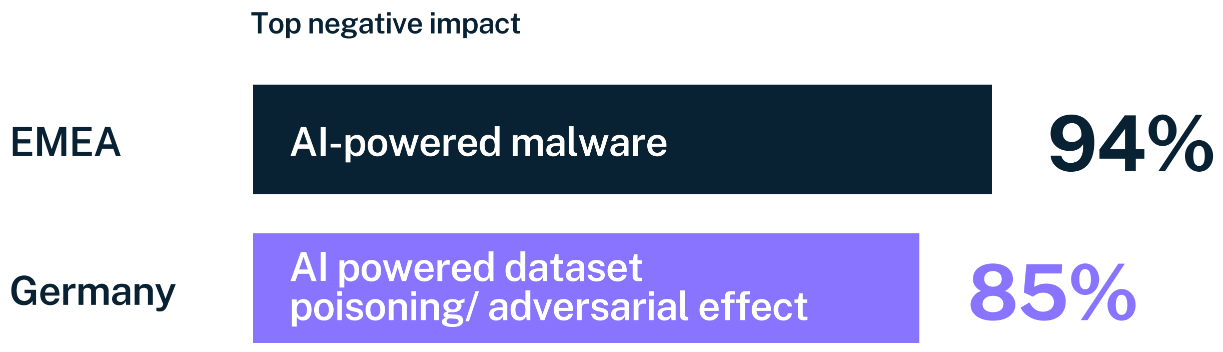
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



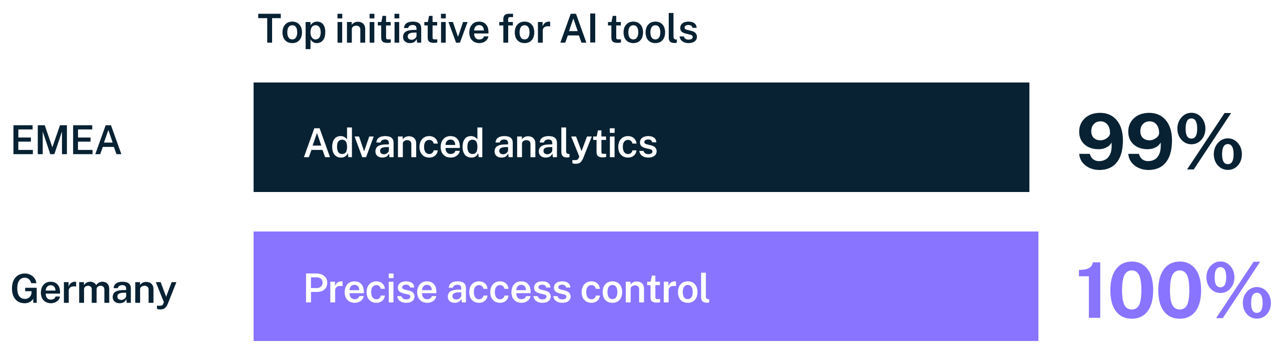
Germany is one of two countries (including Spain) that expect negative impact from AI-powered deepfake scams. Conversely, German respondents show high confidence in their employees' ability to identify deepfakes.

Expect negative impact from AI tools in 12 months



Germany is one of three countries in EMEA (including the Netherlands and Israel) that expect AI-powered dataset poisoning and adversarial effects.

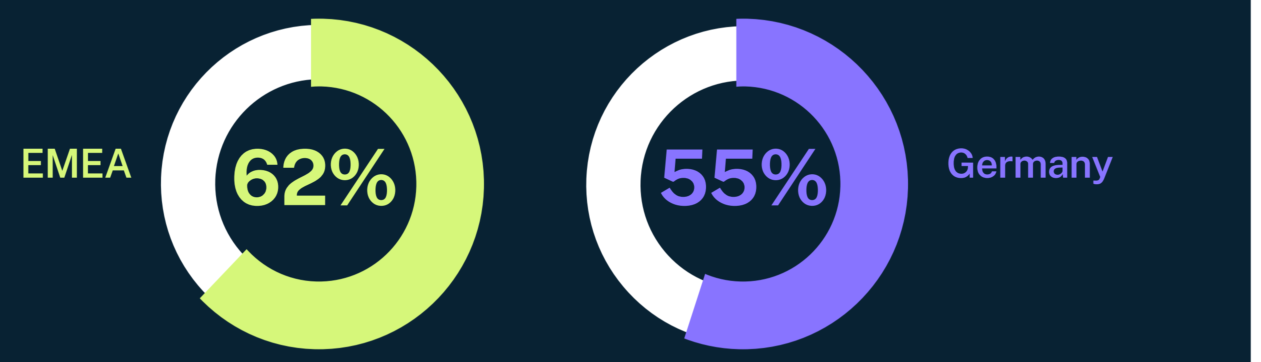
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



In the next 12 months, German organisations leverage AI to implement precise access control to secure every identity.

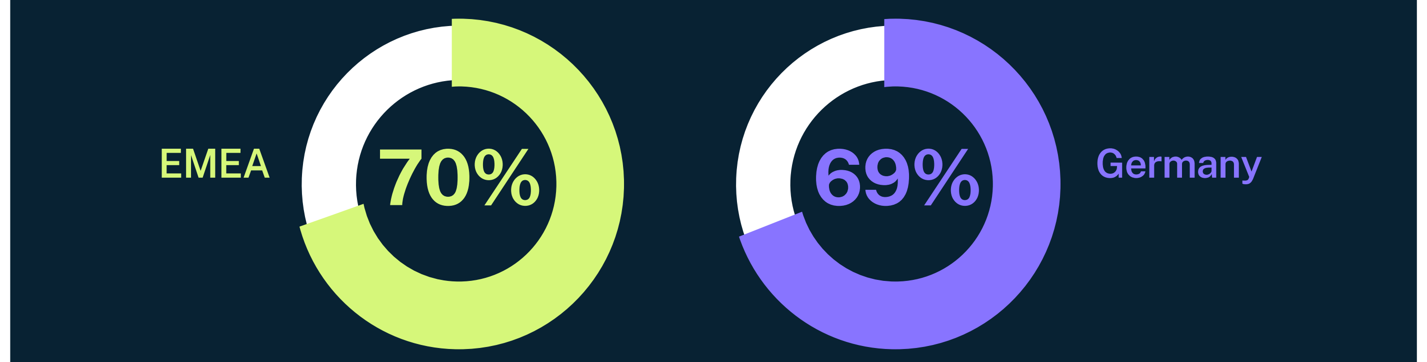
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



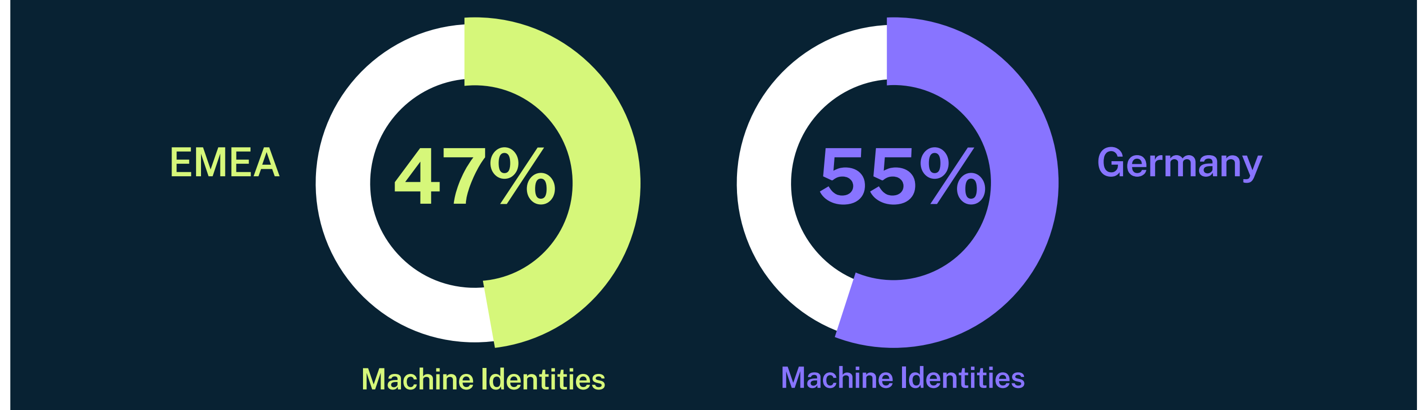
Similar to global and EMEA findings, machine identities are expected to drive the growth of the total number of identities.

Respondents indicate up to 50% of machine identities have access to sensitive data



Contrary to the global and EMEA findings, in the last 12 months, German organisations have invested in securing workload/machine identities as one of the top four investment priorities in post-breach scenarios.

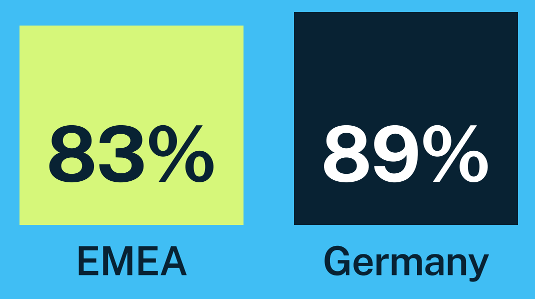
Riskiest identity types



German organisations are concerned with security concerns that are slowing down RPA and automation tool deployment, and security is unable to match the pace of app development.

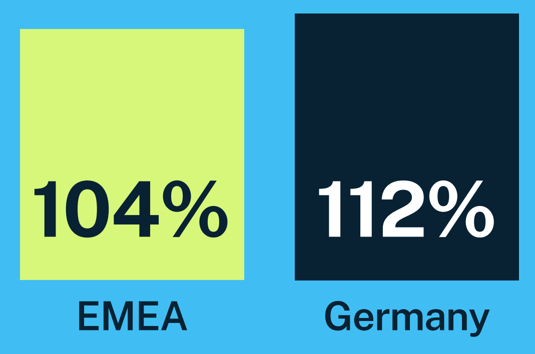
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



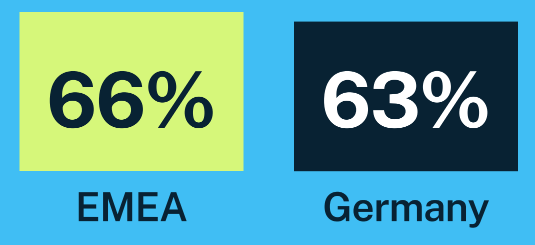
German organisations are expecting a 90% annual growth in use of 3 or more CSPs in the next 12 months.

Expected annual growth of SaaS providers in the next 12 months



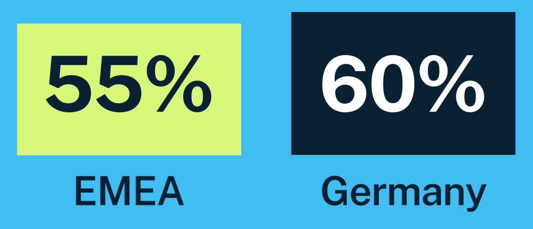
Despite the expected growth in total number of SaaS applications in the next 12 months, German organisations believe that it is the least likely reason to cause an identity-related breach.

Are concerned about third-party risks



Contrary to the concern about third-party risks, German organisations believe third-party identities are the least risky of all identity types.

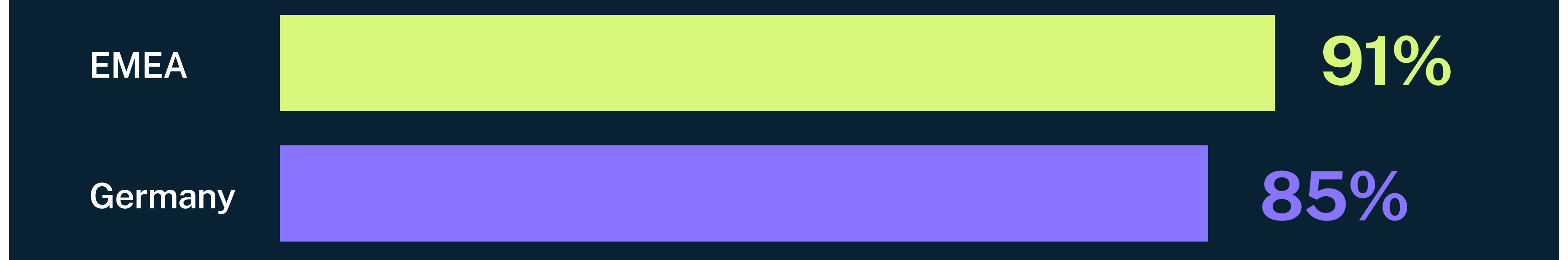
Are concerned about fourth-party risks



German organisations are more concerned about fourth-party providers than most EMEA responses, indicating a heightened awareness of double supply chain attacks.

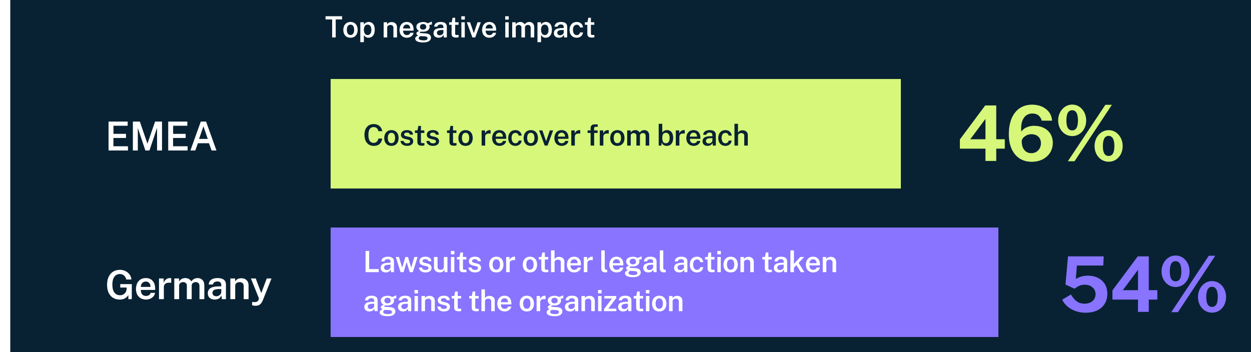
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



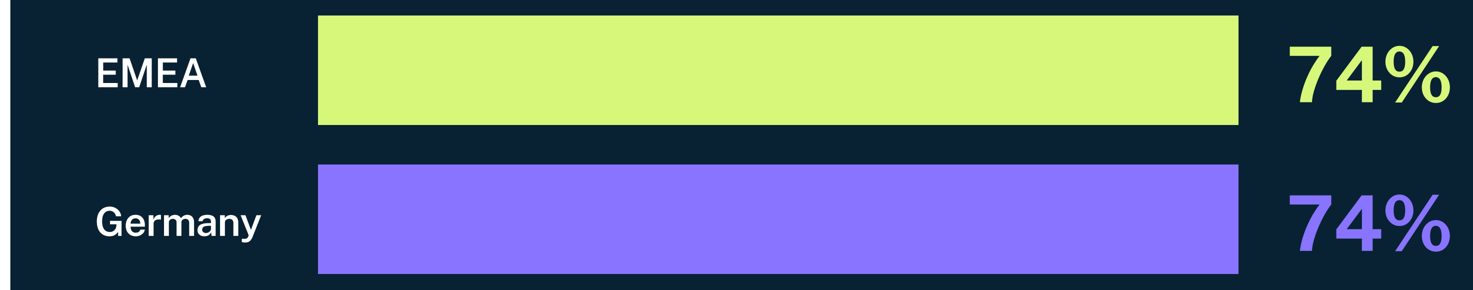
86% of German organisations have either fully or partially automated the phishing analysis processes.

Organisations faced negative impacts on business results due to breach



81% of the German organisations (nearly 10% more than most countries in EMEA) have subscribed to a cyber insurance policy.

Organisations paid ransom but did not recover data



In the next 12 months, 81% of German organisations will increase investments in identity-related products and services by more than 10%.

Italy

In this report, we surveyed 150 respondents in Italy, with 74% of respondents indicating that their organization had over 1,000 employees. Our respondent base includes 54% C-level executives.

Italy follows a similar pattern to EMEA in percentage of organisations that faced an identity-related attack. We find that in the last 12 months in Italy:

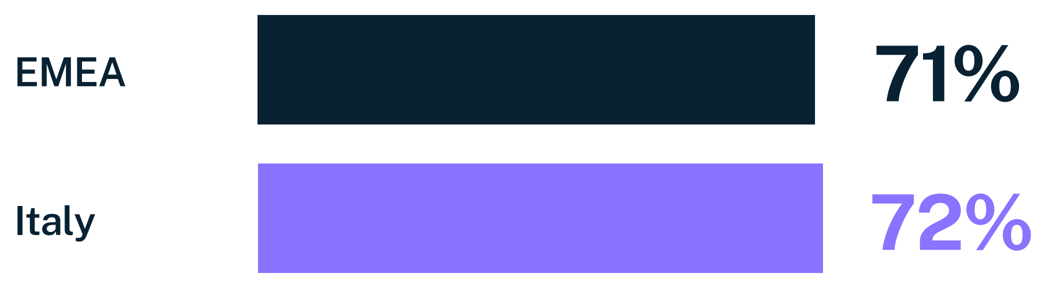
1. 90% faced an identity-related attack at least once compared to 94% in EMEA and
2. 90% faced two or more identity-related attack compared to 94% in EMEA.

