CYBERARK®

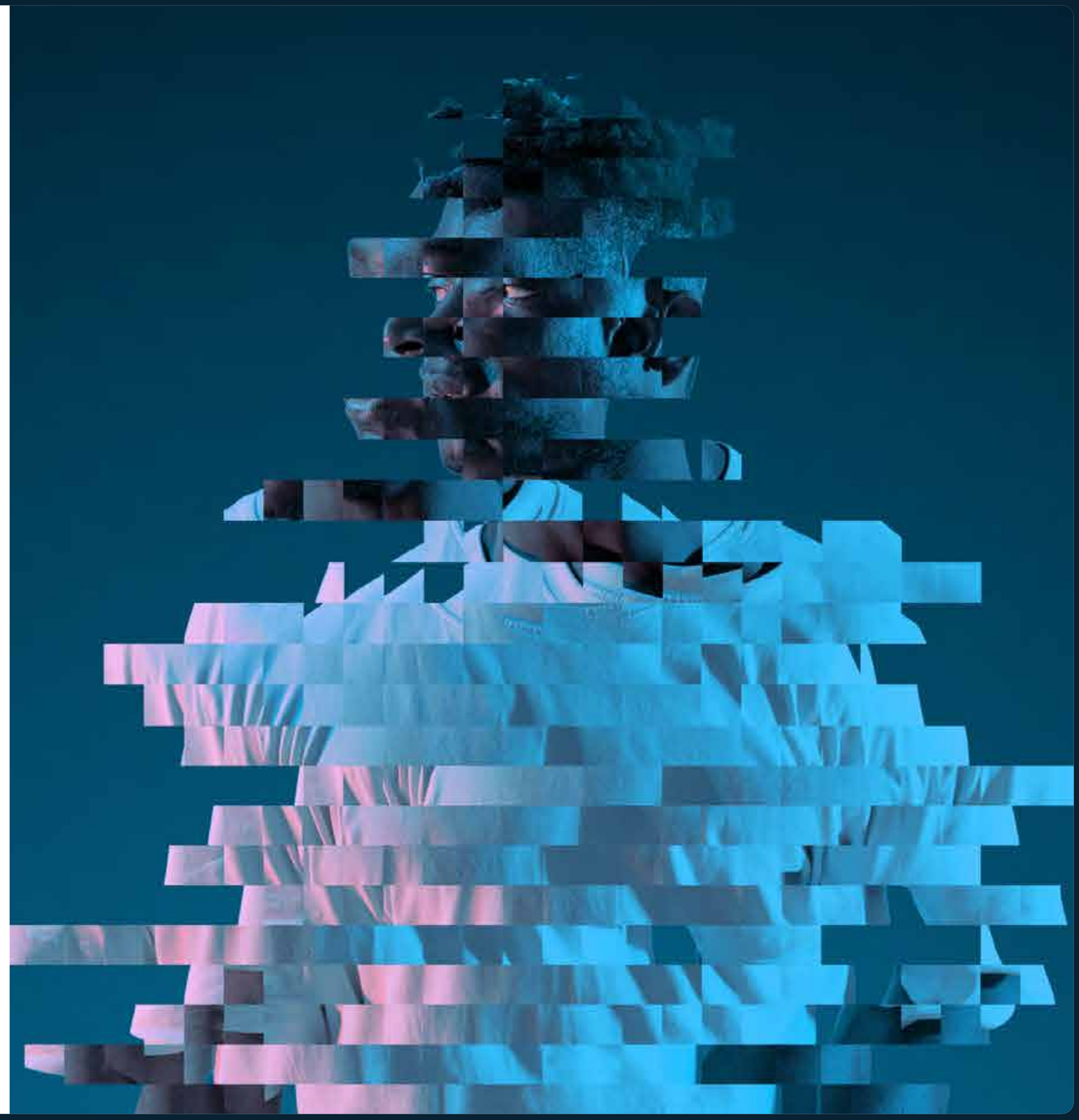
SECURITY MATTERS

Identity Security

Threat Landscape 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 Report is a global survey of 2,400 security decision-makers across 18 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 organizations 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 ongoing AI transformation and pervasive cloud computing, 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 organizations (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 organizations.

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

In the last 12 months, 93% of organizations suffered two or more identity-related breaches. And, with 94% of our respondents using more than 10 vendors for identity-related cybersecurity initiatives, organizations 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 IT environment. 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.

93%

experienced two or more identity-related breaches.

NEW IDENTITIES

47%

Nearly 50% expect identities to grow 3x in the next 12 months (the average is 2.4x).

61%

61% of organizations define a privileged user as human-only.

#1

Machine identities are the #1 driver of identity growth

#1

Machine identities are the riskiest identity types

NEW ENVIRONMENTS

84%

In the next 12 months, 84% of organizations will use three or more CSPs.

89%

The number of SaaS applications will grow by 89%.

91%

are concerned about third-party risks.

82%

are concerned about fourth-party risks.

NEW ATTACK METHODS

89%

were targeted by ransomware at least once.

75%

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

99%

have adopted AI-powered tools.

93%

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 out of 10 organizations 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.

64%

of organizations have or will prioritize ITDR.

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). Much like our 2023 findings, nearly all of our 2024 respondents (99%) are leveraging GenAI in their identity-related cybersecurity initiatives. Unfortunately, so are the bad guys.

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. In the last 12 months, 9 of 10 organizations 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, organizations can expect to be affected by data leakage from compromised AI models, AI-powered malware, and phishing. And, with GenAI, even previously unaffected organizations will find themselves in the crosshairs — and will have to do damage control.

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 organizations are confident that their employees can identify B2B deepfake videos. More on that in a moment.

93% 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:

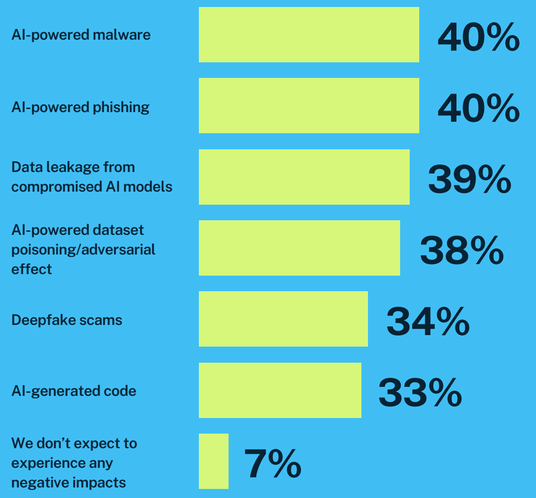
1. Digital transformation (22%)
2. Vulnerable IAM infrastructure (21%)
3. Volume & sophistication of cyberattacks (20%)

Although we can all agree that GenAI is still in its infancy, it should not be a surprise if this technology powers the world's most sophisticated at-scale attacks. In fact, researchers at CyberArk Labs were one of the first in the market to sound the alarm that GenAI could create highly evasive malware capable of slipping undetected past most anti-malware security products.

Get ready for a pivotal and unsettling Decision 2024 as over 4 billion voters prepare to elect leaders in over 60 countries — and AI-powered deepfake campaigns become the weapon of choice for anyone wanting to influence election outcomes.

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

What we learned:
93% of organizations expect AI-related cybersecurity challenges, with malware and phishing topping the list.

