PERMISO

PERMISO STATE OF IDENTITY SECURITY REPORT 2024:

SHINING A LIGHT ON THE ELEPHANT IN THE ROOM

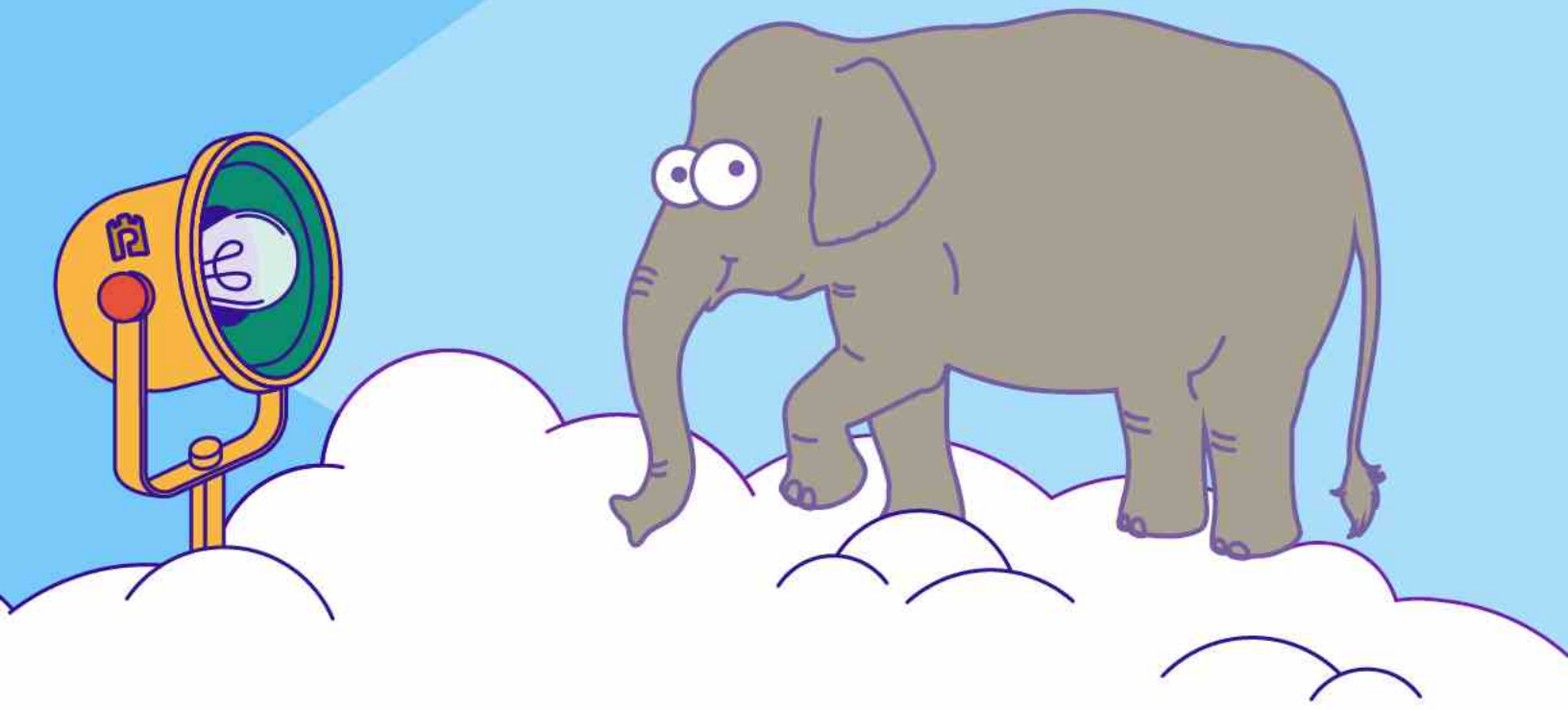


TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Permiso Security State of Identity Security Report (2024) offers a comprehensive analysis of cloud identity and access management practices across global organizations. This study, encompassing over 500 entities, unveils critical trends and challenges shaping the future of identity security.

KEY FINDINGS

93% of Organizations...

can inventory identities across all environments, as well as track keys, tokens, certificates and any modifications that are made to any environment.

85% of Organizations...

can determine "who" is doing "what" across authentication boundaries.

74% of Organizations...

Rate their cloud security maturity as "above average" to "advanced."

56% of Organizations...

rely on IT teams for securing identities across multiple environments.

45% of Organizations...

Remain "concerned" or "extremely concerned" about their current tools being able to detect against identity attacks.

45% of Organizations...

reported an identity security breach.

In 56% of Breaches...

Sensitive data including PII and IP was the target.

In 54% of Breaches...

Impersonation attacks were the leading threat vector.

Employees ...

Are the riskiest identity.