In the next 12 months, 90% Italian organisations expect to adopt three or more CSPs compared to 83% in EMEA. Italian organisations are concerned with overprovisioned access and regulatory compliance as their top two cloud security concerns. Additionally, many Italian organisations suffer from lack of developer/engineering buy-in for corporate cybersecurity initiatives.

Let's look at how Italy compares to EMEA in the four key areas highlighted in this report.

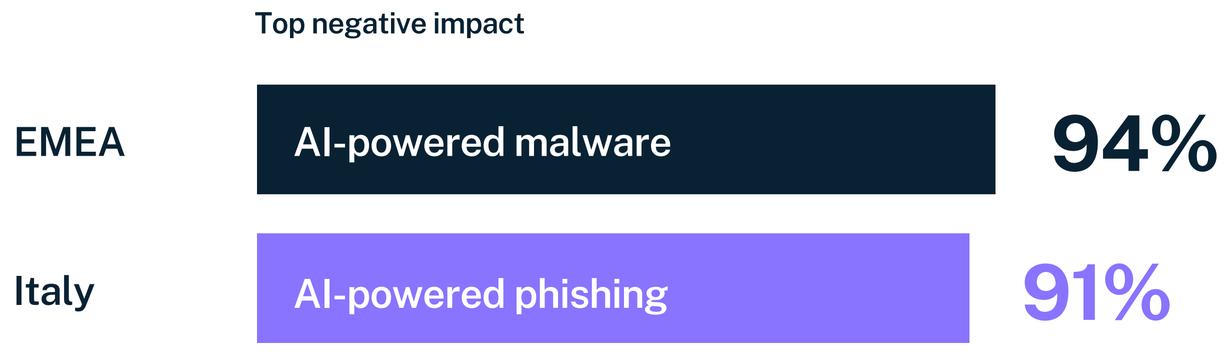
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



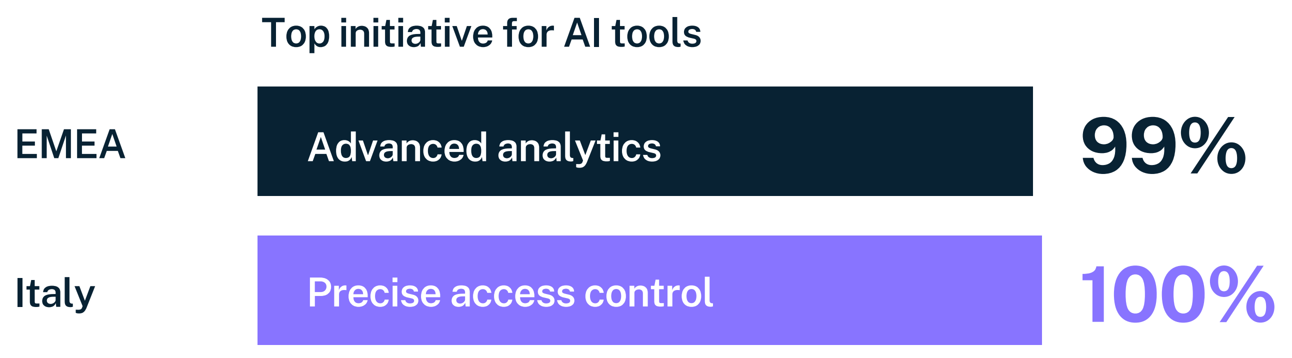
89% of Italian C-level executives are confident in their employees' ability to identify deepfakes of their leaders (compared to 64% of all other respondents)

Expect negative impact from AI tools in 12 months



14% of Italian C-level executives do not expect any negative impact from AI tools, compared to 3% of other respondents.

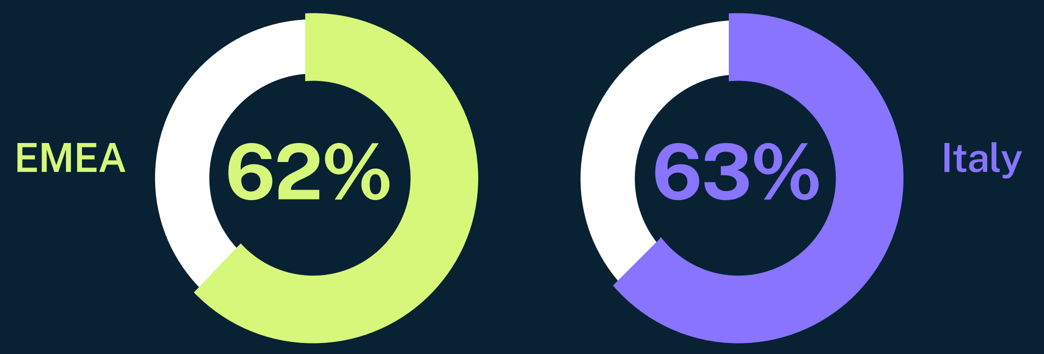
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



Advanced analytics is the top cybersecurity initiative among Italian organisations currently leveraging AI tools.

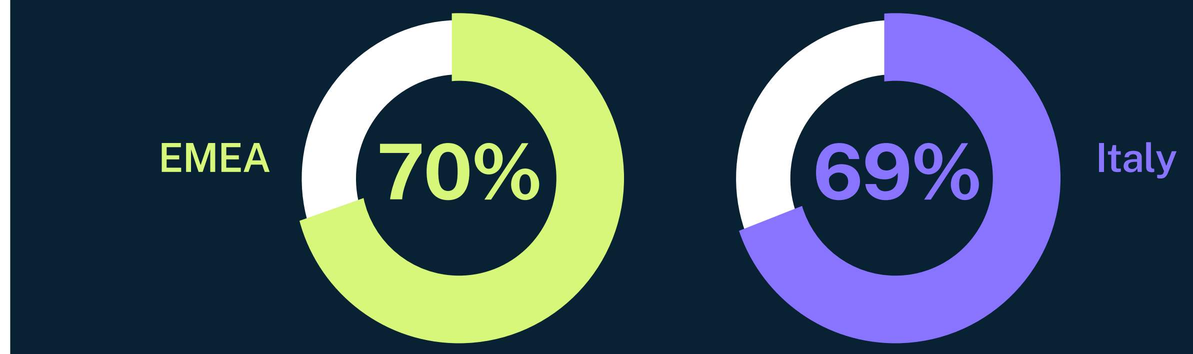
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



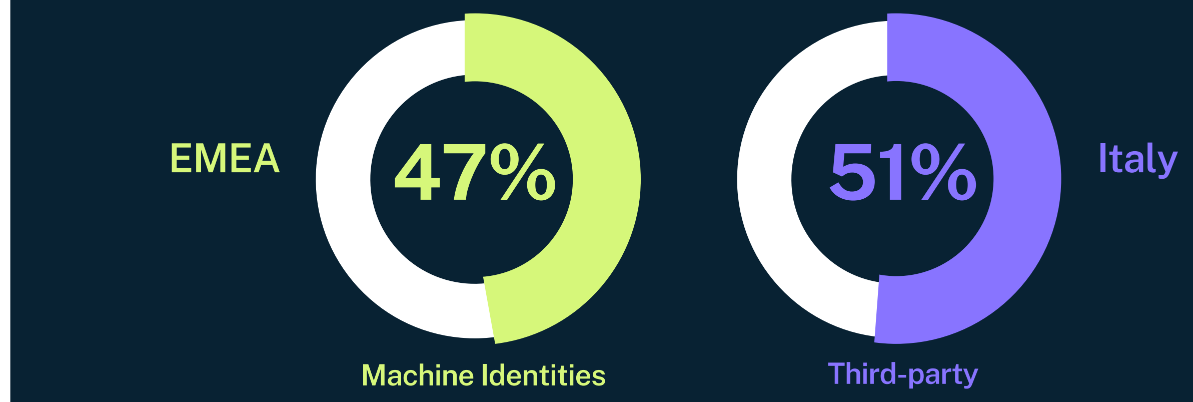
A higher percentage of C-level executives in Italy Respondents define ‘privileged user’ as human only compared to other cybersecurity experts surveyed in the country.

Respondents indicate up to 50% of machine identities have access to sensitive data



Italian organisations include workload and machine identities in their top four investment priorities in post-breach scenarios.

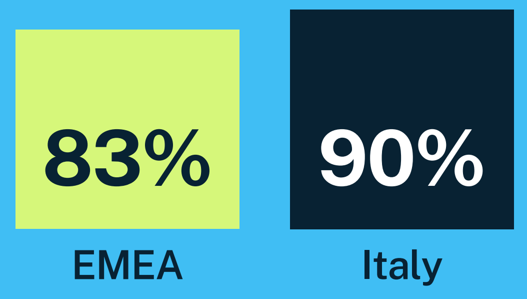
Riskiest identity types



28% of Italian organisations indicate that third-party relationships and machine identities will drive overall identity growth.

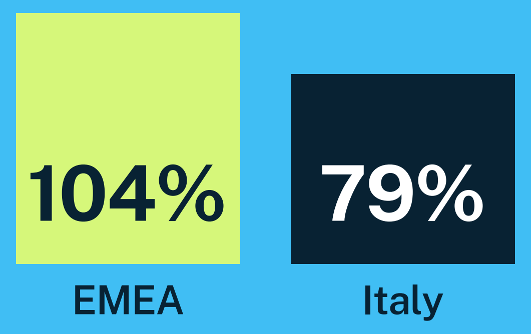
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



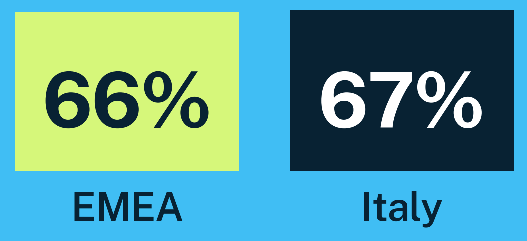
Italian organisations expect a higher annual growth rate of 3+ CSP adoption (57%) compared to EMEA (50%). Overprovisioned access remains a key concern in cloud environments.

Expected annual growth of SaaS providers in the next 12 months



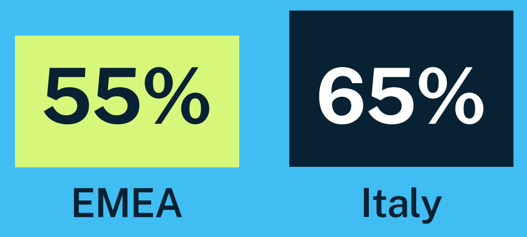
In the next 12 months, Italian organisations will use an average of 175 SaaS applications. However, they indicate that the growing number of on-prem and SaaS applications is one of three reasons least likely to cause an identity-related attack.

Are concerned about third-party risks



Like EMEA findings, despite a higher percentage of C-level executives (compared to other respondents) concerned about third-party risks, investments in vendor risk management are the lowest priority for Italian organisations.

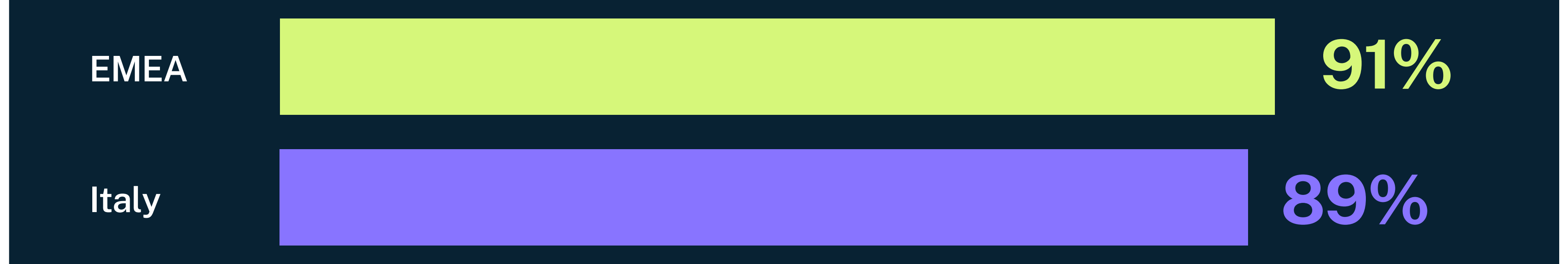
Are concerned about fourth-party risks



89% of C-level executives in Italian organisations are more concerned about fourth-party risks than other cybersecurity experts.

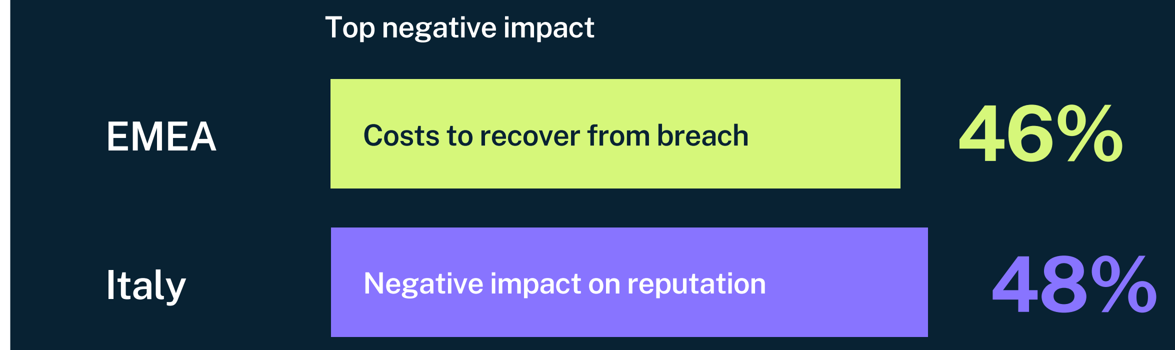
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



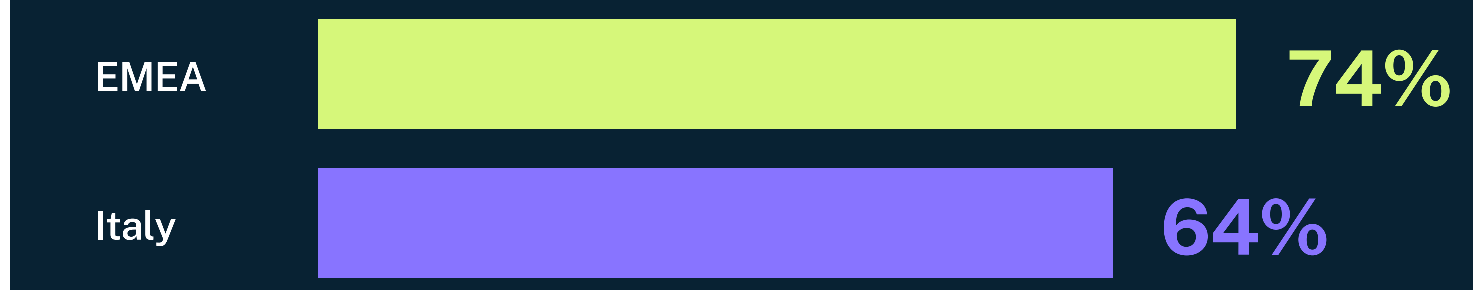
In response to the increasing attacks, 77% of Italian organisations have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



To reduce risk and cyber debt (similar to EMEA insights), more than 2/3 of Italian respondents indicated that their organization has subscribed to cyber insurance.

Organisations paid ransom but did not recover data



92% of Italian organisations plan to increase their investments in identity-related products and services by more than 10% in the next 12 months.

Israel

In this report, we surveyed 100 respondents in Israe, with 58% of Israel respondents indicating their organization had over 1,000 employees. Our respondent base includes 26% C-level executives.