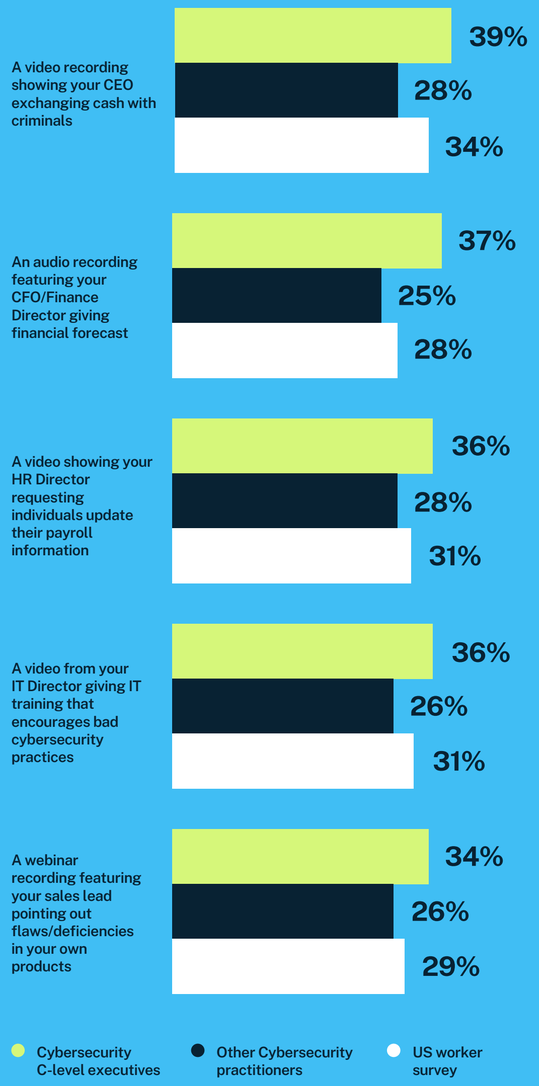


What we asked:

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 (nearly 75%) of executives are **completely confident** that employees can spot deepfakes of their leaders.



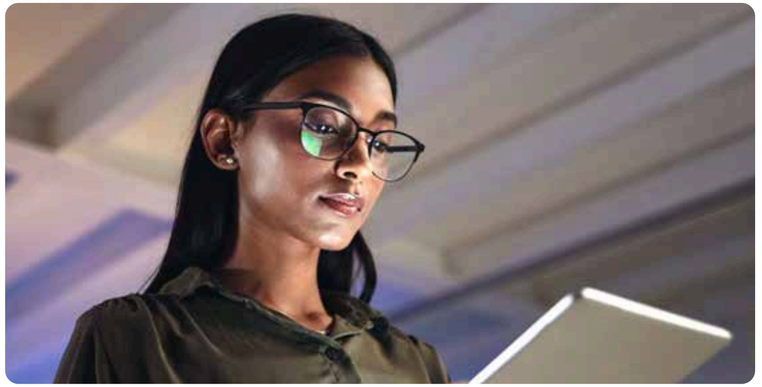
Get ready for a pivotal and unsettling Decision 2024 as over 4 billion voters prepare to elect leaders in over 60 countries — and AI-powered deepfake campaigns become the weapon of choice for anyone wanting to influence election outcomes.

"Don't worry, it's me: President Biden."

In January 2024, several New Hampshire-based voters in the United States received a robocall seemingly from President Joe Biden urging them not to vote in the primary elections. Officials were able to identify and stop this social engineering tactic from having a material impact on the primary elections. However, we can safely assume that not every case will be this lucky. Individual voters are small fry compared to the big bounty nefarious actors can score in B2B environments. In February, a Hong Kong-based multinational company lost HK $200 million (US $25.6 million) to a deepfake scam that fooled a clerk into executing a financial transaction discussed during a virtual meeting where every attendee — even the chief financial officer (CFO) — was fake. Unfortunately, this first-of-its-kind AI heist (and worst day ever for an employee) will not be the last. AI-powered phishing attacks will soon target and potentially breach 100% of organizations.

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

We know that AI-driven phishing and deepfake scams are already working. Our research further tells us we will see a steep rise in GenAI-powered cyberattacks. So why do over 75% of respondents say they're confident their employees can identify deepfake videos or audio of their leaders?

Our persona-level insights paint an interesting picture. We find that C-level executives are entirely confident that their employees can identify these deepfakes compared to other cybersecurity leaders and practitioners surveyed in this report.

Because the impact of deepfakes is both imminent and unquantified, we decided to pose the same question to over 4,000 US-based employees in our 2024 US Office Worker Survey. We found a similar pattern: employees are largely confident in their ability to identify a deepfake video or audio of the leaders in their organization.

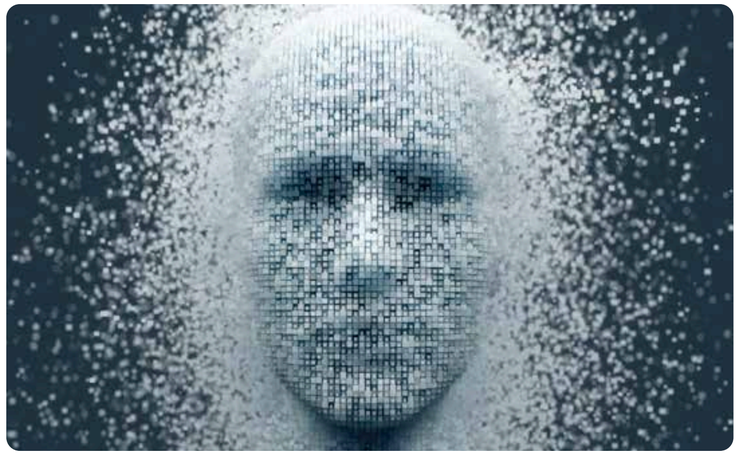
Whether we chalk it up to the illusion of control, planning fallacy, or just plain human optimism, this level of systemic confidence is misguided. The full destructive potential of GenAI remains unknown, and we may not quite grasp how vulnerable we are.

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. The message is clear: the responsibility for the safe usage of AI-powered tools lays 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.

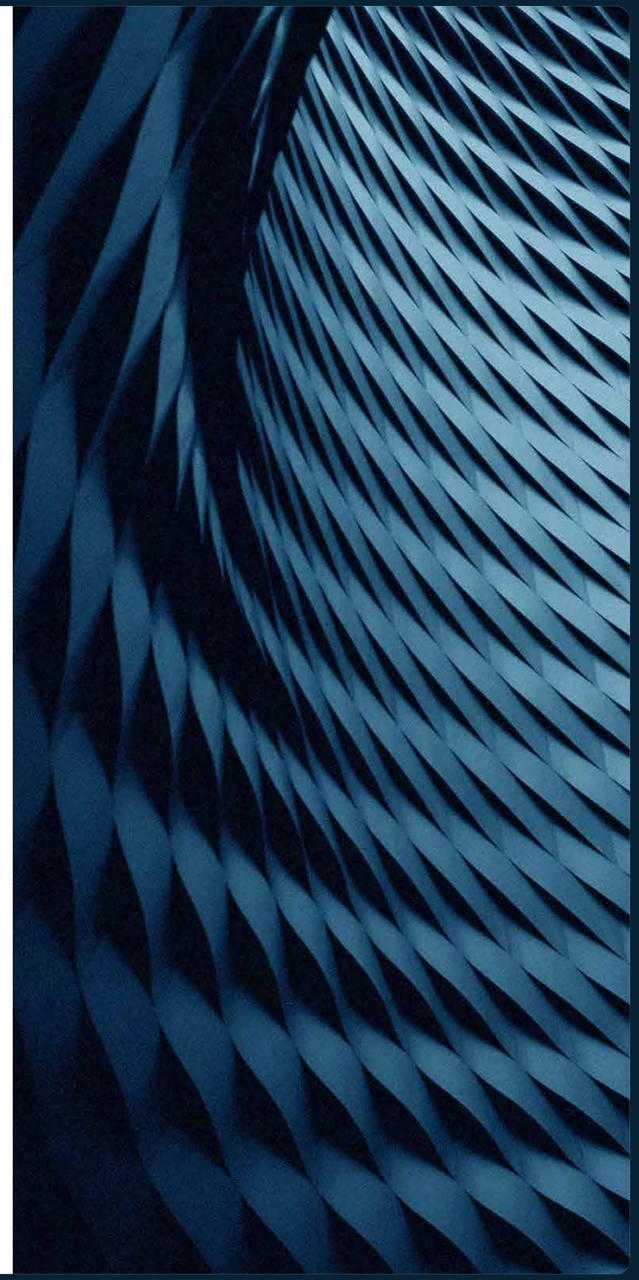
Our advice: Discuss this perception gap with stakeholders in your organization and identify why it might exist. Only when executives and cybersecurity teams are aligned can there be a path to resolution.