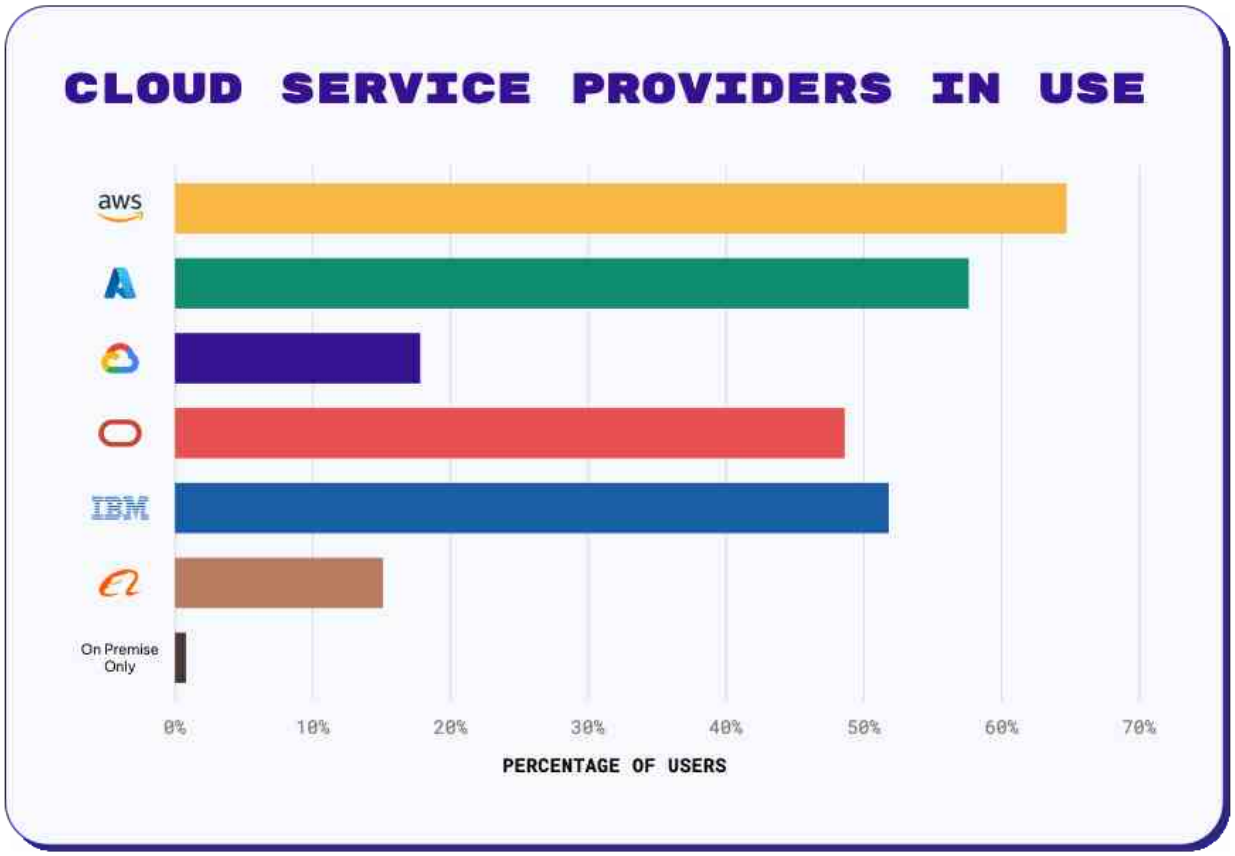
SaaS...

Is the riskiest environment.

The Leading Concern...

Is the ability to detect and prevent credential compromise, account takeover and insider threat.

THE MULTI-CLOUD REALITY RESHAPING IDENTITY SECURITY



Question asked, "Select your cloud services providers in use: (Select all that apply)"

In 2024, we introduced a new question to understand the adoption of public cloud service providers like AWS, Azure, GCP, Oracle Cloud, IBM Cloud, and others. From 510 survey respondents, we gathered information on the cloud service providers being used across organizations.

KEY FINDINGS

1. Organizations use an average of 2.5 cloud service providers
2. AWS leads with 25% market share, followed by Azure (22%) with GCP at 7%
3. IBM Cloud (20%) and Oracle Cloud (19%) show significant adoption

These figures align closely with Statista's Q1 2024 market share data (AWS 31%, Azure 25%, GCP 10%), confirming our survey's representation of broader market trends.

Notably, the results also highlighted substantial adoption of other cloud providers. IBM Cloud and Oracle Cloud demonstrated strong presence, accounting for 20% and 19% of responses respectively.

This diversity in cloud provider usage underscores the need for security solutions that can adapt beyond the "big three" providers.

IMPLICATIONS FOR IDENTITY SECURITY

1. **Expanded Attack Surface:** Multiple cloud providers increase potential entry points for threats.
2. **Multi-Service Complexity:** Each provider brings unique IAM tools and best practices, raising the risk of misconfigurations.
3. **Visibility Challenges:** Organizations find it difficult to maintain comprehensive oversight across diverse cloud environments.