Our Israel insights indicate a significantly high number of identity-related breaches compared to all countries in EMEA. We find that in the last 12 months in Israel:

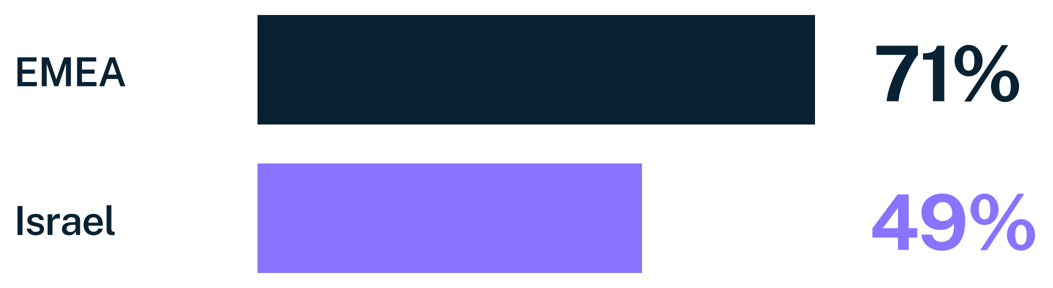
1. 100% faced an identity-related attack at least once compared to 94% in EMEA and
2. 100% faced two or more identity-related attack compared to 94% in EMEA.

Israel stands apart from pan-EMEA findings as the only country that is reversing its adoption rate of 3 or more CSPs. Notably, 75% of Israeli respondents indicate that they are currently leveraging 3 or more CSPs, but in the next 12 months only 51% will leverage 3 or more CSPs. Like the slowdown in adoption of 3 or more CSPs, Israel is the only country in EMEA that indicates a decline of 7% in the total number of SaaS applications in the year ahead. From a cloud security perspective, in addition to data theft, Israeli organisations consider software vulnerabilities as a key concern.

Let's look at how Israel compares to EMEA in the four key areas highlighted in this report.

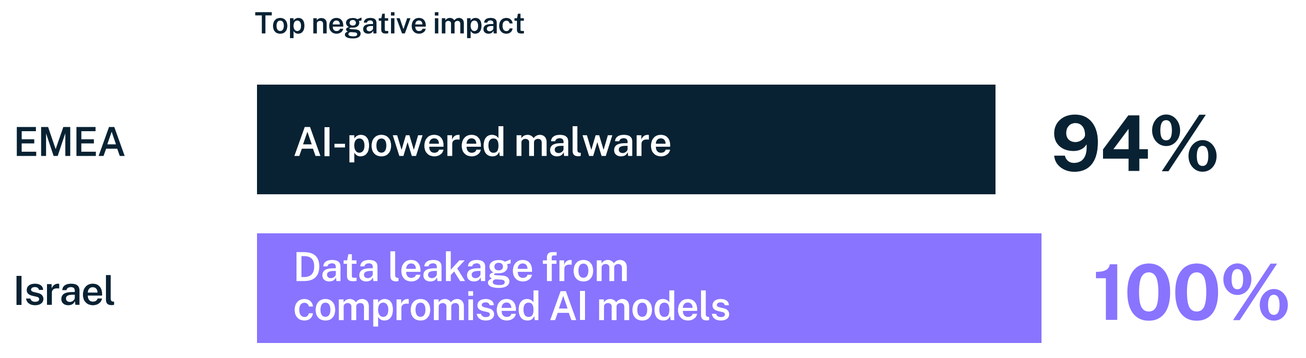
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



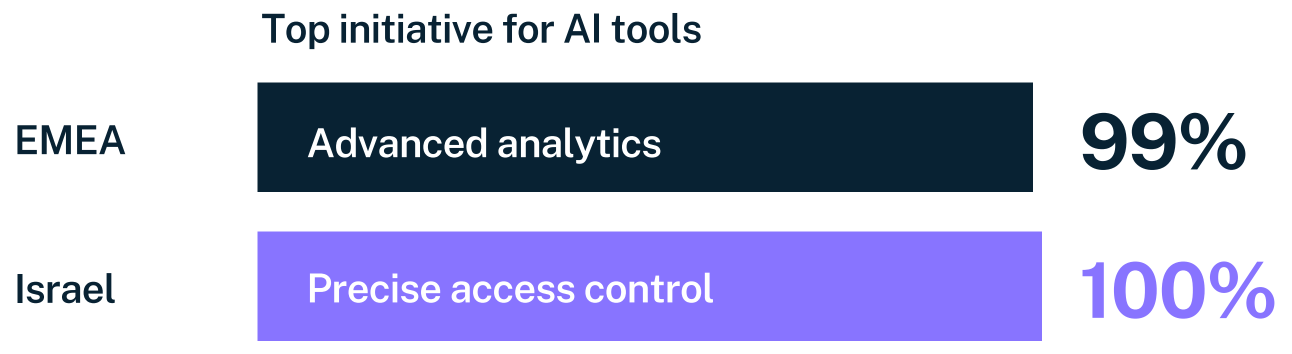
Israel is the only country in which more than half of the respondents (51%) are not confident in their employees' ability to identify deepfakes of their leaders.

Expect negative impact from AI tools in 12 months



Nearly half (48%) of organisations in Israel expect data leakage from compromised AI models to be the top negative impact of AI tools, followed by AI-powered data poisoning. Aside from Israel. The Netherlands is the only other country that expects the same negative impact from AI tools.

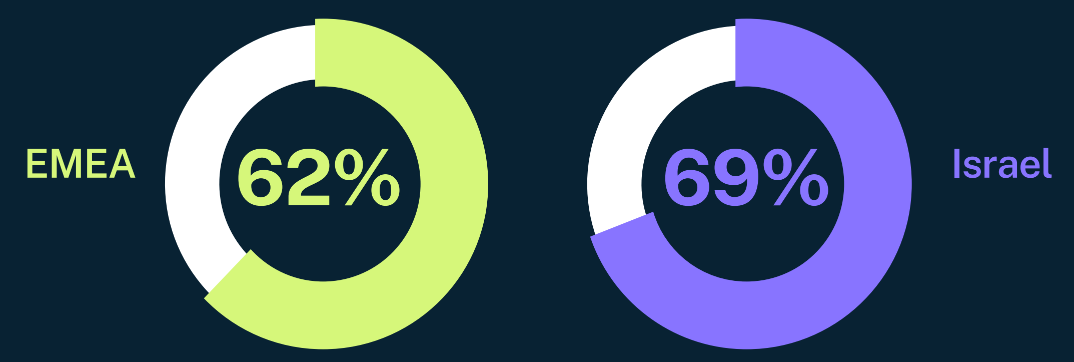
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



In the next 12 months Israeli organisations will prioritize leveraging AI tools to implement precise access control.

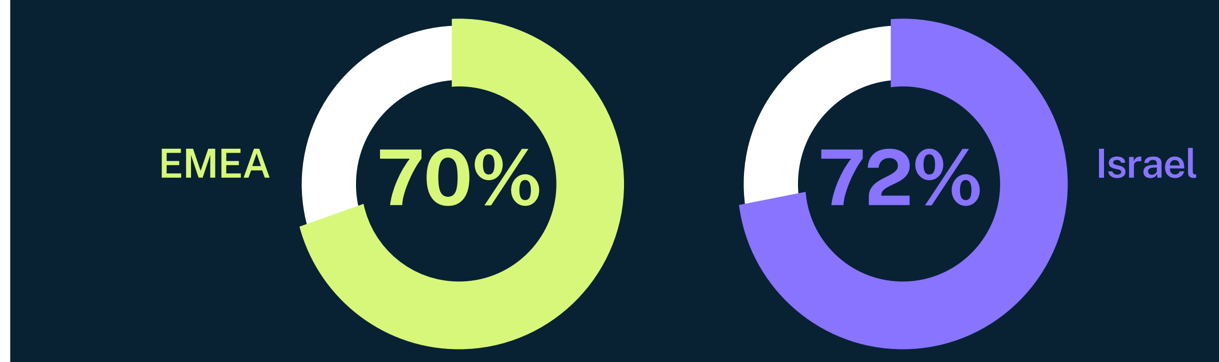
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



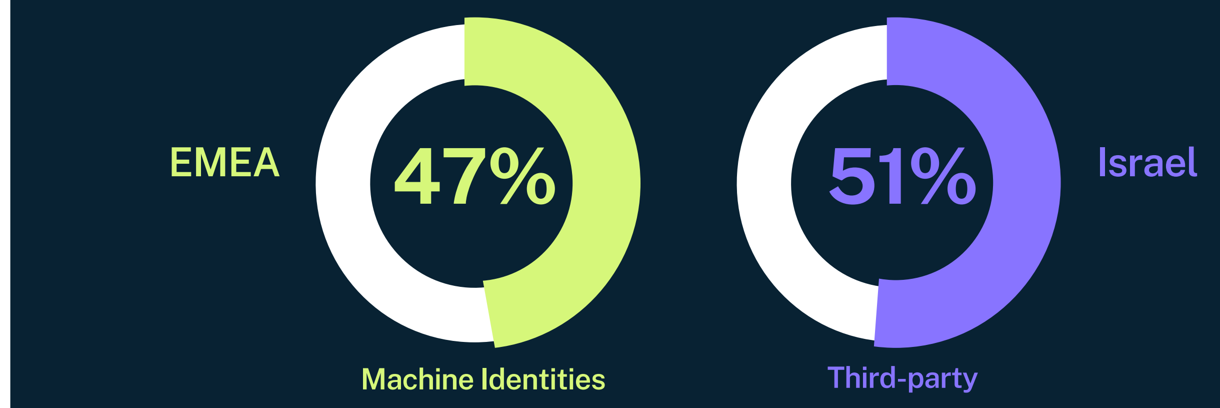
Israeli organisations indicate that a key concern regarding securing machine identities is that they mostly focus on securing human identities.

Respondents indicate up to 50% of machine identities have access to sensitive data



Investments in securing workload/machine identities are the lowest priority in post-breach scenarios for Israeli organisations.

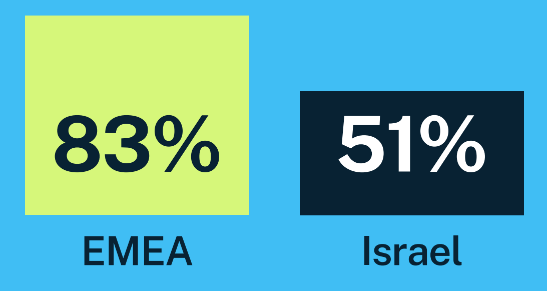
Riskiest identity types



While investments in securing machine identities remains low in Israel, over a quarter of Israeli organisations indicate that they have automated third-party identity management.

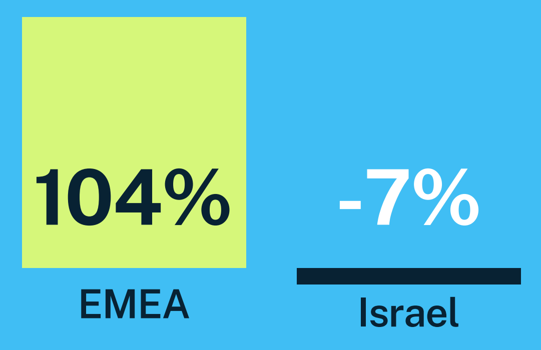
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



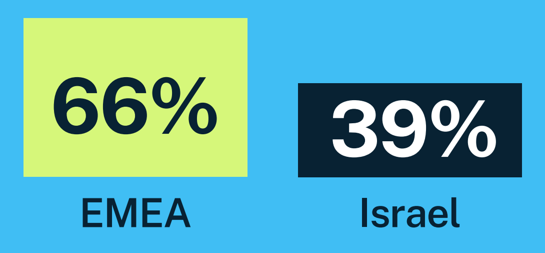
Israel is the only country in EMEA to indicate a 32% decline in usage of CSPs in 12 months. They report a lack of visibility across disparate hybrid environments which could result in the decision to reduce their CSPs.

Expected annual growth of SaaS providers in the next 12 months



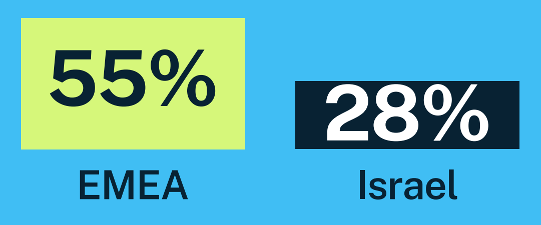
Israeli organisations indicate that a growing number of on-premises and SaaS applications are among the top three reasons for an identity-related breach.

Are concerned about third-party risks



Only a third (28%) of non-executive level respondents are concerned about third-party risks compared to 69% of C-level executives.

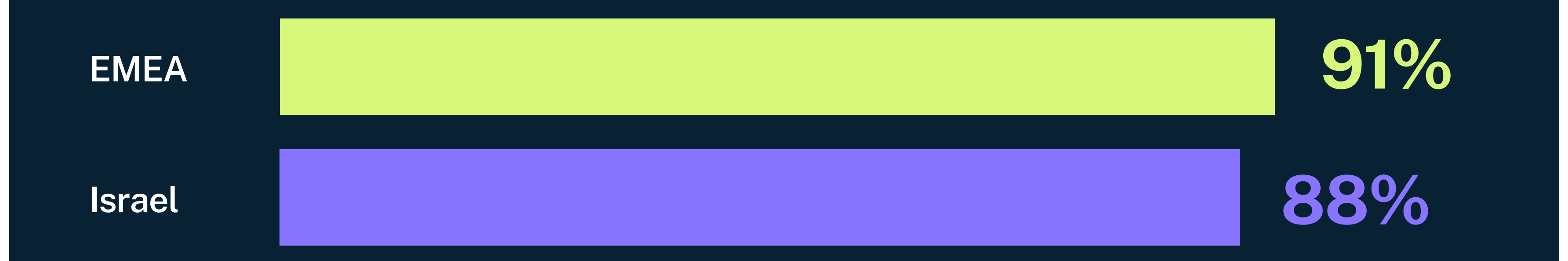
Are concerned about fourth-party risks



Insights from Israel indicate that they are not as concerned about fourth-party risks, pointing to a lack of understanding of double supply chain attacks.

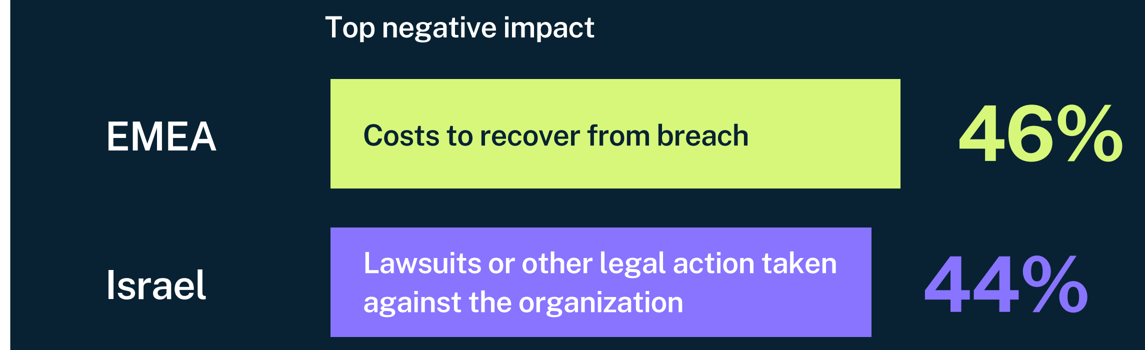
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



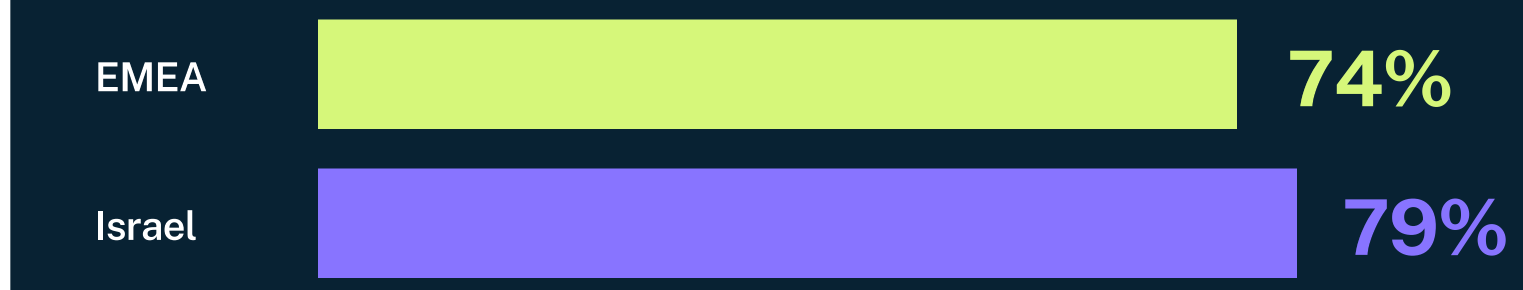
In response to increasing attacks, 83% of Israeli organisations have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



64% of the organisations in Israel have subscribed to a cyber insurance policy.

Organisations paid ransom but did not recover data



Owing to the growing number of identity-related attacks, 77% of Israeli organisations plan to increase investments in identity-related products and services by more than 10% in the next 12 months.