With 99% of organizations 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

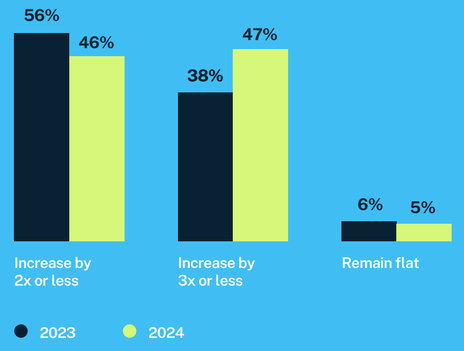
New Era: Rise of the Machines

By now, organizations 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 - making them the most dangerous identities of all.

Over the next 12 months, we predict the number of identities to more than double (2.4x), following the same pattern we saw in 2023. However, nearly half of this year's 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 organization to increase?

What we learned:
Nearly 50% expect the total number to grow by 3x or more.

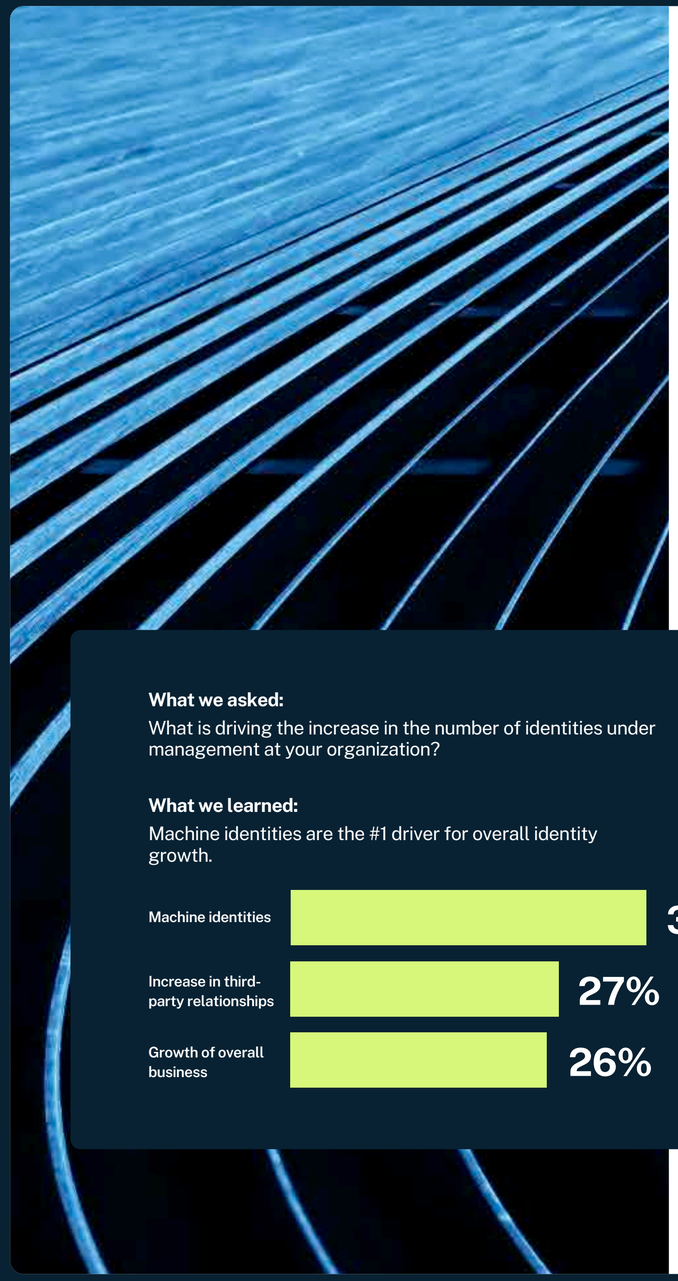


Sci-Fi: Don't Overlook the Machines

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

In 61% of organizations, 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 organizations 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. Humans are only one corner of a million-piece puzzle. Afterall, it won't be long before chatbots or virtual assistants will be phished.



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

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

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, organizations report that their next biggest concern is a machine identity-related security incident that would require significant manual effort to address or remediate.

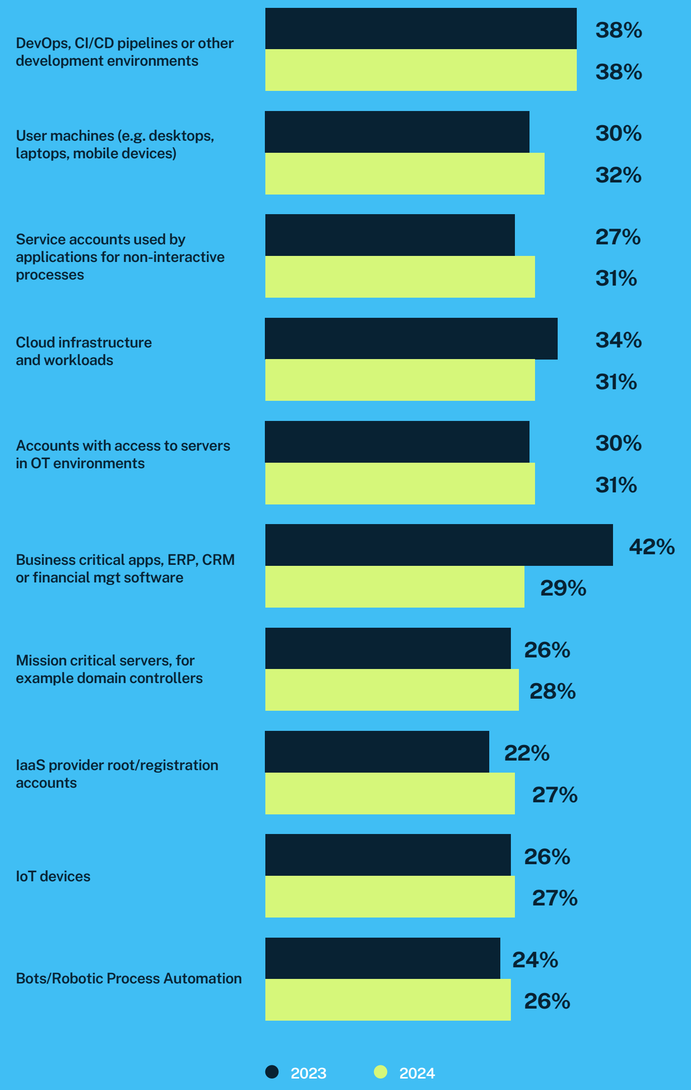
Manage Your Non-Humans Here

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:
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.

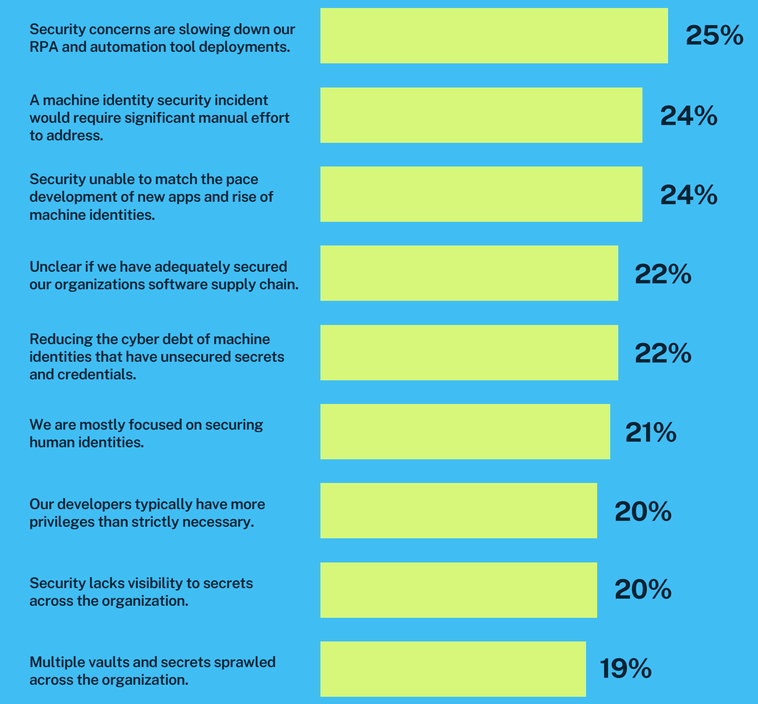
If you lack visibility of secrets within your environment, consider eliminating (or at last reducing) multiple vaults and secrets sprawl.