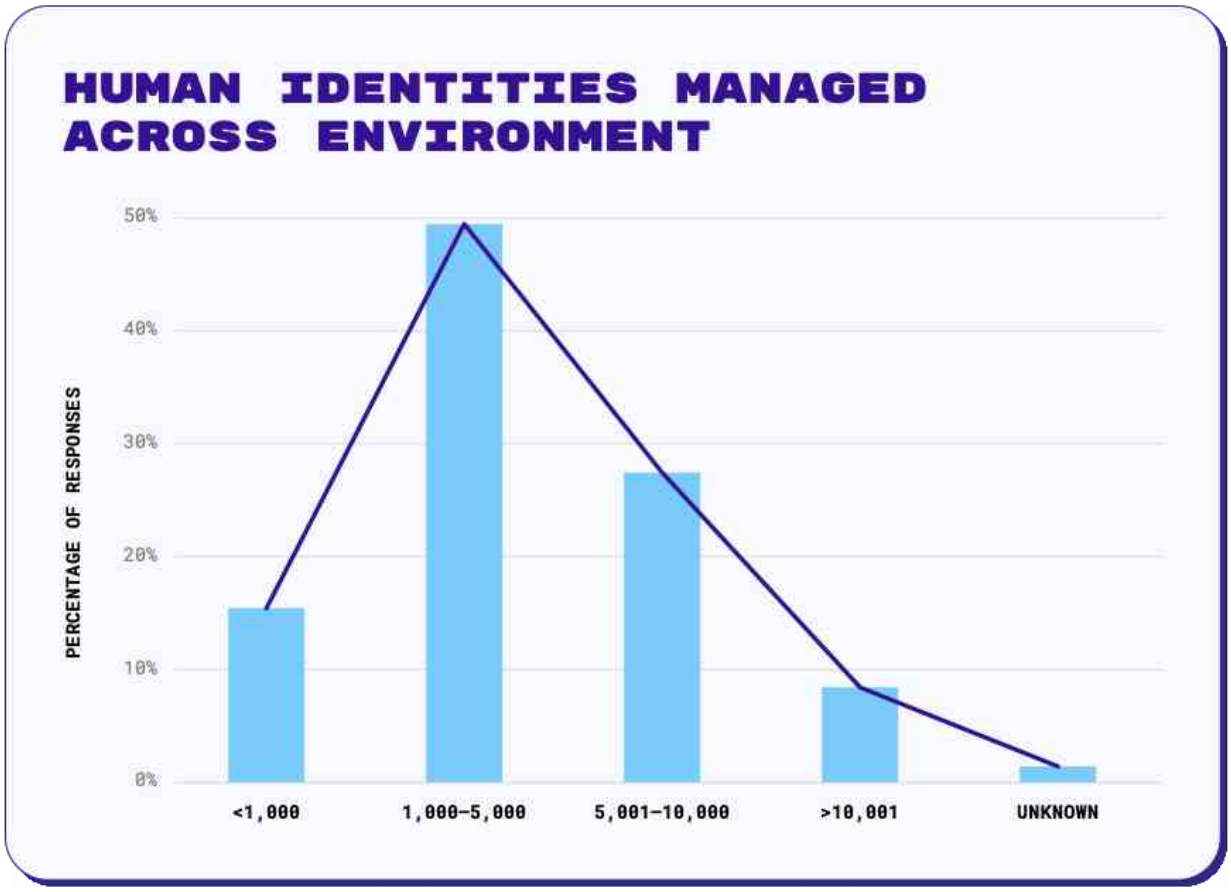
RECOMMENDATIONS

1. Implement cross-cloud identity governance solutions for unified visibility and control.
2. Standardize identity policies and automate enforcement across all cloud providers.
3. Adopt adaptive identity security solutions that can adjust to unique requirements of different cloud platforms.
4. Invest in advanced analytics and continuous monitoring capabilities to detect anomalies across all cloud environments.

LOOKING AHEAD

As multi-cloud strategies and adoption continue to evolve, organizations must balance the benefits of flexibility while also avoiding vendor lock-in. Identity-centric security solutions that can seamlessly operate across multiple cloud providers will be crucial for maintaining robust security postures in this complex landscape.

IDENTITY MANAGEMENT EVOLVES AS ORGANIZATIONS SCALE AND TIGHTEN CONTROL



Question asked, "How many human identities do you manage across cloud and on-premise environments? examples: human identities for AWS, Okta, Azure, AD, GCP, Auth0, PingIdentity, etc)"

KEY FINDINGS

- 48.4% of organizations now manage 1,000-5,000 identities, up from 39.1% in 2023
- Organizations managing over 10,000 identities decreased from 16.2% to 8.2%
- Small-scale identity management (under 1,000) slightly decreased from 17.2% to 15.1%

2024 marks a significant change in how organizations manage human identities across cloud and on-premise environments.