Netherlands

In this report, we surveyed 100 respondents in Netherlands, with 84% of respondents indicating their organization had over 1,000 employees. Our respondent base includes 55% C-level executives.

Netherlands follows a similar pattern to EMEA in percentage of organisations that have faced an identity-related attack. We find that in the last 12 months in Netherlands:

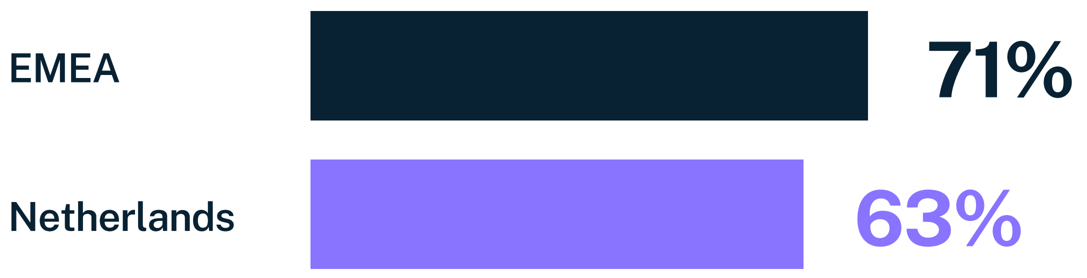
1. 96% faced an identity-related attack at least once compared to 94% in EMEA and
2. 96% faced two or more identity-related attack compared to 94% in EMEA.

A third of respondents in the Netherlands indicate that digital transformation initiatives are most likely to cause an identity-related breach in their organization. This risk will be further amplified as 93% of respondents will leverage three or more CSPs in the next 12 months, compared to 49% who leverage 3 or more CSPs today. In terms of cloud security, the Netherlands is the only country that ranks regulatory compliance as the top concern, followed by concerns regarding data protection. While machine identities are driving the overall growth of identities for Netherlands-based respondents, they indicate third-party identities as being the riskiest identity type.

Let's look at how the Netherlands compares to EMEA in the four key areas highlighted in this report.

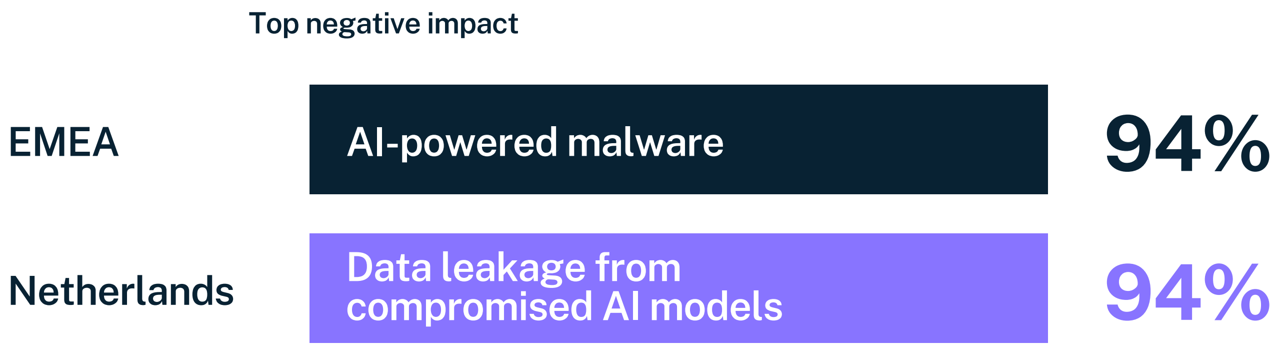
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



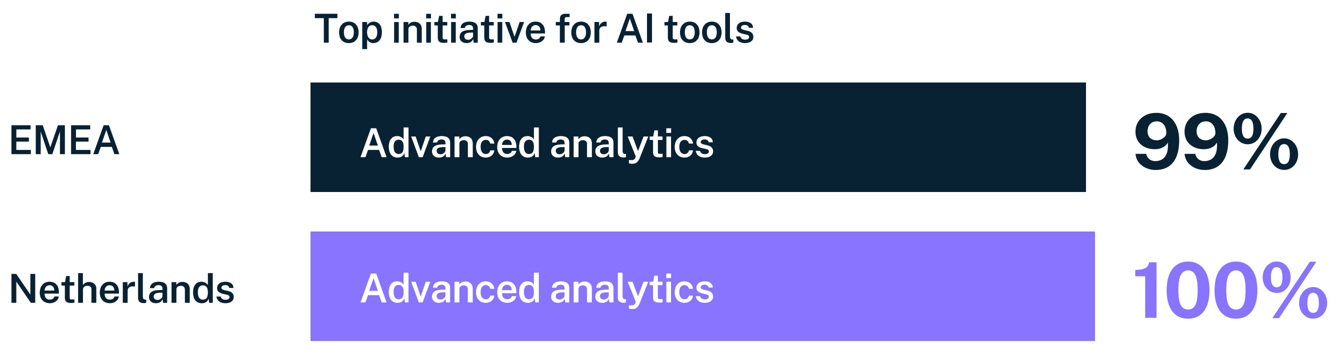
The Netherlands is the only country in which both C-level executives and other respondents are equally confident in their employees' ability to identify deepfakes of their leaders.

Expect negative impact from AI tools in 12 months



In Netherlands, C-level executives expect AI-powered dataset poisoning to be a greater threat than data leakage from compromised AI models.

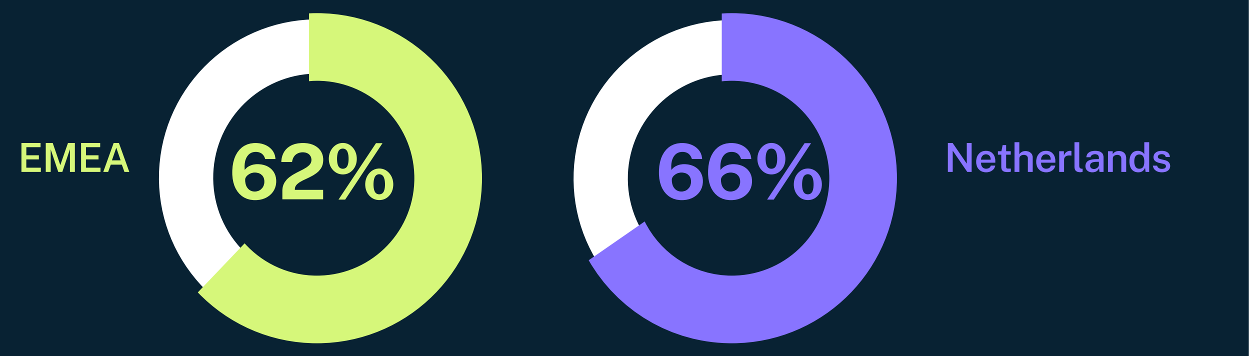
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



Currently, organisations in the Netherlands leverage AI tools for automation and flexibility. In the next 12 months they will focus on advanced analytics.

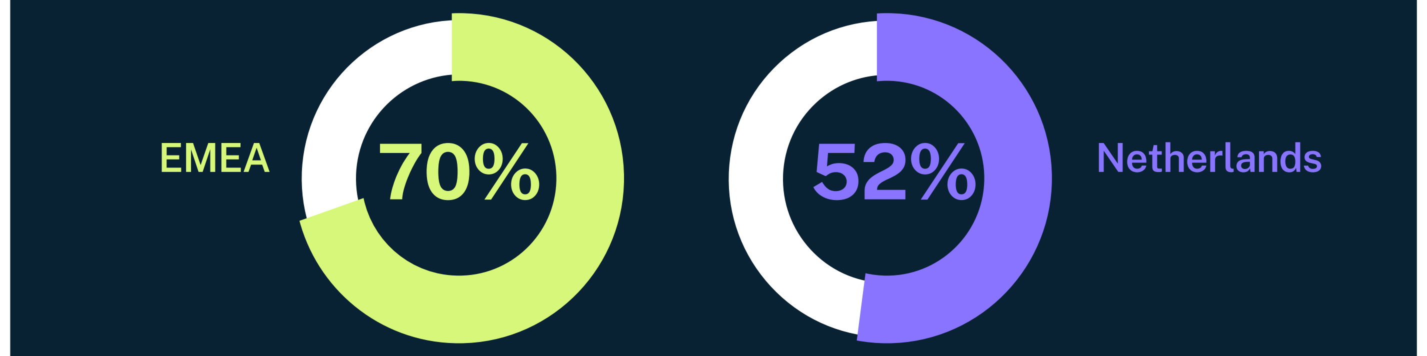
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



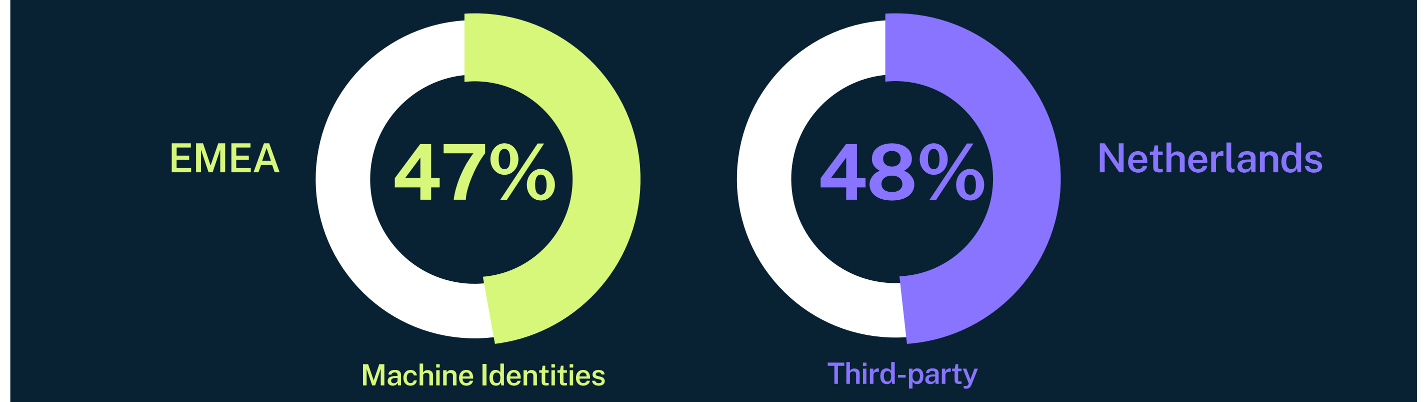
In the Netherlands, all respondents (C-level vs. others) largely define ‘privileged users’ as human identities only but we find greater alignment on the fact that this is an incorrect definition.

Respondents indicate up to 50% of machine identities have access to sensitive data



A higher number of Netherlands respondents (48%, compared to 30% from EMEA) indicate that more than 50% of machine identities have access to sensitive data.

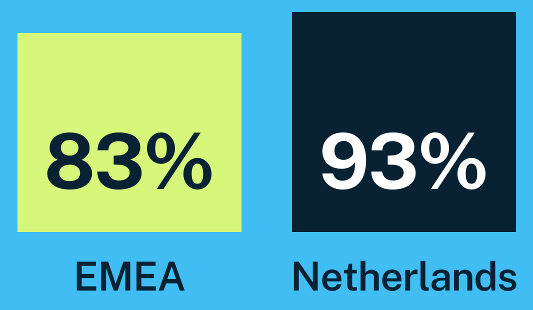
Riskiest identity types



Business growth fuels the rise in identity numbers but machine identities are overlooked.

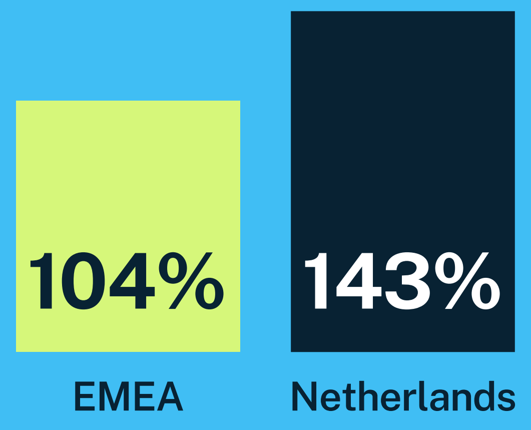
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



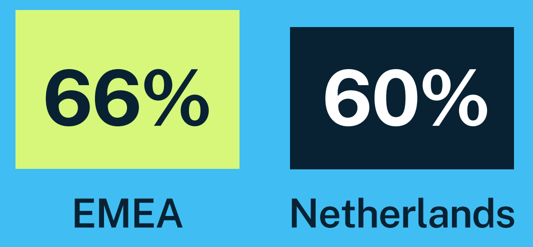
Organisations in the Netherlands (including Germany) anticipate a greater 3+ CSP adoption annual growth rate (90%) than EMEA (50%). One of the fundamental concerns in cloud systems is still regulatory compliance.

Expected annual growth of SaaS providers in the next 12 months



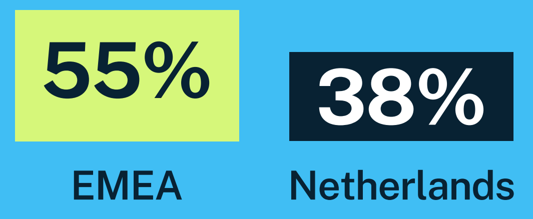
Application proliferation is one of the nation's #2 causes of breaches.

Are concerned about third-party risks



In comparison to other nations, the Netherlands has a lower percentage of respondents that are concerned about fourth-party risks.

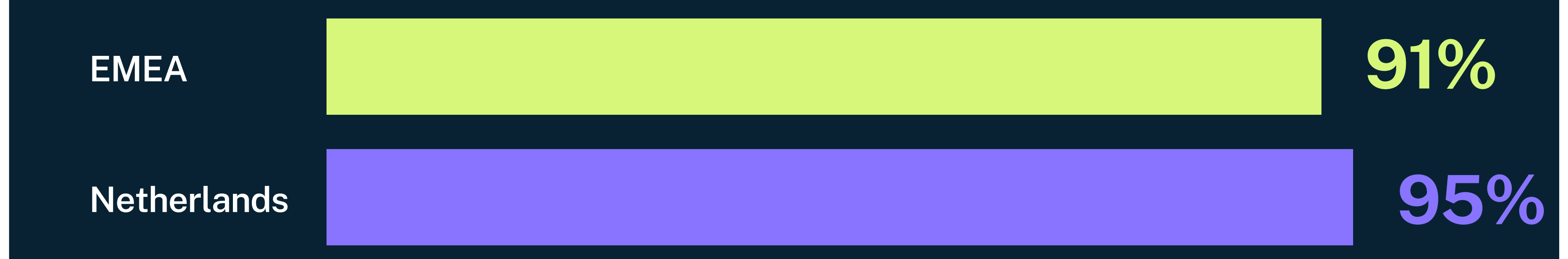
Are concerned about fourth-party risks



In the Netherlands, cyber specialists and C-level executives are more concerned about third-party risks than fourth-party threats, suggesting a lack of awareness regarding the increasing threat posed by double supply chain attacks.

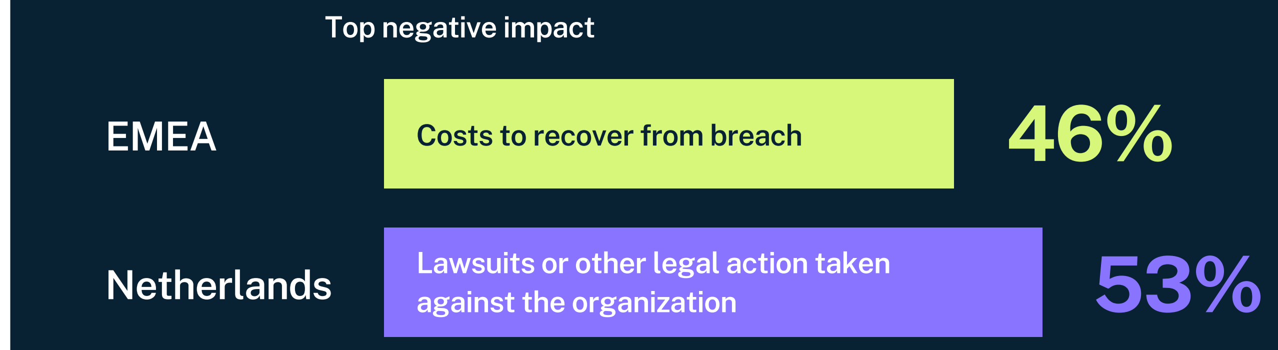
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



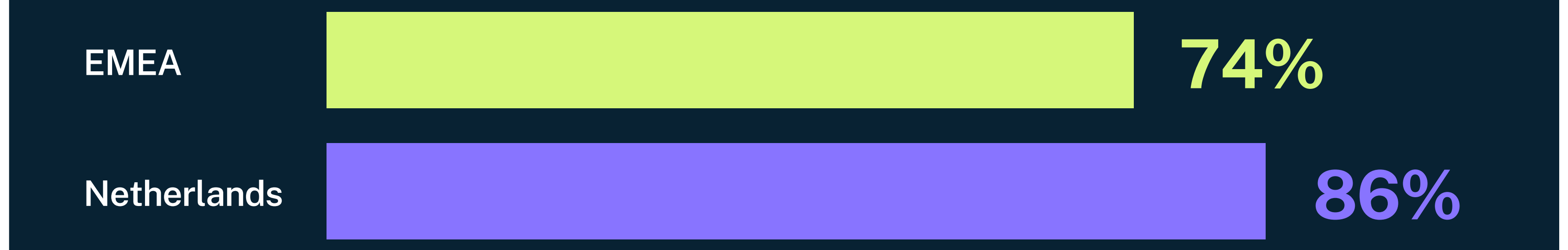
In response to the increase in attacks, 91% of respondents in the Netherlands have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



69% of the Netherlands' organisations have subscribed to a cyber insurance policy.