What we asked:

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

What we learned:

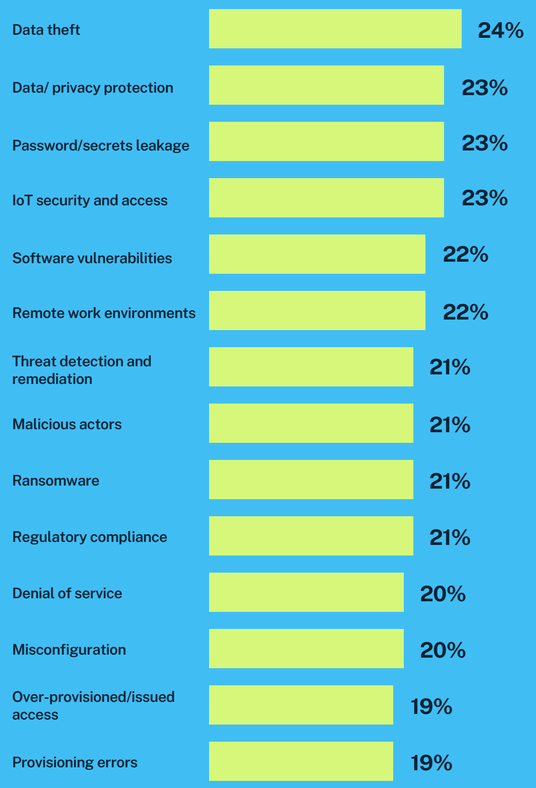
Security concerns are slowing down automation. Also, the threat of a machine identity-related security incidents could cause significant manual effort to remediate.



Chain Reaction: Third- and Fourth-party Risks

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

What we learned:
All organizations have cloud security concerns.



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?

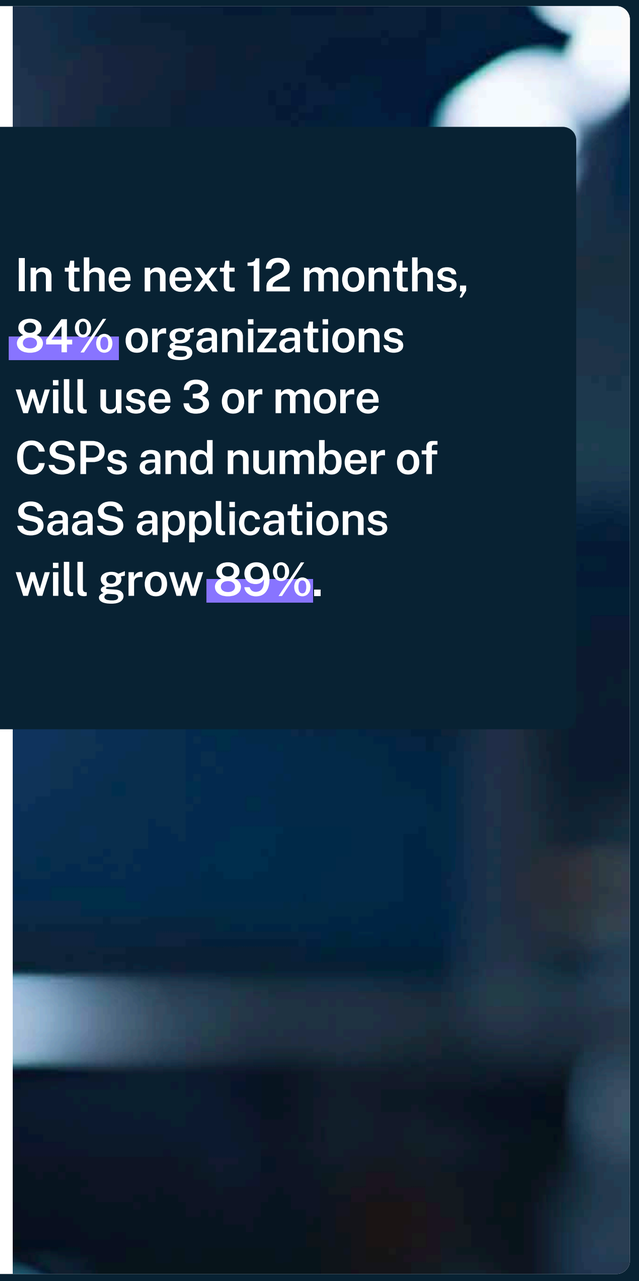
You've heard about third-party providers (product or service companies your organization engages with directly). Fourth parties contract with your third parties and typically provide products or services to support your organization's digital business. Unfortunately, a compromise on one party leads to 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 organizations 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, 84% organizations will use 3 or more CSPs and number of SaaS applications will grow 89%.



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 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 (24%)
2. Data/privacy protection (23%)
3. Password/secret leakage (23%)
4. IoT security and access (23%)
5. Software vulnerabilities (22%)

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.

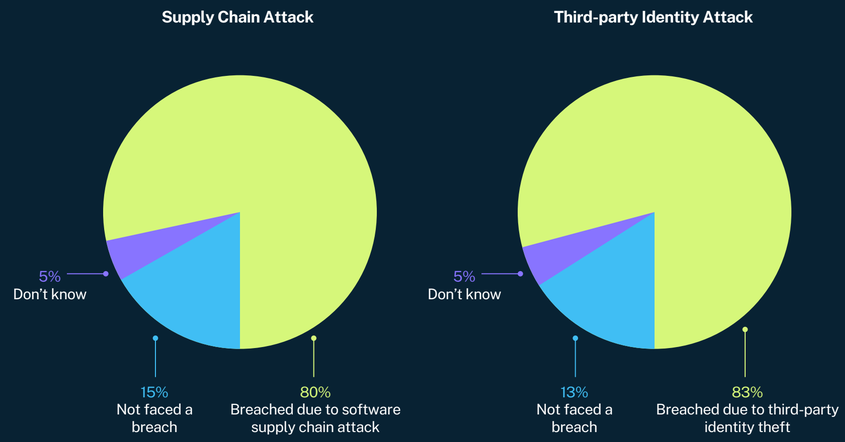
80% of organizations experienced an identity-related breach due to a software supply chain attack.

What we asked:

How often has your organization faced a successful identity-related breach due to a software supply chain attack in the last 12 months?

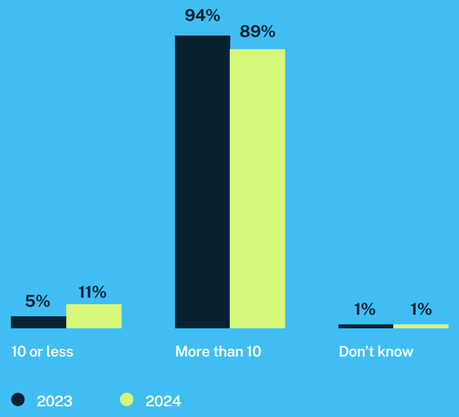
What we learned:

Majority of organizations have suffered from a supply chain attack and third-party identity theft.



What we asked:
On average, how many identity-related vendors has your organization onboarded to date?