- **Mid-Range Boom:** Nearly half of all organizations (48%) now manage between 1,000-5,000 identities, up from 39.1% in 2023. This surge suggests a possible 'sweet spot' for balancing security, efficiency, and scale in today's digital landscape.
- **Big Players Downsizing:** Interestingly, the proportion of organizations managing over 10,000 identities has nearly halved, dropping from 16% to 8%. Are enterprises consolidating identities, or have they found new efficiencies in managing large-scale environments?
- **Small-Scale Stability:** Organizations with fewer than 1,000 identities remain a consistent minority, slightly decreasing from 17.2% to 15.1%. This stability indicates that even smaller enterprises are maintaining complex digital ecosystems.

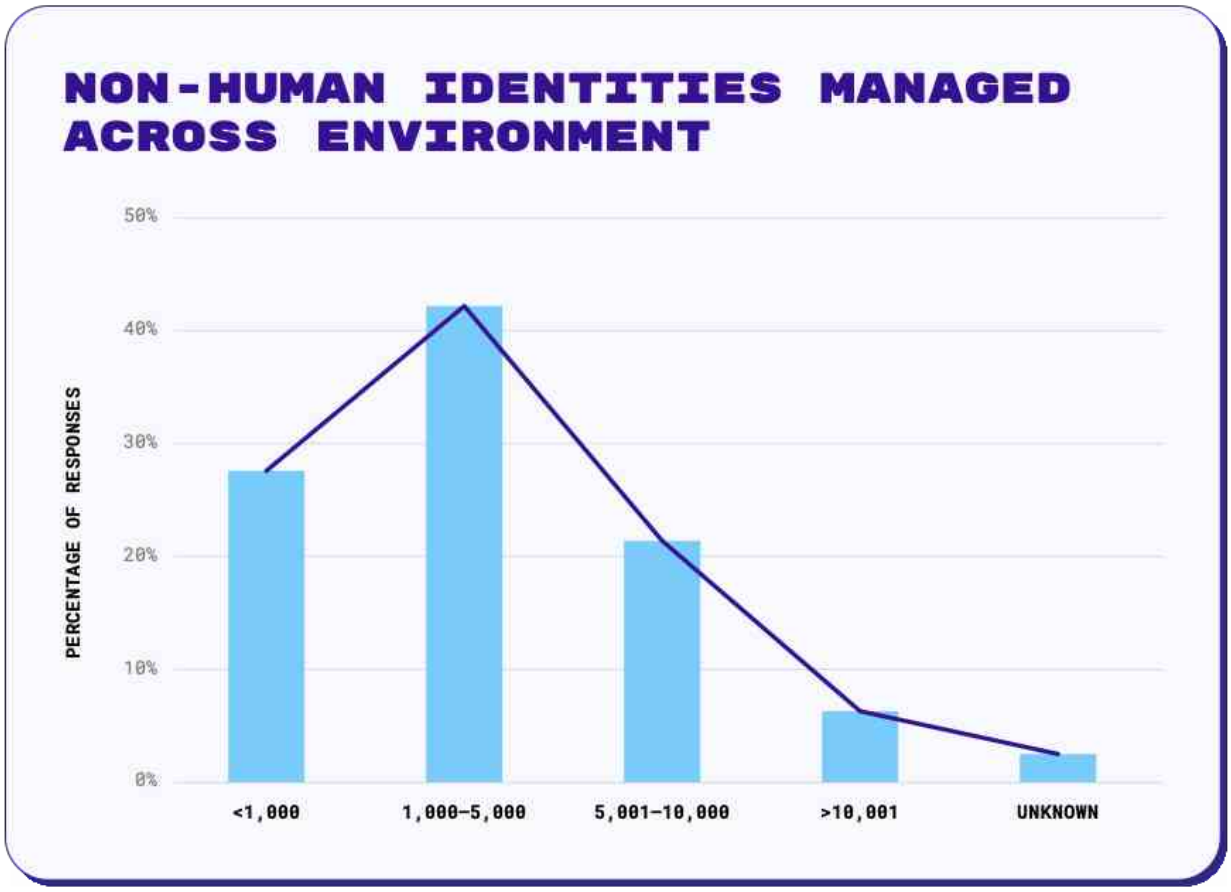
WHAT THIS MEANS FOR SECURITY

1. **Scalability is King:** With the mid-range segment growing, solutions must efficiently handle thousands of identities without compromising security.
2. **Consolidation Drives Efficiency:** Large enterprises are likely finding ways to streamline their identity ecosystems, potentially reducing attack surfaces.
3. **Visibility Gaps Persist:** The emergence of the 'Unknown' category highlights the ongoing challenge of maintaining comprehensive identity oversight.
4. **One Size Doesn't Fit All:** The diverse spread of identity scales emphasizes the need for flexible, adaptable security strategies.

LOOKING AHEAD:

As organizations continue to refine their approach to identity management, we expect to see increased demand for solutions that offer scalability, efficiency, and comprehensive visibility. The ability to adapt to changing identity landscapes will be crucial for maintaining robust security in an increasingly complex digital world.