Organisations paid ransom but did not recover data



Employees in the Netherlands consider significant distractions from core business among the #2 post-breach impacts in their organisations.

EMEA COUNTRY SPOTLIGHT: SPAIN

Spain

In this report, we surveyed 150 respondents in Spain, with 68% of respondents indicated their organization had over 1,000 employees. Our respondent base includes 10% C-level executives.

Spain follows a similar pattern to EMEA in percentage of organisations that have faced an identity-related attack. We find that in the last 12 months in Spain:

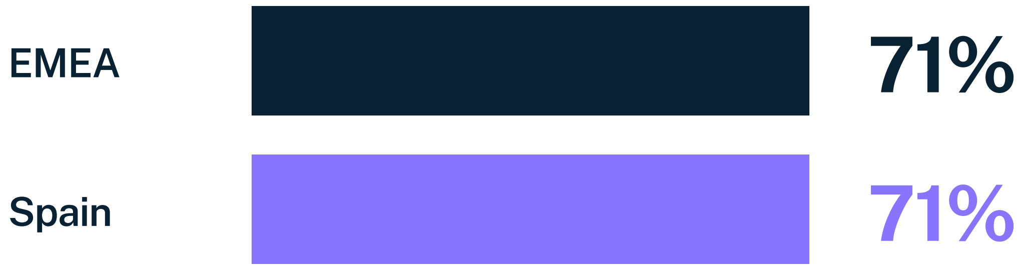
1. 97% faced an identity-related attack at least once compared to 94% in EMEA and
2. 97% faced two or more identity-related attack compared to 94% in EMEA.

Respondents in Spain indicate that digital transformation initiatives, a vulnerable identity access management (IAM) and usage of third-parties or external vendors are among the top three causes of identity-related attacks in their organisations. Machine identities are driving the annual growth of the total number of identities and are the riskiest identity type. Eighty-one percent of respondents indicate that up to 50% machine identities have access to sensitive data, but less than half (41%) indicate that their organisation defines 'privileged users' as both human and machine identities.

Let's look at how Spain compares to EMEA in the four key areas highlighted in this report.

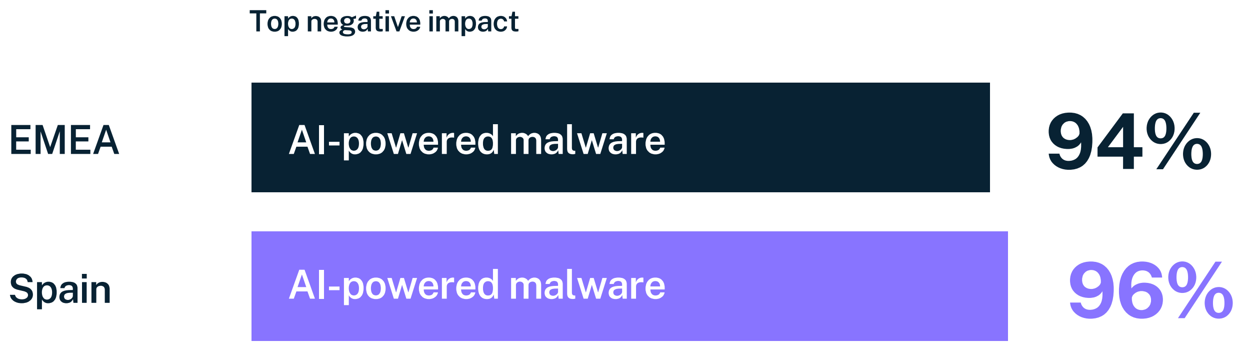
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



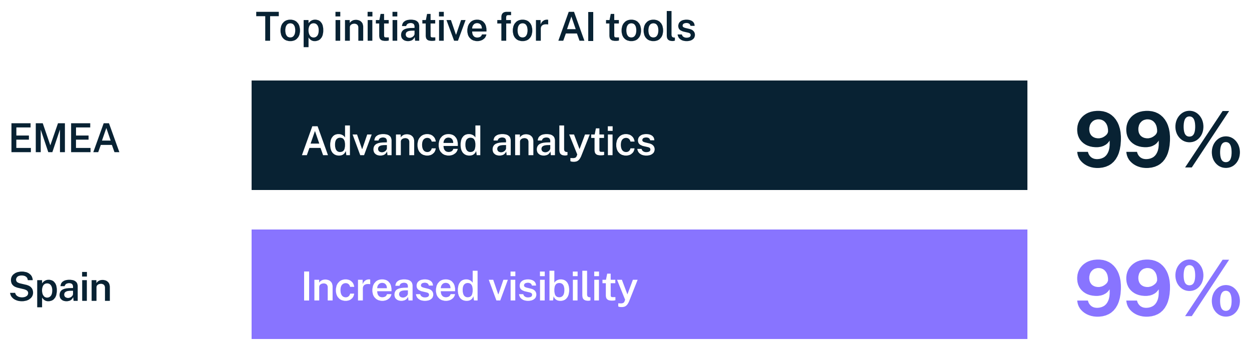
In Spain, nearly all (99%) C-level executives are more confident that their employees can identify deepfakes of their leaders, compared to other respondents (68%).

Expect negative impact from AI tools in 12 months



Respondents in Spain reported that rapid adoption of GenAI is the least likely to cause an identity-related breach.

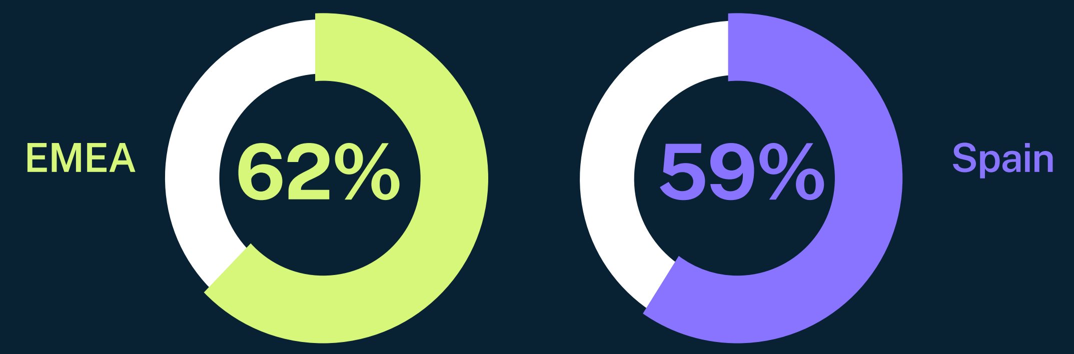
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



Respondents in Spain indicate that their organisation leverages AI tools in identity security initiatives to address the lack of cybersecurity skills. In the next 12 months, they will leverage AI tools to increase visibility.

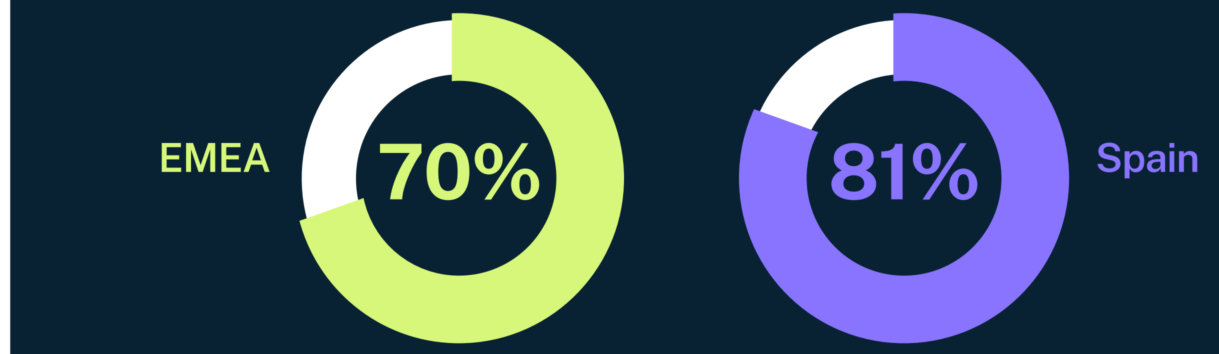
2. New Era: Rise of the Machines

Respondents define ‘privileged user’ as human-only



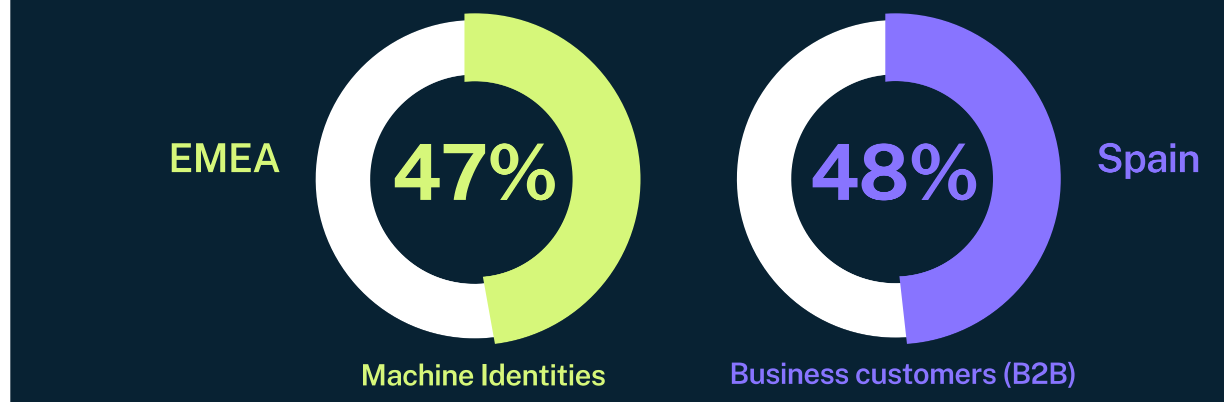
Insights from Spain are consistent with global and EMEA findings in that machine identities are primary drivers of annual growth of all identity types.

Respondents indicate up to 50% of machine identities have access to sensitive data



Spanish organisations have witnessed a surge in investments in machine identities, ranking among the top #5 technologies.

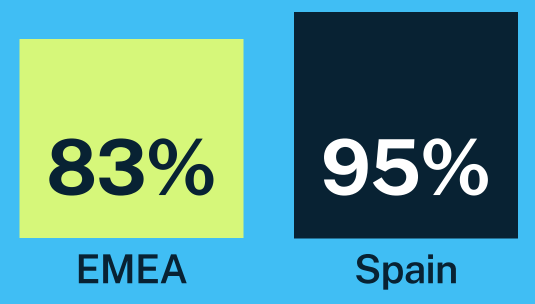
Riskiest identity types



The majority of the employees in the UAE consider unmanaged DevOps, CI/CD pipelines, and development environments posing significant security risks in their organisations.

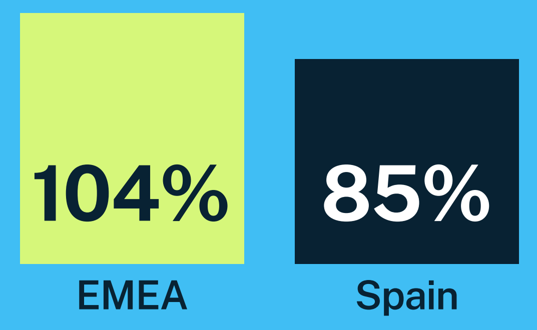
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



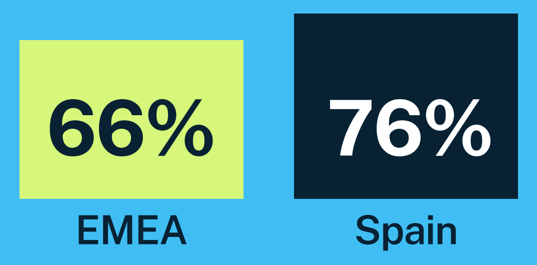
Organisations in Spain anticipate a greater 3+ CSP adoption annual growth rate (59%) than EMEA (50%).

Expected annual growth of SaaS providers in the next 12 months



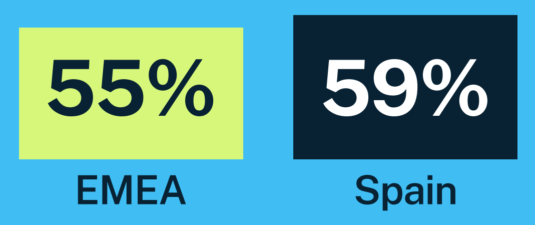
Spanish respondents indicate that they will use an average of 136 SaaS apps over the next 12 months. They also indicate that a growing number of on-premises and SaaS apps are among the top four causes of an identity-related breach.

Are concerned about third-party risks



Nearly a quarter (23%) of Spanish organisations indicate that using third parties or external vendors could lead to security breaches.

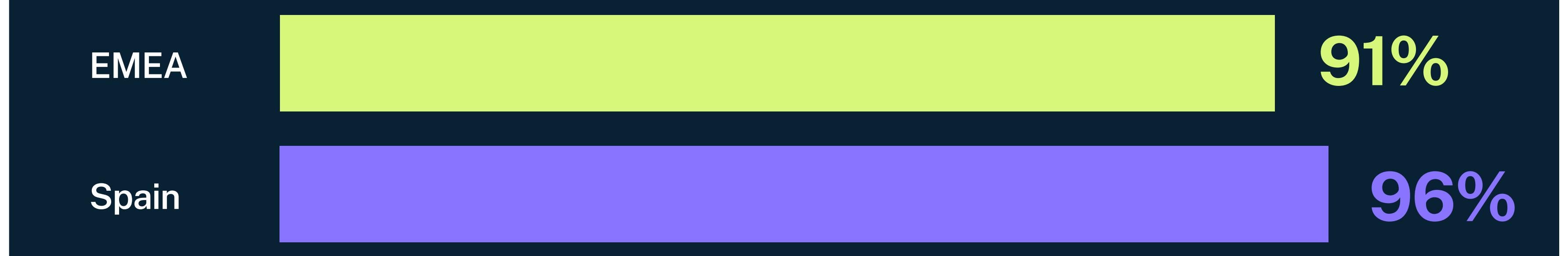
Are concerned about fourth-party risks



Three-quarters (67%) of non-executive level respondents are more concerned about fourth-party risks than C-level leaders in Spain.

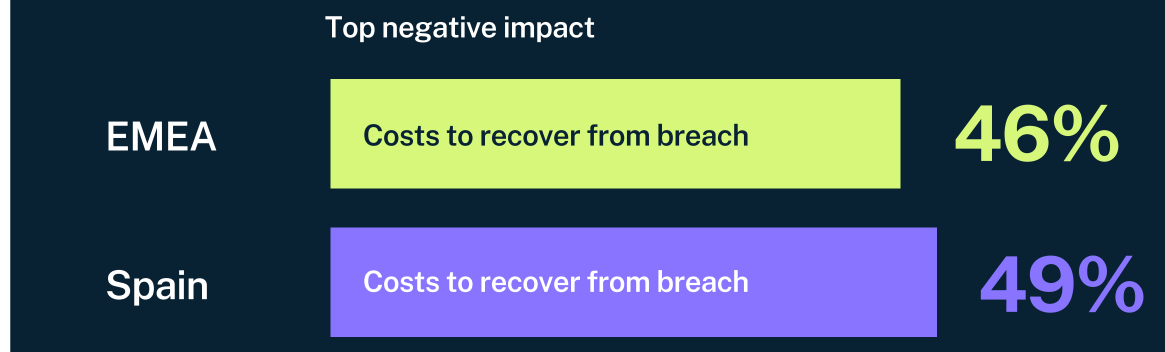
4. Cyber Debt: "Shiny Object" Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



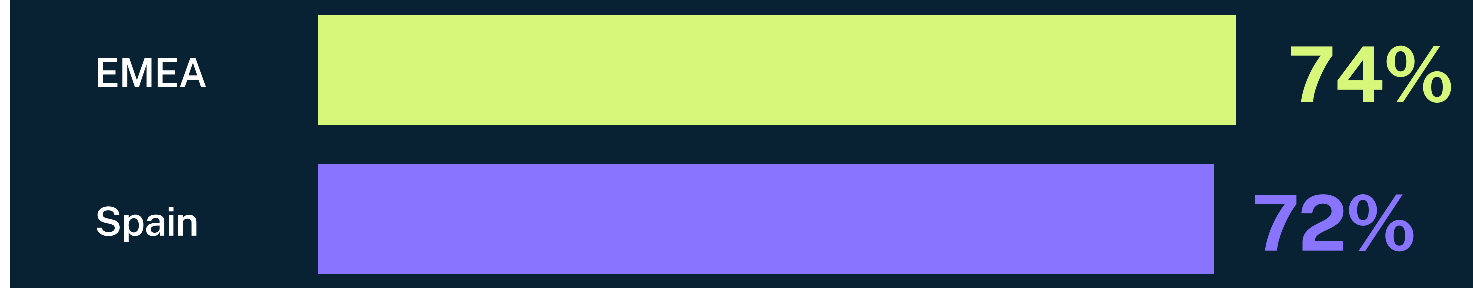
In response to the increasing attacks, 83% of Spain's organisations have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



To reduce risk and cyber debt, 72% of organisations in Spain have subscribed to cyber insurance policies.