What we learned:
Organizations 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 80% of organizations experienced an identity-related breach due to a supply chain attack, and 57% of these breached organizations 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, 26% of respondents chose "lack of visibility across multiple identity-related point tools, products and services" as the top two truest statements for their organizations. 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 organizations 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:

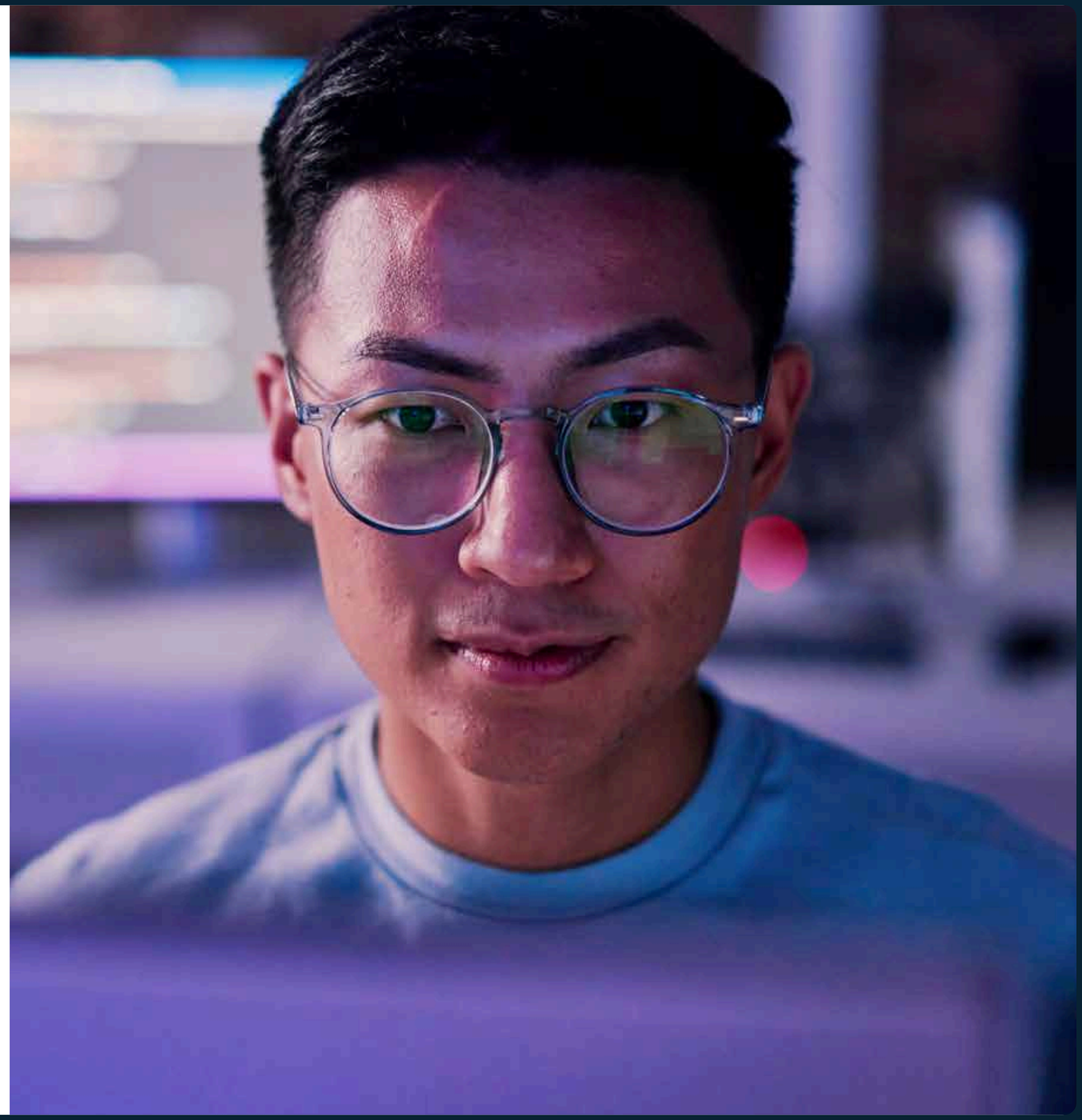
1. **Audit and evaluate** all legacy and new technologies across your environment.
2. **Assess the risks** of these disparate tools address vs. the time and effort required to maintain them.
3. **Create a plan** to consolidate your technology stack based on the right balance for your organization. Do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

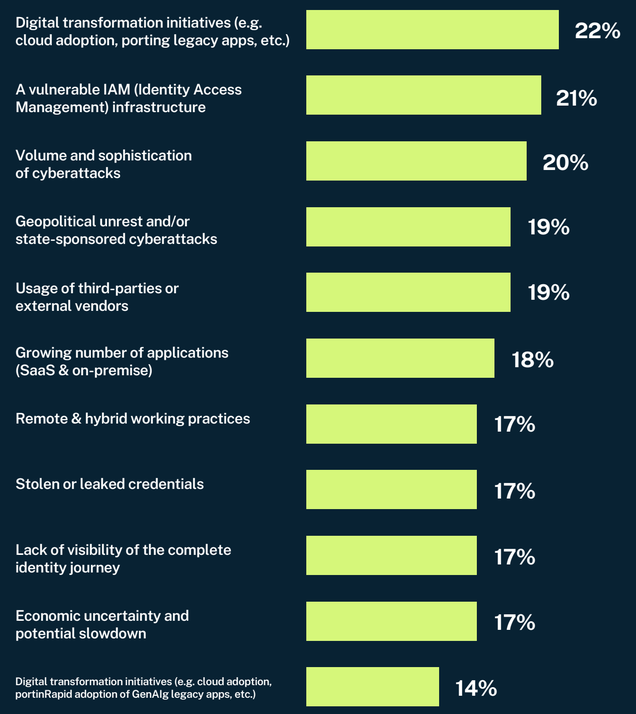
The More Things Change, the More They Stay Insane

Digital transformation continues to be the top cause of identity-related attacks. Breaches due to phishing and vishing attacks have impacted 9 of 10 organizations. Nearly the same number of organizations were targeted by ransomware in 2024 (90%) as compared to 2023 (89%) with a higher number of organizations reporting damage (irretrievable loss of data).

90% were targeted by ransomware and 75% 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 organization?

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 64% of organizations report up to 50% of human identities have access to sensitive data, compared to 75% in 2023.

In our 2024 survey, 36% of respondents believe that more than half of their human identities have access to sensitive data. That’s up 11% 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 Attack 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:

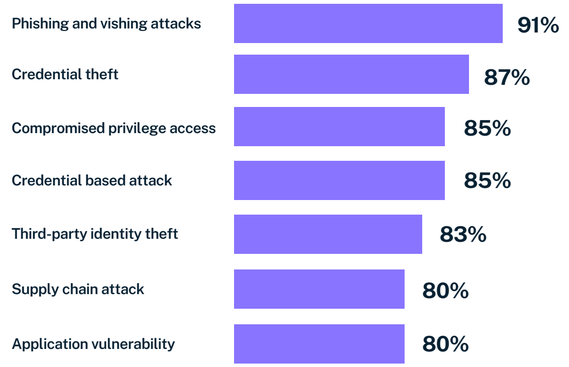
1. Phishing and vishing happen when a user is contacted by email, telephone or text message by someone posing as a close personal contact or on behalf of a legitimate institution. Ransomware is a common example of phishing and vishing attacks.
2. Credential theft is a type of cybercrime that involves 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:

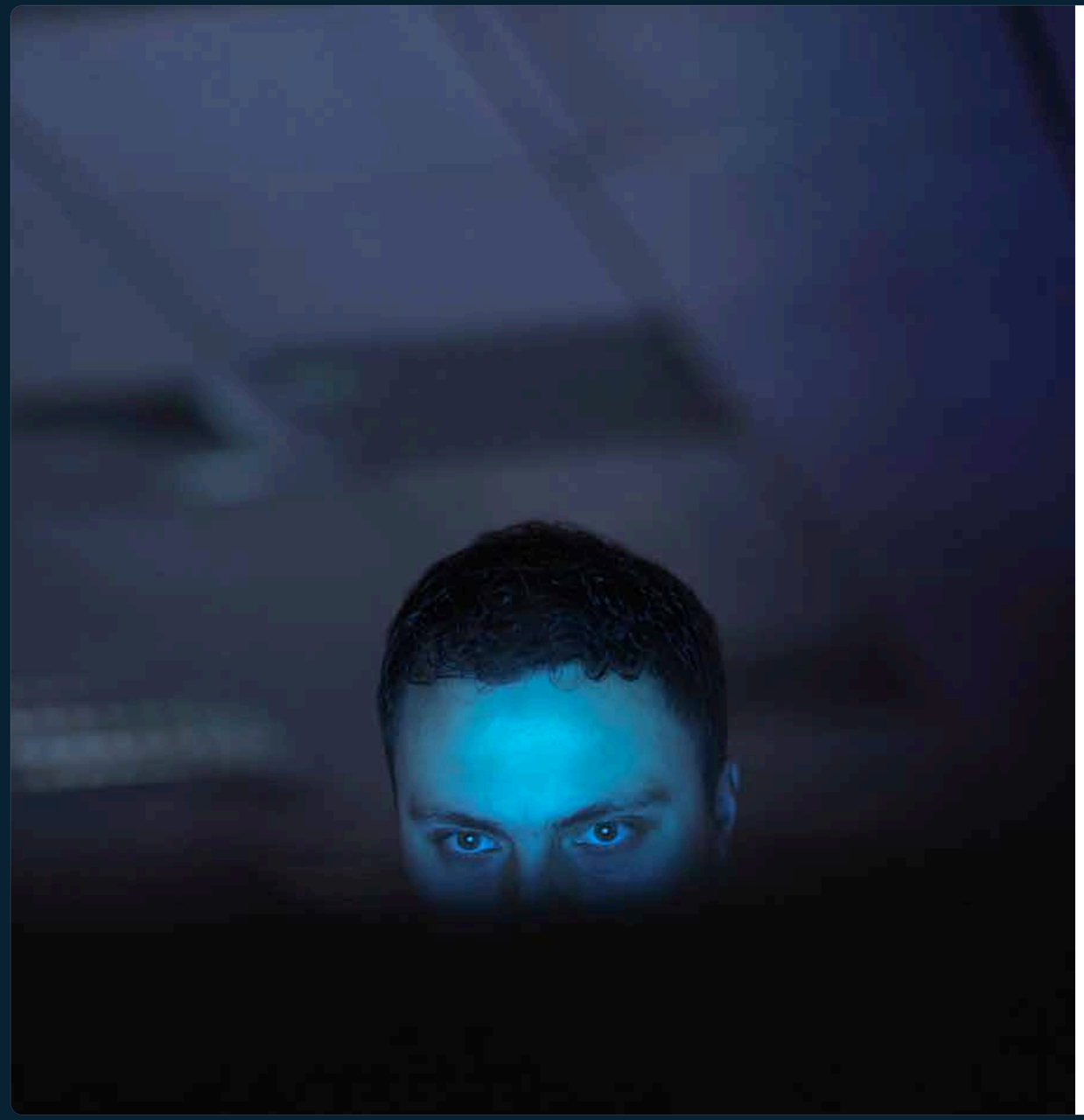
How often has your organization faced a successful identity-related breach in the last 12 months?

What we learned:

Phishing and vishing attacks impacted 9 out of 10 organizations 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. Organizations 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 organizations 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 organizations in the financial, healthcare and life sciences sectors have a significantly higher rate of this twofold injury: paying ransom without recovering data.

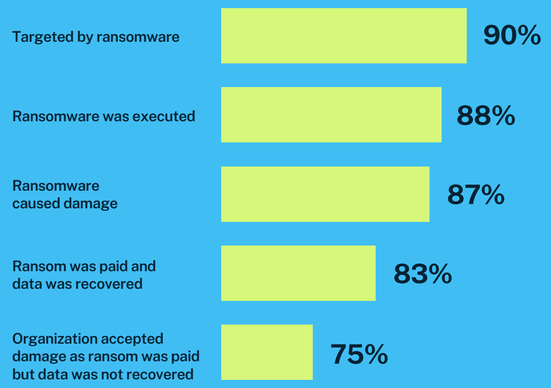
Any Breach Is a Bad Breach

Nearly all (99%) of organizations 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 4% of organizations 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 organization 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.



We know. It's not an easy choice.

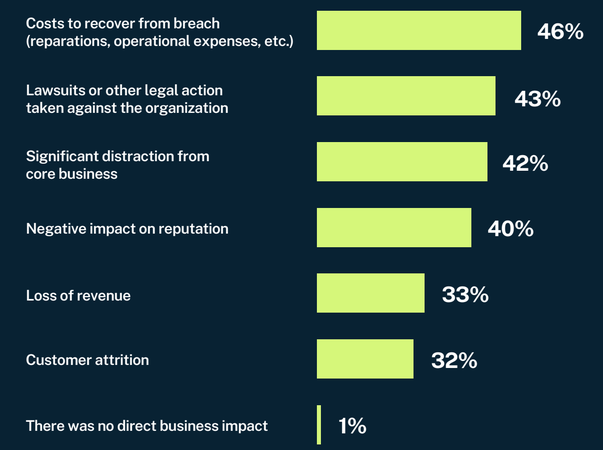
This takes us back to the lessons learned in the risky third- and fourth-party sections of this report. Organizations are concerned with these vendor risks, but the only thing they can do (which most report they don't) is increase investments and the frequency of vendor risk assessment.

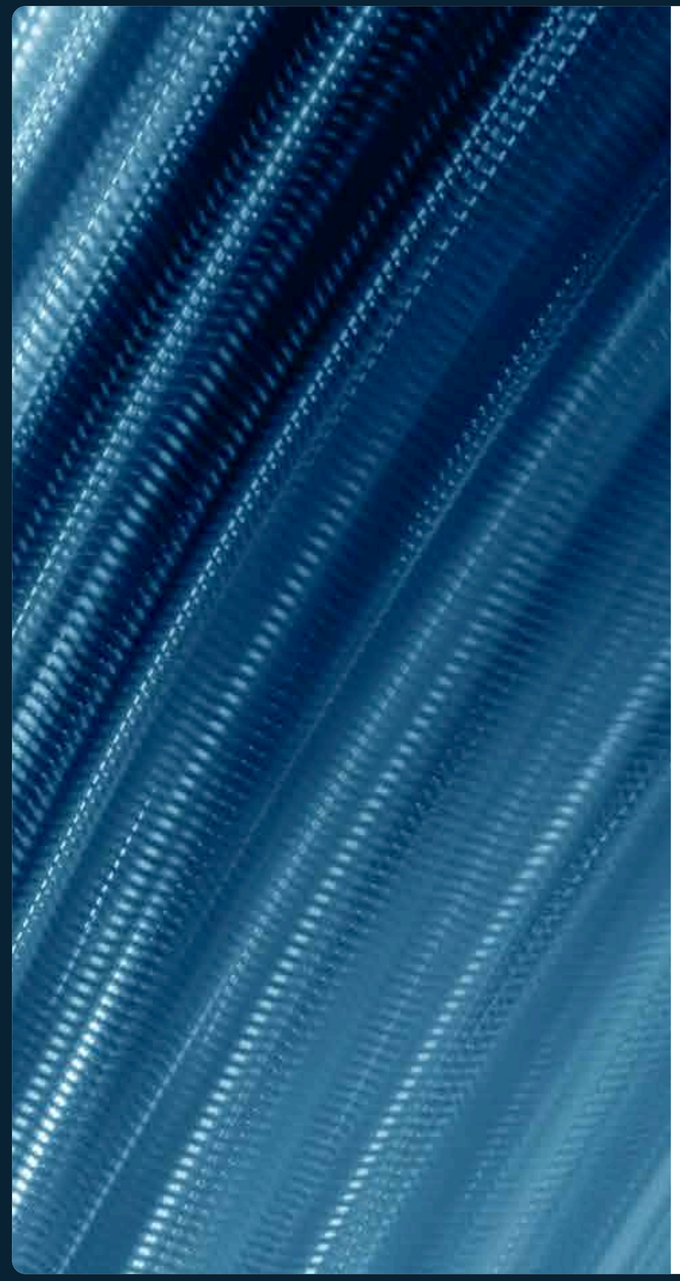
CyberArk Insights

In its 2024 Global Risks Report, 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 organization suffer any direct impact to business results due to the breaches in the last 12 months?

What we learned:
Nearly all organizations who were breached faced negative impact on their business





What This Means for You

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.