NON-HUMAN IDENTITIES TAKE CENTER STAGE IN CLOUD ENVIRONMENTS



Question asked, "Question asked, "How many non-human identities (service accounts, keys/tokens or secrets) do you manage across your cloud environment?"

In 2024, we've witnessed a seismic shift in the identity landscape. Non-human identities – the silent workhorses of cloud environments – have exploded in number, fundamentally altering the security equation for organizations worldwide.

MID-RANGE DOMINANCE

The most striking change is the concentration of non-human identities in the 1,000-5,000 range, now representing 42.2% of surveyed organizations. This surge possibly suggests a 'Goldilocks zone' where automation and cloud services are being leveraged extensively, yet still manageably.

However, it could point to a gross underestimation of the sheer number of non-human identities that exist in a typical environment stemming from a lack of visibility, a scenario of 'out of sight, out of mind' playing out for most organizations.

IMPLICATIONS FOR IDENTITY SECURITY

1. **Identity Proliferation:** The substantial increase in non-human identities necessitates more sophisticated management and security strategies.
2. **Automation Challenges:** With more organizations managing larger numbers of identities, automated solutions for provisioning, monitoring, and deprovisioning become crucial.
3. **Visibility Imperative:** Despite improved awareness, organizations must continue to enhance their visibility into non-human identities to mitigate potential security risks.
4. **Scalability Demands**: Security solutions must be capable of handling the growing number of non-human identities without compromising effectiveness.
5. **Policy Complexity:** The diversification of identity types requires more nuanced and adaptable security policies.

SPOTLIGHT ON LARGE - SCALE OPERATORS

While fewer in number, organizations managing over 10,000 non-human identities (6%) face unique challenges. These environments likely represent cutting-edge, highly automated infrastructures that push the boundaries of current security paradigms.

THE VISIBILITY CHALLENGE

The introduction of an 'Unknown' category (3%) in our 2024 survey is telling. It highlights a critical issue: some organizations are operating with significant blind spots in their identity landscape.

LOOKING AHEAD: THE NON-HUMAN IDENTITY CHALLENGE

As non-human identities continue to proliferate, we anticipate:

1. Intelligence governance to adapt policies to diverse identity types and proactive risk management

2. Increased focus on real-time monitoring and anomaly detection for machine behaviors
3. Ecosystem integration to ensure seamless security across hybrid environments

This shift from managing keys to managing diverse non-human identities represents a maturation in cloud security practices. It reflects a growing understanding of the critical role that machine identities play in modern digital infrastructures.

THE ELUSIVE QUEST FOR COMPREHENSIVE IDENTITY MANAGEMENT

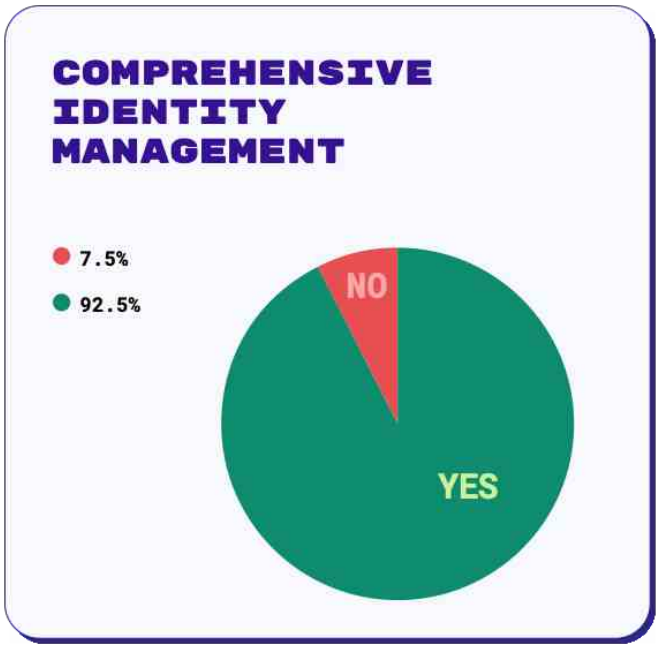
Our survey reveals an intriguing shift in organizations' ability to maintain a comprehensive inventory of identities accessing their cloud and on-premise environments.

THE NUMBERS TELL A STORY

→ 2023: 89% claimed comprehensive inventory

→ 2024: 93% report the same

At first glance, this 4% increase might seem modest. However, in the complex world of identity management, this uptick represents a significant stride forward.



Question asked, "Question asked, "How many non-human identities (service accounts, keys/tokens or secrets) do you manage across your cloud environment?"

As cloud environments become more complex, maintaining visibility across all identity types - from human users to non-human identities, across IaaS, PaaS, and SaaS - becomes increasingly challenging. The rise in affirmative responses suggests growing confidence among organizations in their identity management capabilities. This confidence, however, raises questions: Is it well-founded, or does it mask underlying challenges?

Interestingly, while more organizations claim comprehensive inventory, this very claim might indicate a lack of awareness about potential blind spots. The most security-conscious organizations often express more uncertainty, not less.