Organisations paid ransom but did not recover data



83% of organisations in Spain plan to increase investments in identity-related products and services by more than 10% in the next 12 months

United Arab Emirates

In this report, we surveyed 100 respondents in UAE, with 86% of UAE respondents indicating their organization had over 1,000 employees. Our respondent base includes 43% C-level executives.

Like Israel, organisations in the UAE also suffered a higher volume of identity-related attacks compared to EMEA. We find that in the last 12 months in UAE:

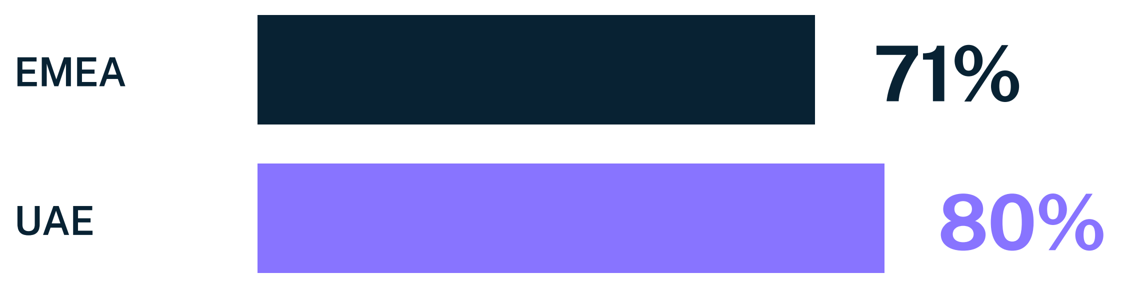
1. 99% faced an identity-related attack at least once compared to 94% in EMEA and
2. 99% faced two or more identity-related attack compared to 94% in EMEA.

UAE is the only country wherein respondents indicate that remote and hybrid work continues to be the number one cause of an identity-related breach in their organisation. In post-breach situations over the last 12 months, organisations in the UAE have invested in securing endpoints along with identity access governance (IGA) capabilities.

Let's look at how UAE compares to EMEA in the four key areas highlighted in this report.

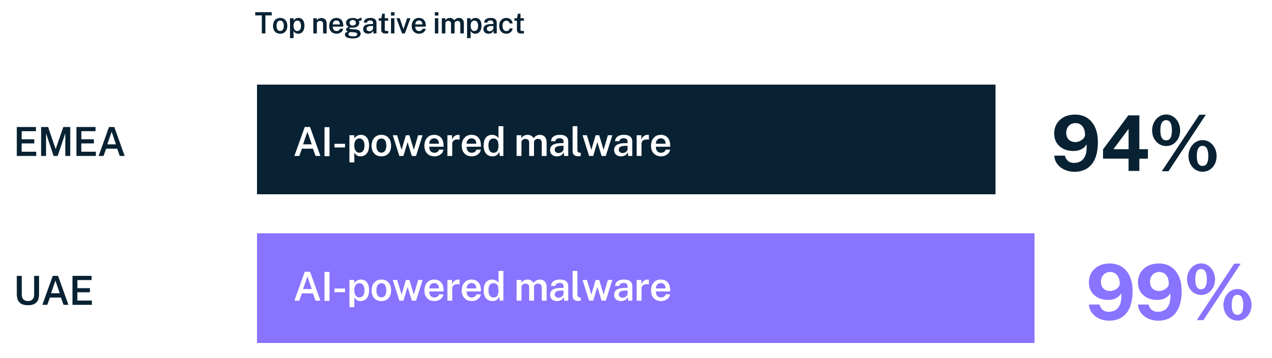
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



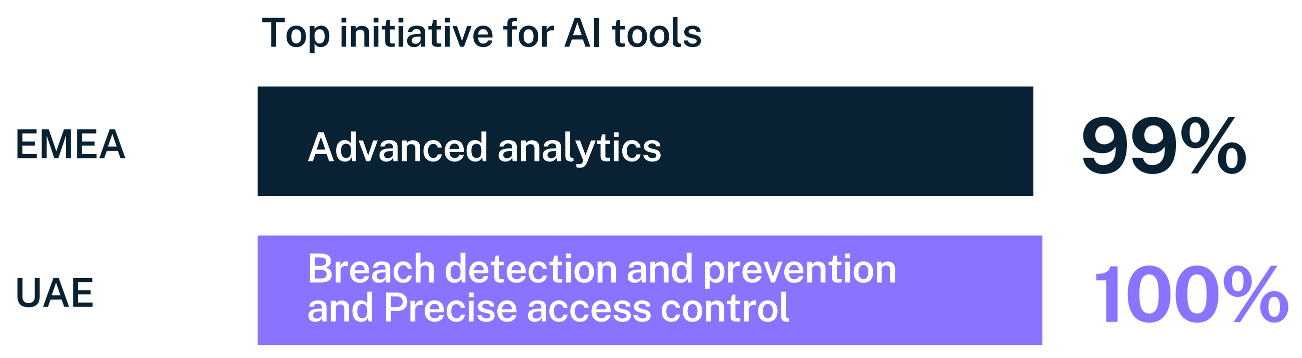
In the UAE, C-level respondents (86%) are confident in their employees' ability to identify deepfakes of their leaders compared to 74% of all other respondents.

Expect negative impact from AI tools in 12 months



C-level respondents in the UAE expect AI-powered malware as top negative impact from AI tools in the next 12 months compared to all other respondents who expect AI-powered data poisoning as the top adversarial effect of AI tools.

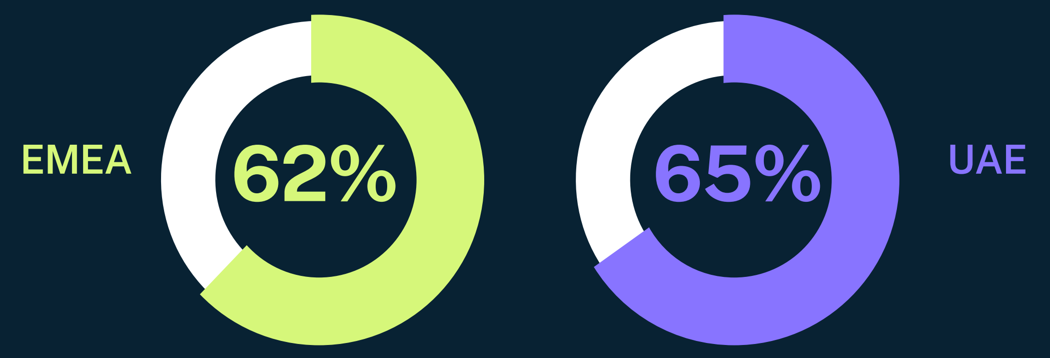
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



UAE respondents indicate that currently they are leveraging AI tools in advanced analytics initiatives and expect to focus on breach detection and prevention as well as precise access control in the next 12 months.

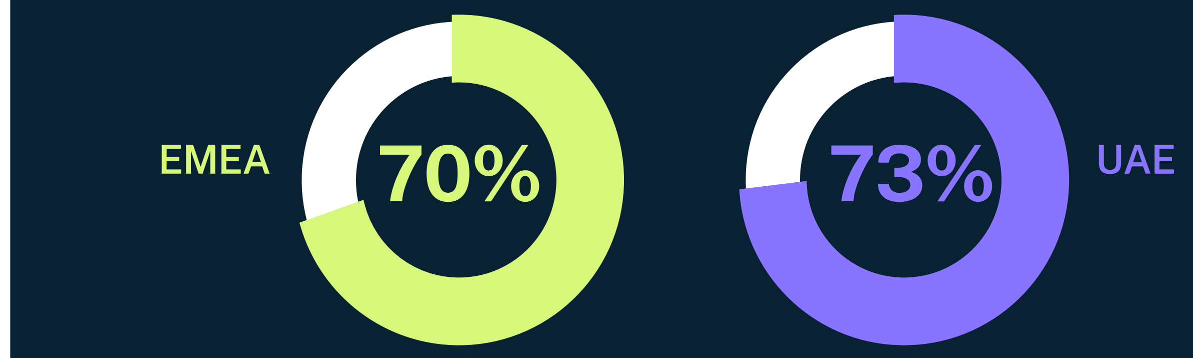
2. New Era: Rise of the Machines

Respondents define 'privileged user' as human-only



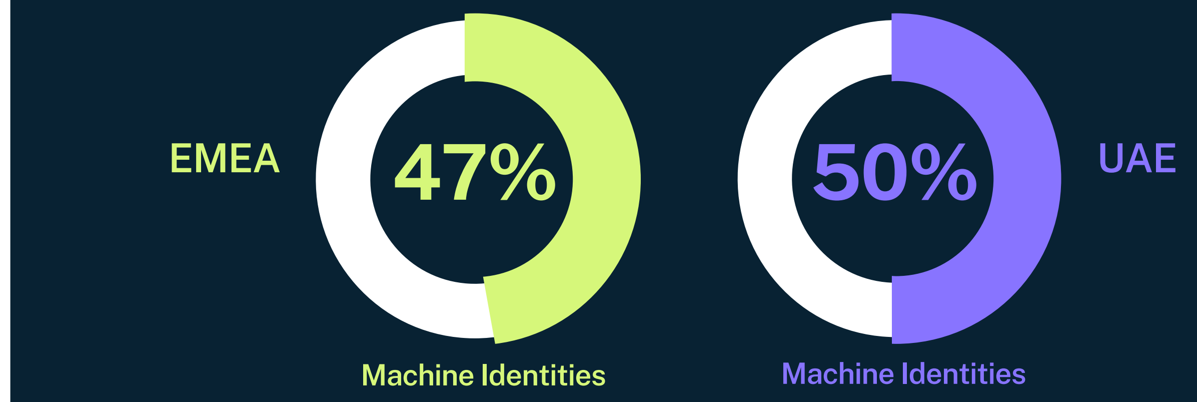
UAE organisations must reevaluate their definition of privileged user as machine identities are driving the overall annual growth of all identities.

Respondents indicate up to 50% of machine identities have access to sensitive data



73% respondents from UAE indicate up to 50% of all identities – human and machine – have access to sensitive data thus supporting the need to reevaluate their definition of a privileged user.

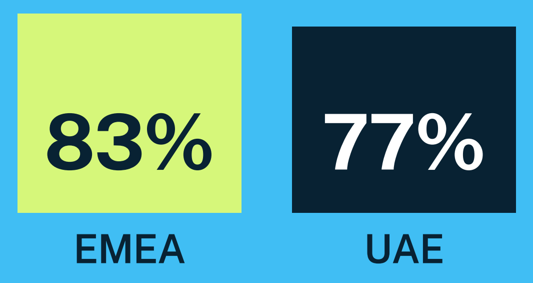
Riskiest identity types



Workload and machine identities is least investment priority in post-breach scenarios in the UAE.

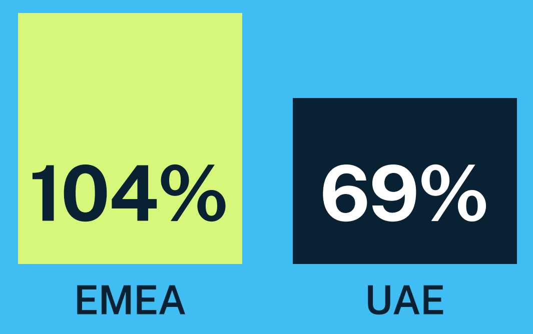
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



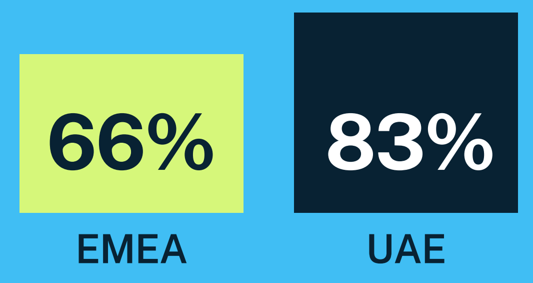
64% of organisations in UAE currently leverage three or more than EMEA (55%). Insights indicate that data/ privacy protection and software vulnerabilities are the top two cloud security concerns in the UAE.

Expected annual growth of SaaS providers in the next 12 months



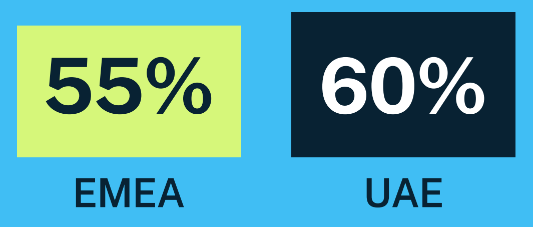
Respondents in the UAE indicate that the growing use of on-premises and SaaS applications is the #2 cause of an identity-related breach.

Are concerned about third-party risks



Over a quarter of UAE's organisations have automated third-party identity management.

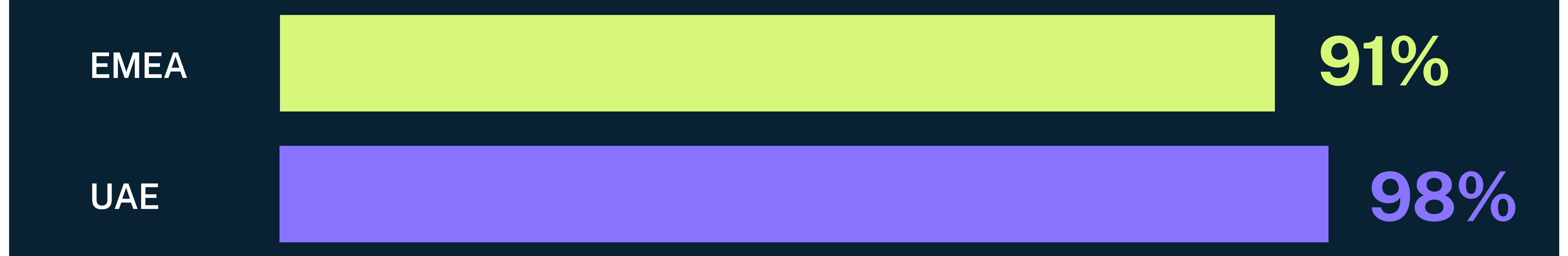
Are concerned about fourth-party risks



A higher number of non-C-level respondents (72%) in the UAE are concerned about risks from fourth-party providers, compared to C-level respondents (44%) indicating a better understanding of potential double supply chain attacks.