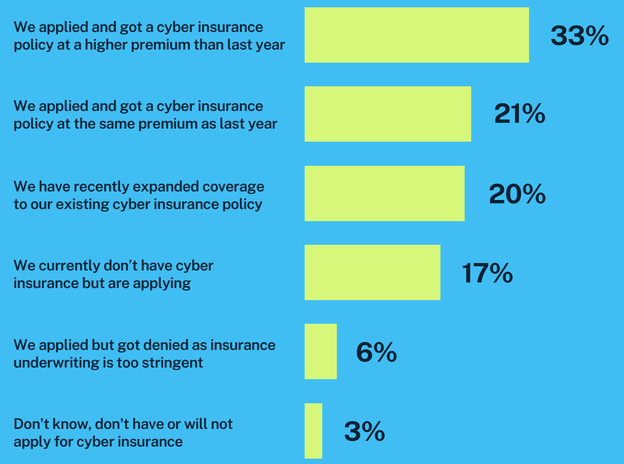
1. WEF_The_Global_Risks_Report_2024.pdf (weforum.org)

What we asked:

Which of the following statements related to cyber insurance is true for your organization??

What we learned:

One-fifth of organizations 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. Organizations are evolving their cybersecurity strategies with new capabilities and task automation. Identity security organizations 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% — organizations indicated that they will prioritize new tools or technologies in the next 12 months. Topping that list: ITDR. This emerging security discipline will help organizations 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 organizations 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.

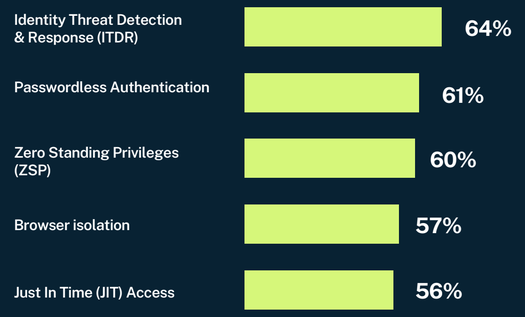
Automation executes predefined tasks and reduces manual intervention. AI, on the other hand, incorporates machine learning from large datasets to ultimately make decisions without explicit programming. As your organization steers from automation towards rapid AI-powered decision-making, the key is to 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.

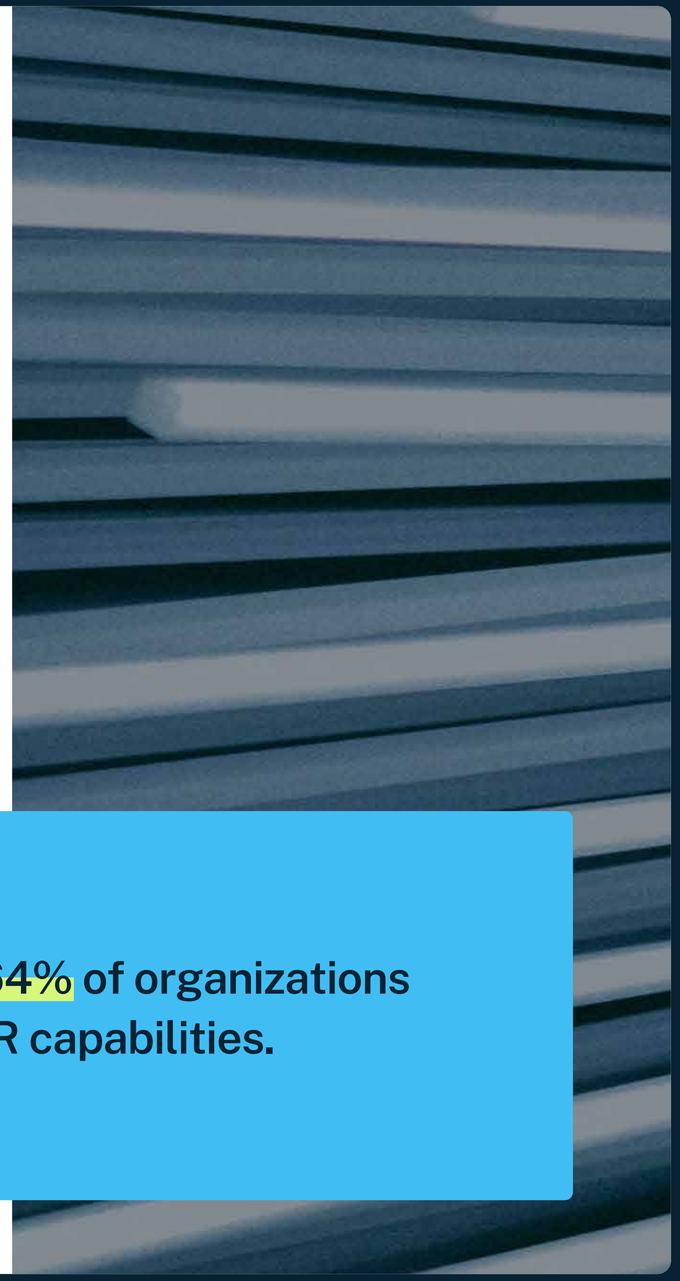
What we asked:

How has, or will, your organization 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.

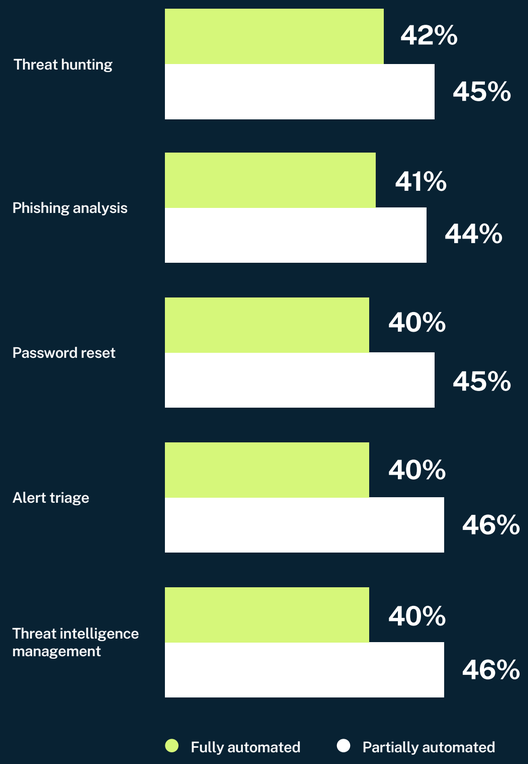




For the next 12 months, 64% of organizations have or will prioritize ITDR capabilities.

What we asked:
To what extent are the following cybersecurity processes/use cases automated in your organization?

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

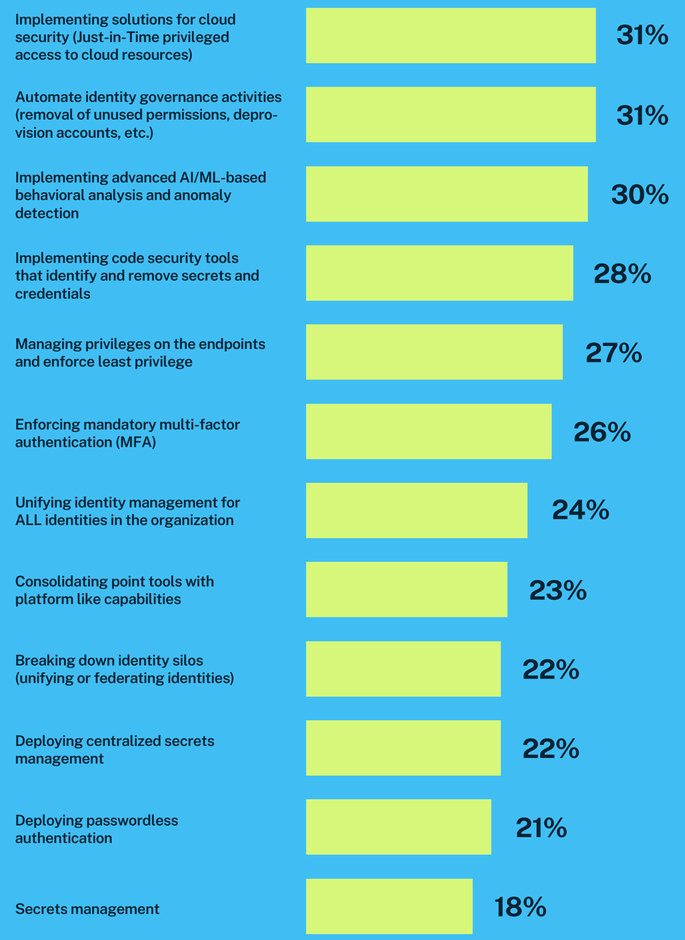
Apart from the need for endpoint security, federated identity, cloud infrastructure entitlements manager (CIEM) and multi-factor authentication (MFA), we'd like to draw your attention to the smartest bets for your post-breach investments.