BRIDGING THE CHASM BETWEEN PERCEIVED AND ACTUAL IDENTITY RISKS

IDENTITY TYPES RISK RANKING

NON-HUMAN IDENTITIES	VENDORS	GUESTS	EMPLOYEES

LOWEST RISK — HIGHEST RISK

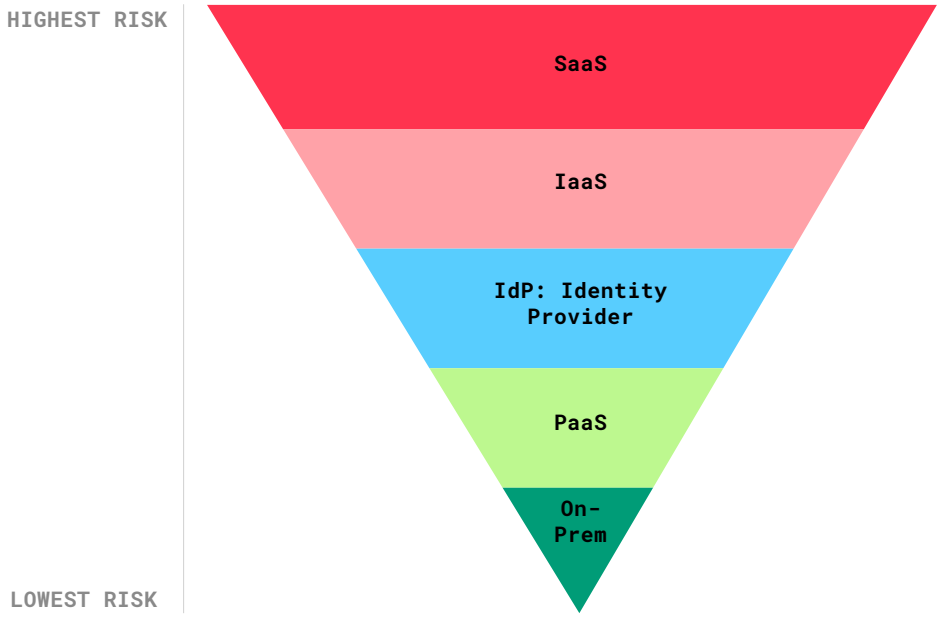
Question asked, "Stack-rank your riskiest identities (drag and drop with the riskiest identity in the top spot and least risky identity in the bottom spot)."

Employees, perennially seen as the weakest link in the security chain, predictably top the list. The placement of guests and vendors in the middle tiers acknowledges the risks associated with external human actors.

However, the positioning of non-human identities as least risky raises red flags. In an era where machine identities often outnumber human users and possess extensive privileges, this low-risk perception could be a ticking time bomb in many organizations' security strategies.

Organizations show a clear disconnect between perceived risks of different identity types and environments.

SHIFTING OUR GAZE TO THE ENVIRONMENTS, SAAS DOMINATES RISK



Question asked, Stack-rank your riskiest environments (drag and drop with the riskiest environment in the top spot and least risky in the bottom spot).

Here, the cloud sits at the top. SaaS environments, often adopted quickly and sometimes without proper oversight, are viewed as the biggest risk. This aligns with growing concerns about shadow IT and the challenges of securing rapidly expanding cloud services.

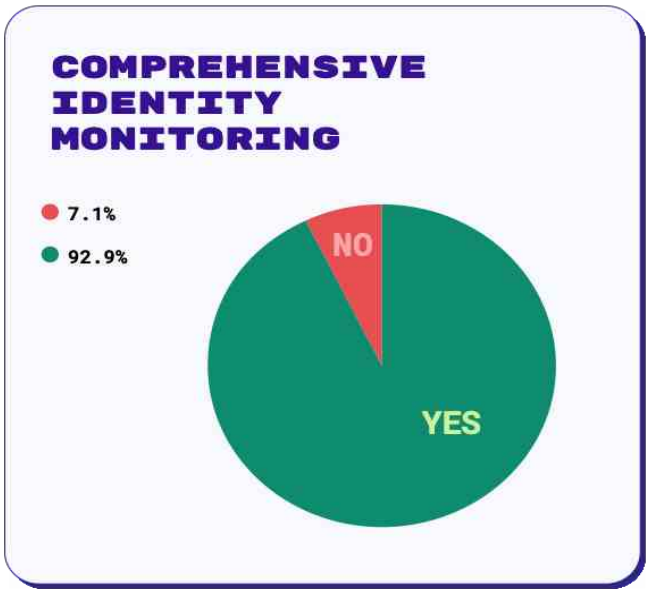
The middle ranking of Identity Providers (IdPs) is a concern. As the gatekeepers of access across multiple systems and environments, IdPs represent a potential single point of failure that, if compromised, could have cascading effects across an organization's entire IT ecosystem. Perhaps most surprising is the perception of on-premises environments as the least risky. This perception may be outdated, overlooking hidden vulnerabilities in legacy systems and the challenge of keeping security on par with modern cloud platforms.