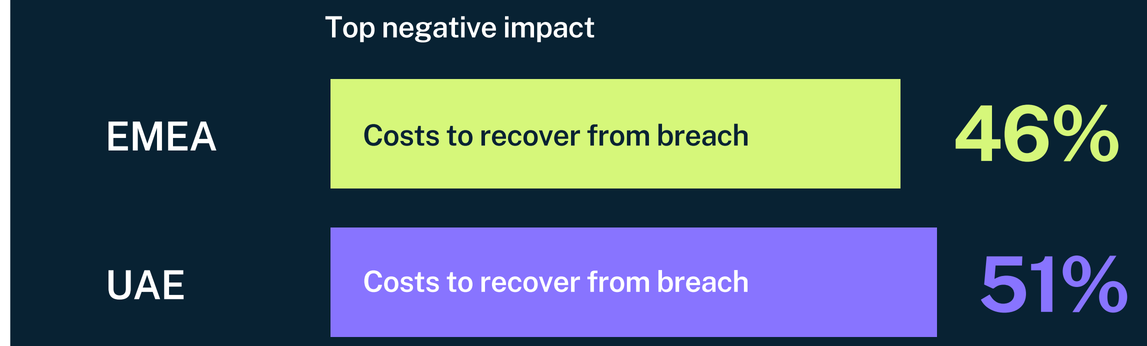
4. Cyber Debt: "Shiny Object" Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



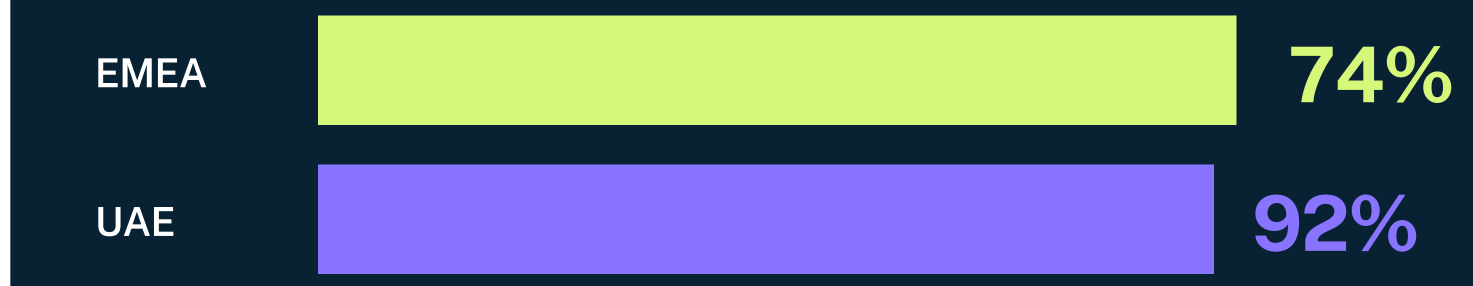
In response to the increasing attacks, 92% of UAE's organisations have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



To reduce risk and cyber debt, 81% of UAE's organisations have cyber insurance policies.

Organisations paid ransom but did not recover data



56% of UAE organisations plan to increase their investments in identity-related products or services by more than 10% in the coming year.

United Kingdom

In this report, we surveyed 150 respondents in United Kingdom, with 61% of United Kingdom respondents indicating their organization had over 1,000 employees. Our respondent base includes 27% C-level executives.

UK follows a similar pattern to EMEA in percentage of organisations that have faced an identity-related attack. We find that in the last 12 months in UK:

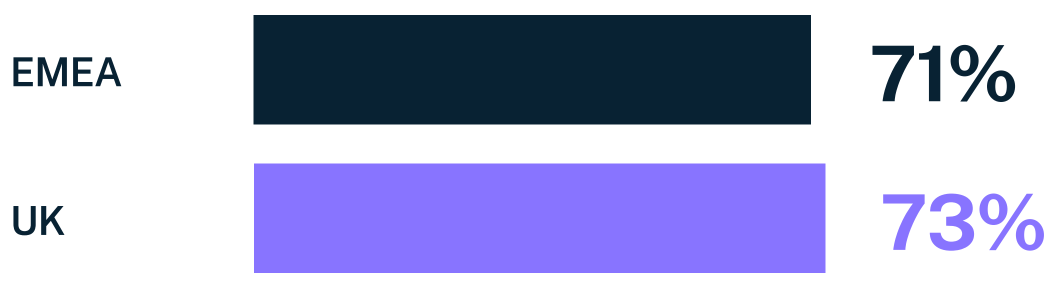
1. 93% faced an identity-related attack at least once compared to 94% in EMEA and
2. 93% faced two or more identity-related attack compared to 94% in EMEA.

UK respondents expect stolen or leaked credentials and a vulnerable IAM infrastructure to cause an identity-related attack in the next 12 months. UK insights report a significantly high annual growth (261%) in the number of SaaS applications, compared to EMEA (104%). Nearly all (95%) of respondents expect negative feedback from AI tools. They (53%) expect AI-powered malware as the primary driver of negative impact from AI tools.

Let's look at how United Kingdom compares to EMEA in the four key areas highlighted in this report.

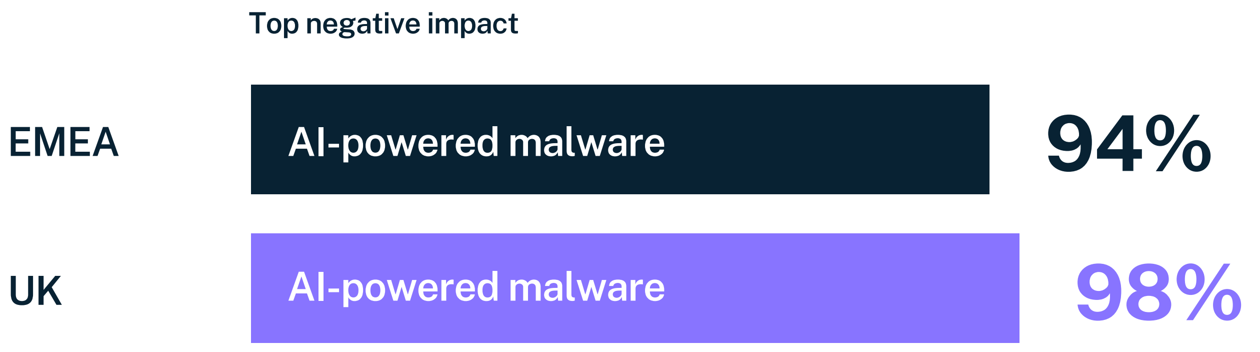
1. GenAI: Promise, Potential – And Peril

Respondents are confident in their employee's ability to identify deepfakes of their leaders



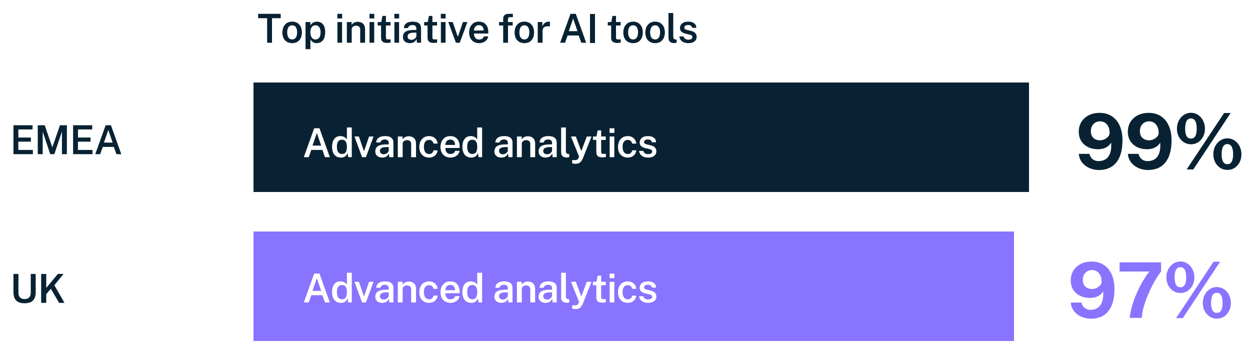
In the UK, C-level respondents (87%) are confident in their employees' ability to identify deepfakes of their leaders compared to 68% of all other respondents.

Expect negative impact from AI tools in 12 months



In the UK, C-level executives expect data leakage from compromised AI models as the top 3 negative impact from AI tools in addition to AI-powered malware and phishing .

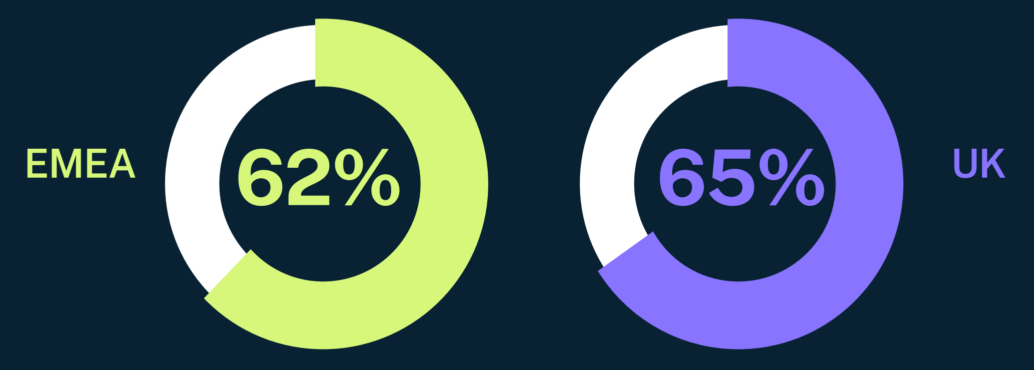
Respondents leveraging AI tools in identity-related cybersecurity initiatives in next 12 months



Currently organisations in the UK are leveraging AI for increased visibility in their identity-related initiatives.

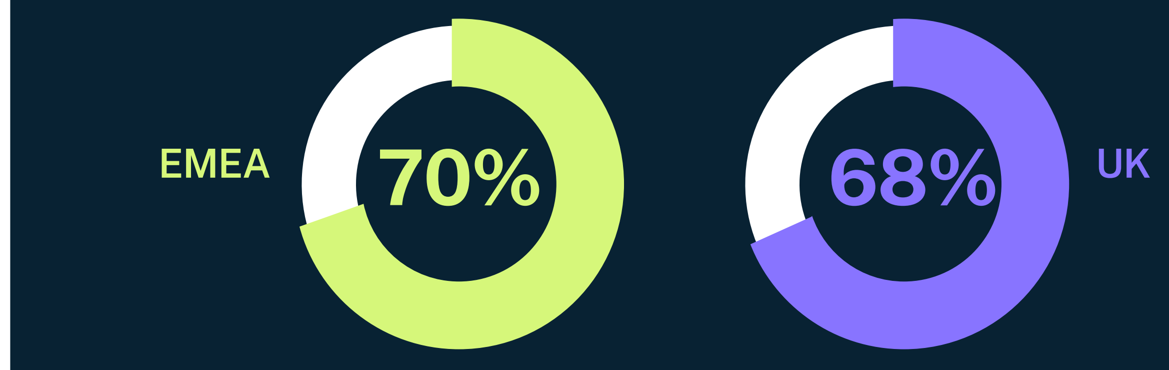
2. New Era: Rise of the Machines

Respondents define 'privileged user' as human-only



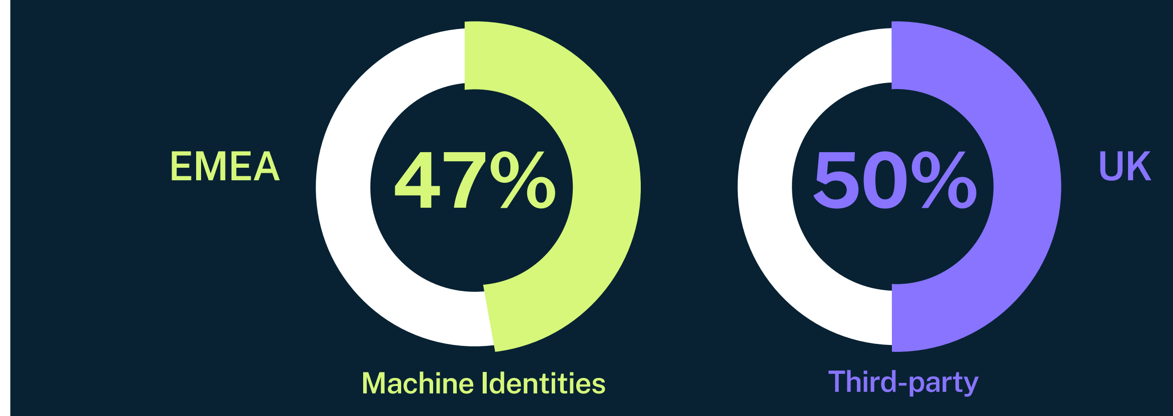
In the UK, 32% of respondents indicated that more than 50% of machine identities have access to sensitive data. These organisations need to reevaluate their definition of 'privileged user' to include machine identities.

Respondents indicate up to 50% of machine identities have access to sensitive data



68% respondents from UK indicate up to 50% of all identities – human and machine - have access to sensitive data thus supporting the need to reevaluate their definition of a privileged user.

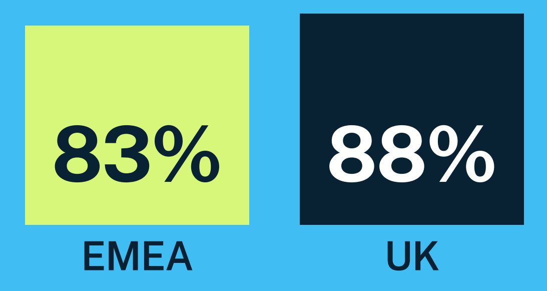
Riskiest identity types



Although respondents in the UK indicate that machine identities are among the top two riskiest identity types, their primary concern is on securing human identities.

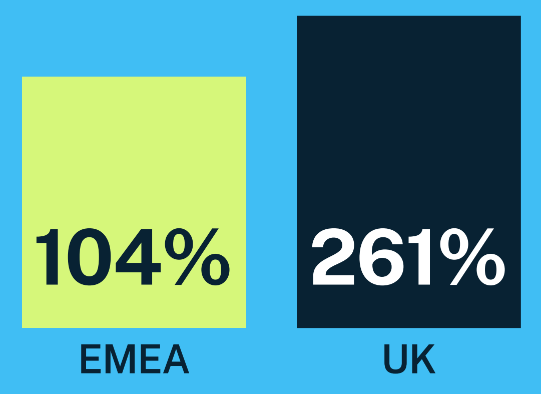
3. Chain Reaction: Third and Fourth-party Risks

Expect to leverage 3 or more CSPs in next 12 months



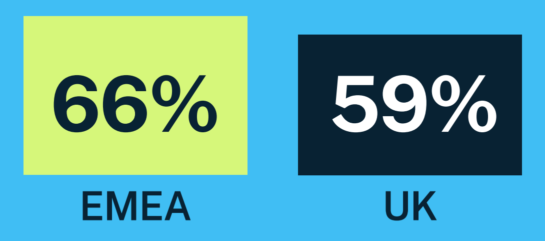
Organisations in the UK anticipate a higher annual growth rate of 3+ CSP adoption (55%) than EMEA (50%).

Expected annual growth of SaaS providers in the next 12 months



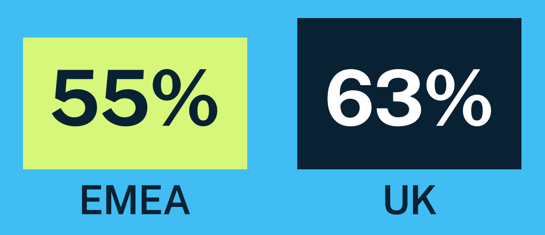
In the next 12 months, UK organisations will use an average of 308 SaaS applications, compared to 179 in EMEA.

Are concerned about third-party risks



In the UK, automating third-party identity management was the top post breach investment areas in the last 12 months.