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 organization 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.

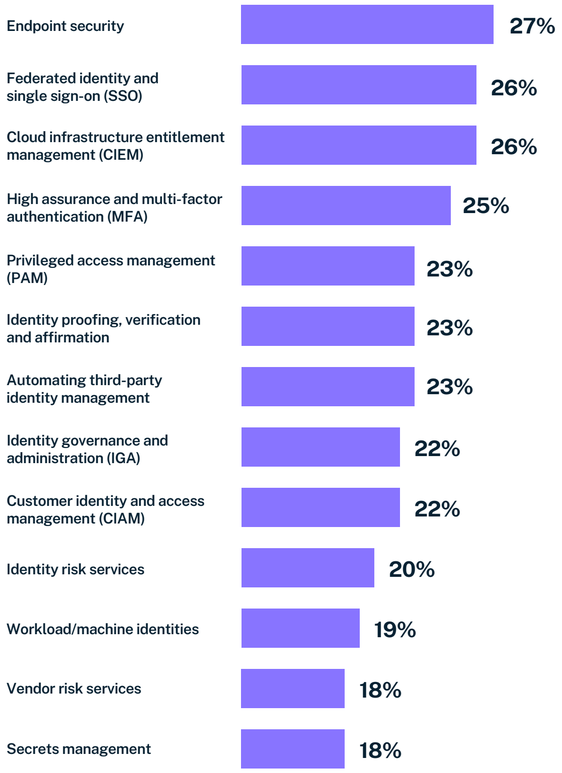


What we asked:

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

What we learned:

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 nonnegotiable 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.

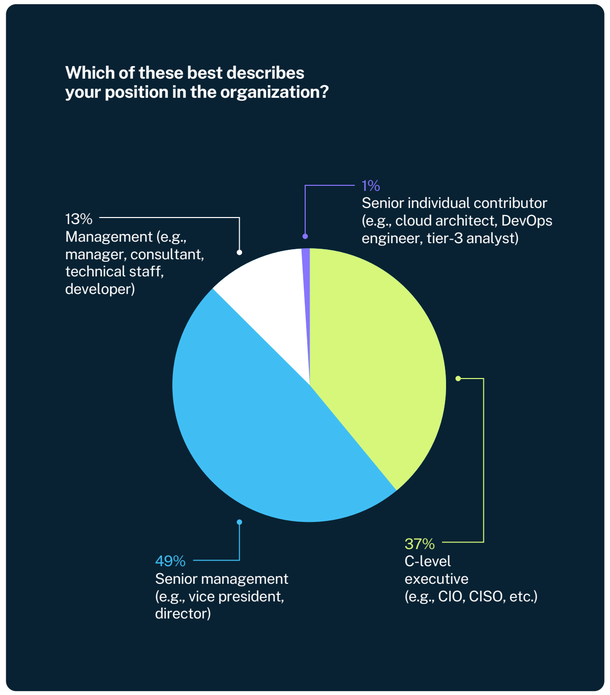
You are undoubtedly in a fast-paced world with a long list of daily Sisyphean challenges. Every defense you put up becomes a game that bad actors love to win. And it only takes one misstep by anyone on your team to bring down the stack of cards.

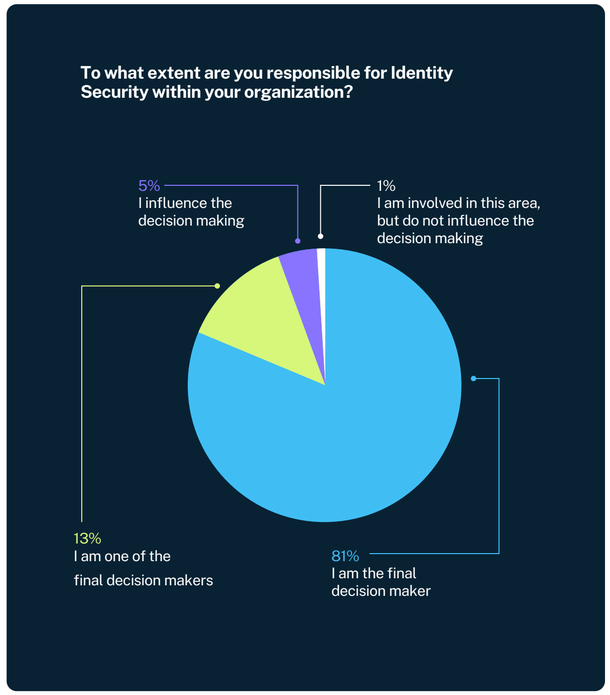
The one advantage we have is each other.

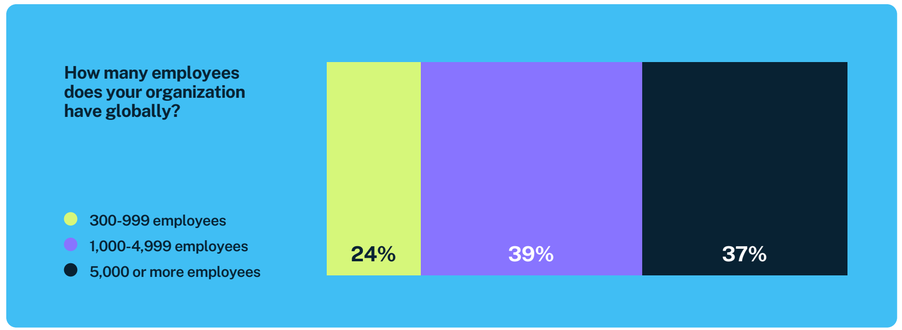
"Talent wins games, but teamwork and intelligence win championships." That’s not our quote (it’s Michael Jordan’s) but the advice is timeless. The team at your back isn't limited to your immediate colleagues. It spans your entire organization and even to your third- and fourth-party providers. It may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

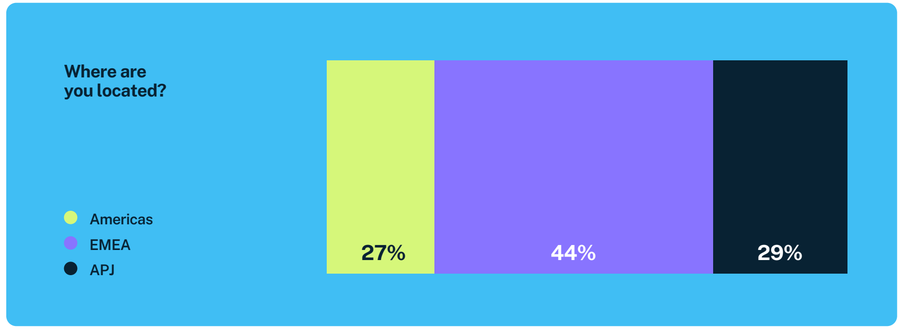
DEMOGRAPHICS

The CyberArk 2024 Identity Security Threat Landscape Report was conducted across private and public sector organizations of 500 employees and above. It was conducted by B2B technology research partners Vanson Bourne amongst 2,400 cybersecurity decision makers. Respondents were based in Brazil, Canada, Mexico, the US, France, Germany, Italy, the Netherlands, Spain, the UK, UAE, Australia, India, Hong Kong, Israel, Japan, Singapore and Taiwan.









CYBERARK®

SECURITY MATTERS

See how you can maximize risk reduction with an identity security approach.

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 organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit https://www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.