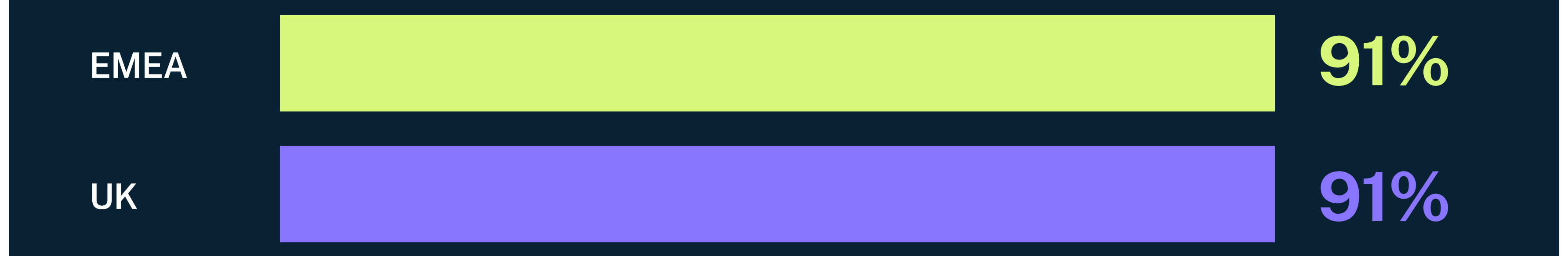
Are concerned about fourth-party risks



A higher percentage of C-level executives in UK organisations are more concerned about fourth-party risks than third-party risks. This indicates a healthy understanding of double supply chain attacks

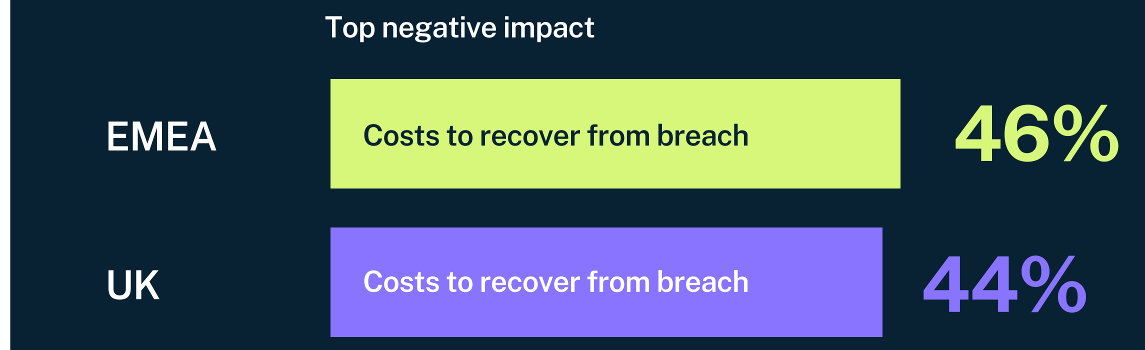
4. Cyber Debt: “Shiny Object” Syndrome and a Blind Spot

Organisations breached due to phishing and vishing attacks



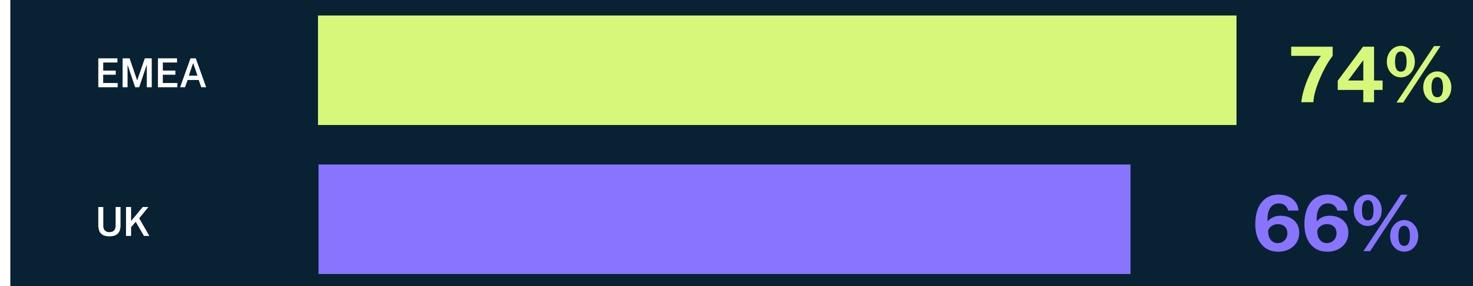
In response to increasing attacks, 89% of UK’s organisations have automated the phishing analysis process.

Organisations faced negative impacts on business results due to breach



More than two-thirds of UK enterprises subscribe to cyber insurance.

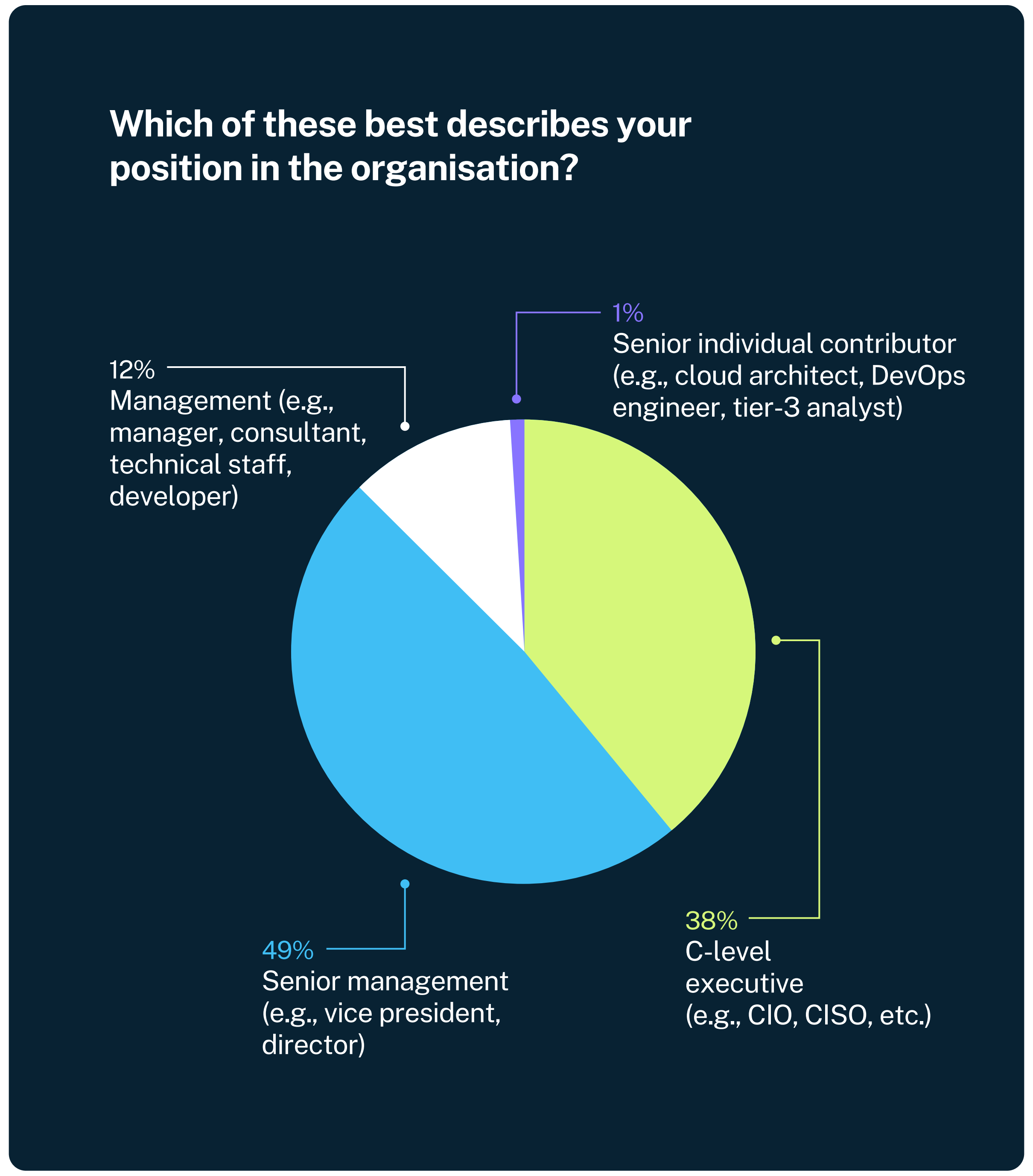
Organisations paid ransom but did not recover data

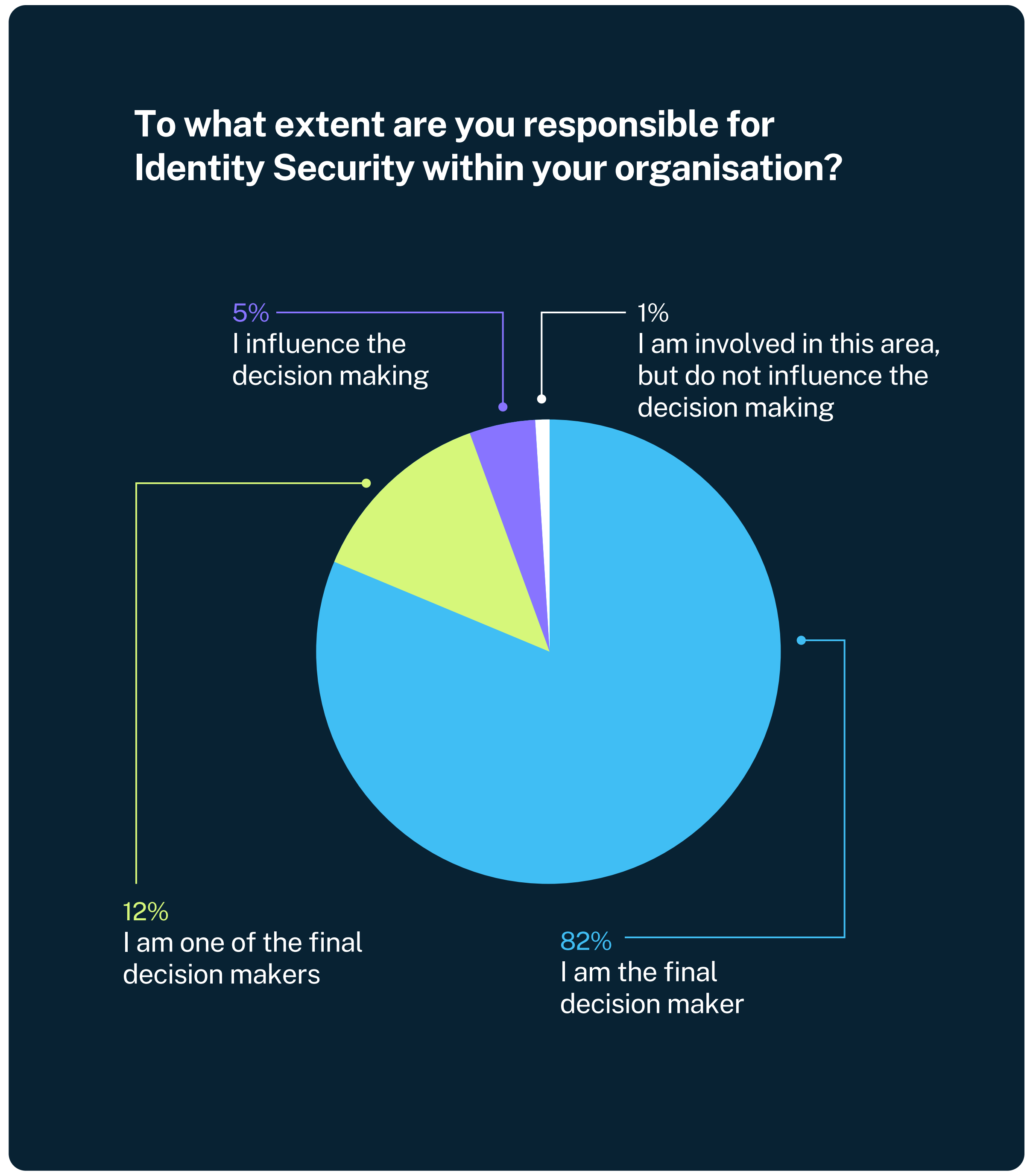


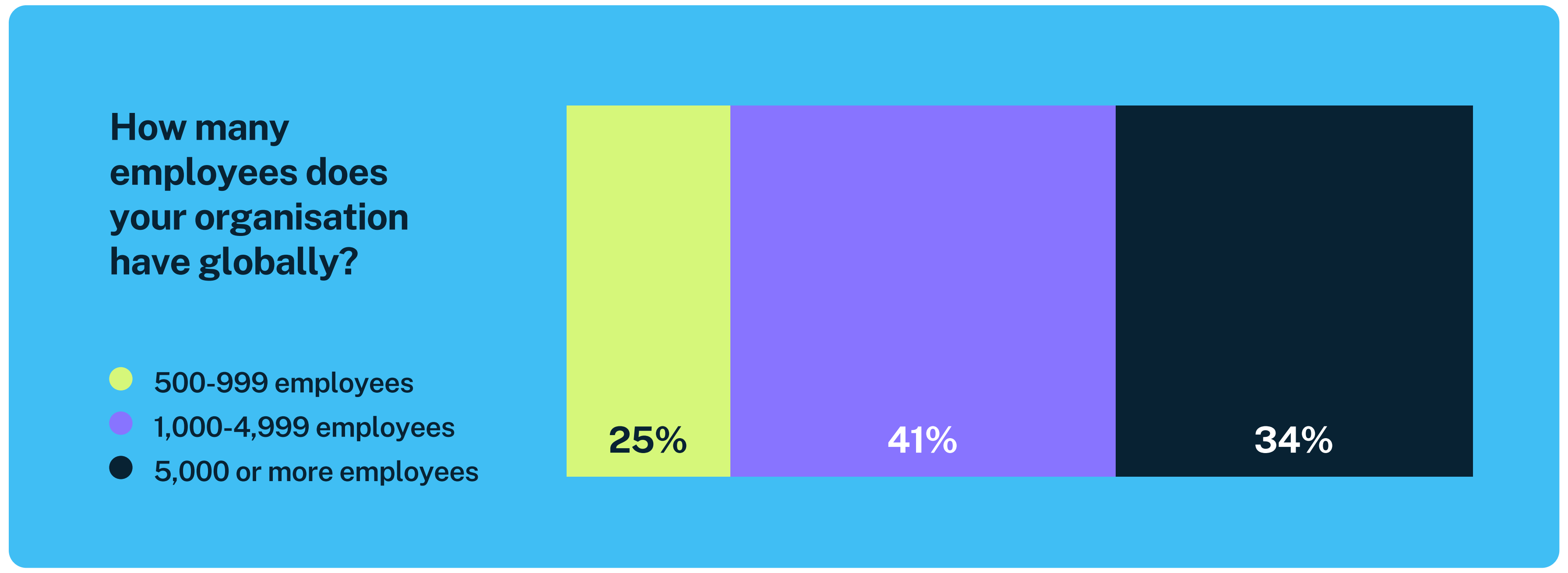
85% of the UK’s organisations plan to increase their investments by more than 10% in the coming year.

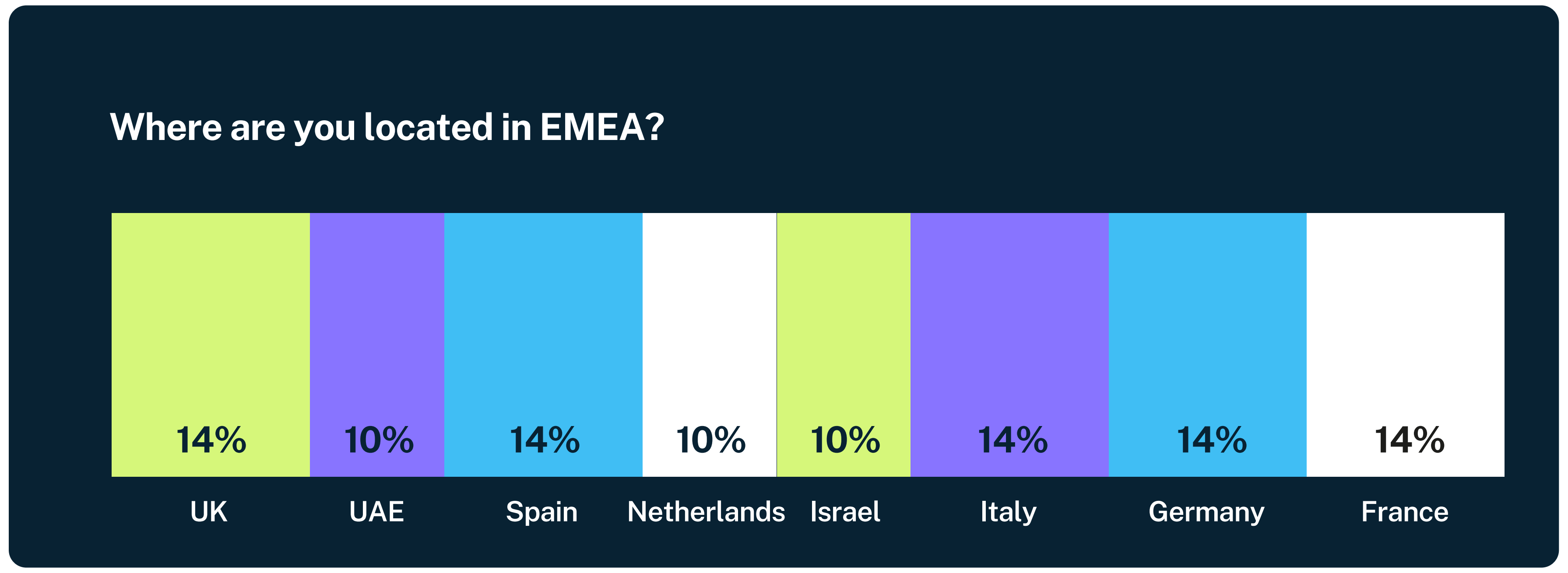
DEMOGRAPHICS

The CyberArk 2024 Identity Security Threat Landscape Report was conducted across private and public sector organisations of 500 employees or more. It was conducted by B2B technology research partner Vanson Bourne amongst 1,050 cybersecurity decision-makers. Respondents were based in France, Germany, Italy, the Netherlands, Spain, the UK, UAE and Israel.









CYBERARK®

SECURITY MATTERS

Read the global research report for additional insights into the key findings.

Learn More

About CyberArk
CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organisations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S.