The "Identity Risk Disconnect" revealed in this data – where non-human identities and critical infrastructure like IdPs are underestimated – represents a significant gap between perception and reality in many organizations' security postures.

THE ILLUSION OF COMPREHENSIVE IDENTITY MONITORING

In 2023, 90% of respondents claimed the ability to monitor services and resources accessed by identities in real-time across their cloud environments. Fast forward to 2024, and we see a slight uptick to 93% when asked about tracking the usage of keys, tokens, and certificates, as well as environmental modifications.

At first glance, these numbers paint a picture of robust IAM practices across the industry. However, peeling back the layers reveals a more complex reality.



"Question asked, "Are you able to track the usage of keys, tokens, certificates and any modifications that are made to any environments?"

THE VISIBILITY MIRAGE

Despite the high percentage of organizations claiming comprehensive monitoring capabilities, this data stands in stark contrast to the visibility gaps uncovered in other areas of our survey. The discrepancy suggests a potential overestimation of monitoring effectiveness or, more concerningly, a lack of understanding about what truly constitutes comprehensive identity monitoring in today's complex IT landscapes.

THE CONFIDENCE-CAPABILITY GAP

The persistently high percentages of organizations claiming advanced monitoring capabilities year over year raise a critical question: Are these capabilities truly advancing, or are we witnessing a plateau in monitoring sophistication against an ever-evolving threat landscape?

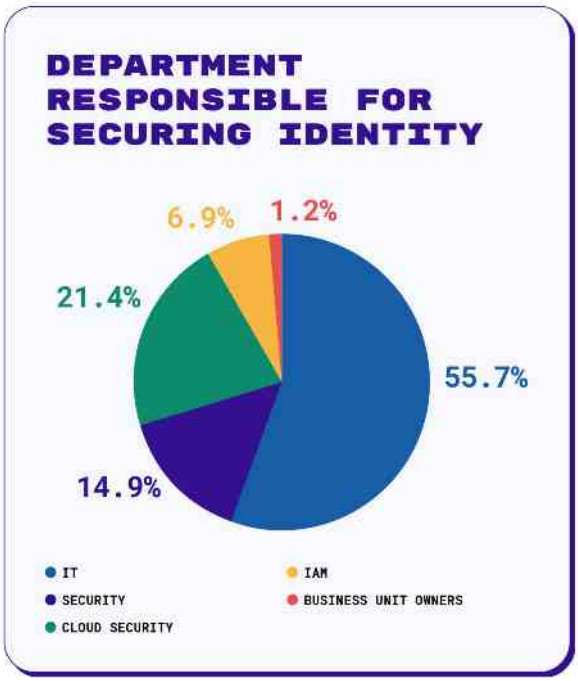
THE UNSEEN THREAT

Perhaps most telling is the small percentage of organizations that are either unsure or admit to lacking real-time monitoring capabilities. In 2023, 10% fell into this category, dropping slightly to 7% in 2024. While a minority, these organizations represent a significant vulnerability in the broader ecosystem.

"Truly understanding how all identities—both human and non-human—behave is more than a technical issue; it's essential for business. Closing the gap between what we think and what's real in identity monitoring is key to building strong, flexible security systems for the future." – Paul Nguyen, Co-Founder and Co-CEO, Permiso Security

THE IDENTITY SECURITY RESPONSIBILITY FALLS THROUGH THE CRACKS

Our survey reveals a shocking reality: Despite identity being the cornerstone of modern cybersecurity, in more than half organizations, IT departments, not specialized identity teams, are responsible for securing identities in an organization. This misalignment could leave companies vulnerable to sophisticated identity-based attacks.



Question asked, "Which department is responsible for securing identities across all environments?"

The numbers tell a concerning story:

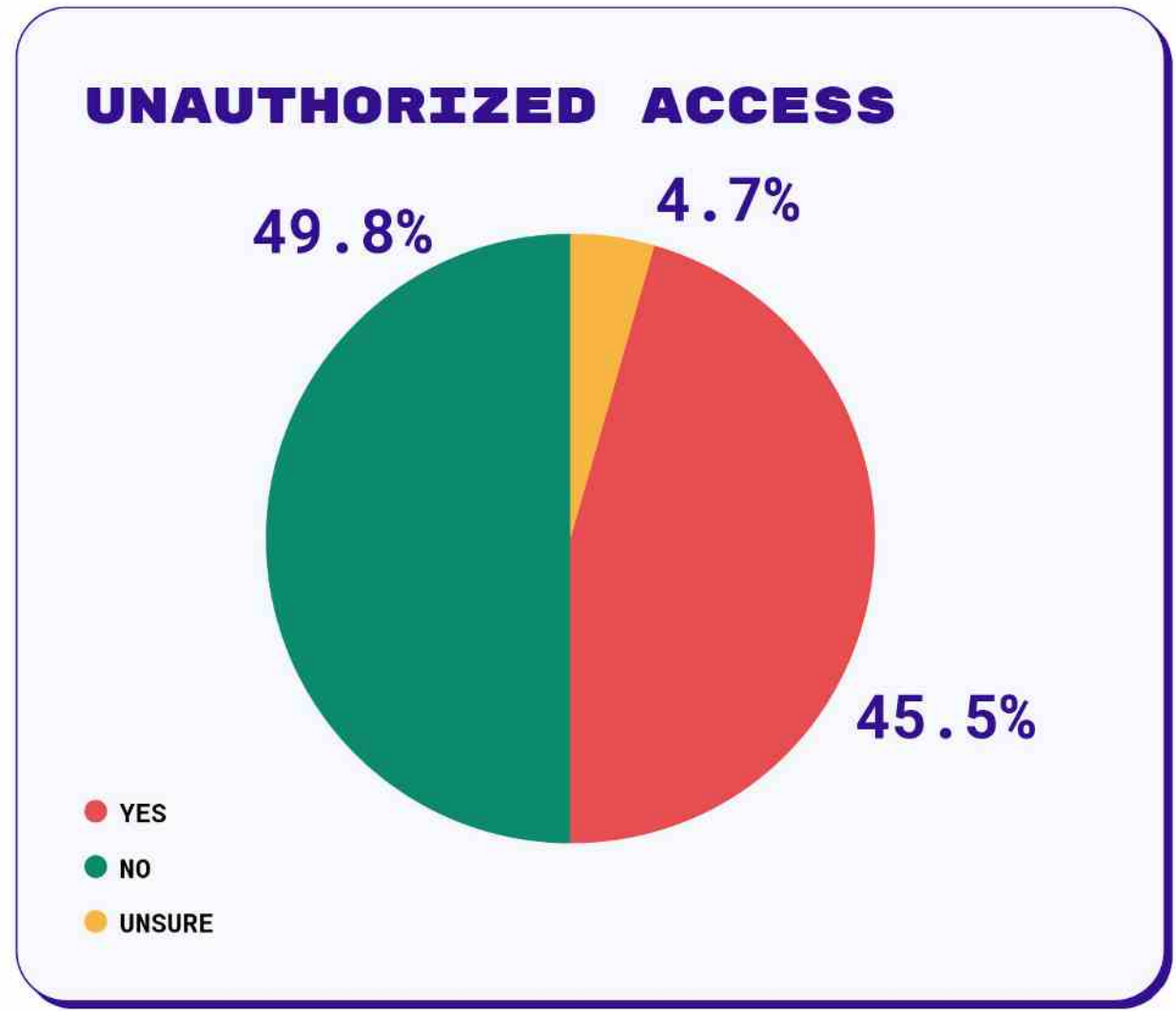
- A staggering 56% of organizations assign identity security to IT departments
- Dedicated IAM teams are in charge in only 7% of cases
- Even traditional security teams (15%) and cloud security teams (21%) play smaller roles

The minimal involvement of dedicated IAM teams (7%) is particularly concerning. It suggests many organizations haven't recognized identity security as a distinct discipline requiring specialized skills. As identity-based attacks increase, this lack of focus could leave organizations unprepared.

The scattered responsibility across IT, cloud security, and traditional security teams indicates that consensus is lacking on the correct approach to securely manage identities in organizations. This fragmented approach may lead to inconsistent security practices and potential vulnerabilities that can be exploited by threat actors.

Organizations are treating digital identities - which define who we are, what we can do, and when and how we can do it - as just another IT task. It's the equivalent of asking a family doctor to perform open-heart surgery. To truly secure their digital identities, companies need specialist "identity surgeons" – dedicated IAM teams armed with the right knowledge and the right set of tools. This isn't just about security; it's about safeguarding the digital essence of your business, its data and its people.

UNAUTHORIZED ACCESS REMAINS A STUBBORN THREAT IN CLOUD ENVIRONMENTS



Question asked, "Has there ever been unauthorized access into your cloud services environments?"

The 2024 survey results reveal that unauthorized access remains a significant threat in cloud environments, despite some improvements. This highlights an ongoing gap between security measures and evolving attack tactics.

THE UNSETTLING REALITY OF COMPROMISED CREDENTIALS

In 2023, we posed a pointed question: “Has there ever been unauthorized access into your cloud environment via a compromised credential?“ The responses were alarming:

- A staggering 49% of organizations admitted to experiencing unauthorized access.
- 45% reported no such incidents.
- 6% were unsure, highlighting a troubling lack of visibility.

This data paints a stark picture: nearly half of all cloud environments surveyed had been breached through compromised credentials. The implications are profound, suggesting that traditional security measures were failing to safeguard against one of the most fundamental attack vectors.

A YEAR LATER: MARGINAL IMPROVEMENT, PERSISTENT THREAT

Fast forward to 2024, and we see a landscape that has evolved, but not dramatically improved. Our follow-up question, “Has there ever been unauthorized access into your cloud services environments?“ revealed:

- 46% of organizations reported unauthorized access incidents.
- 5% remained unsure.
- 50% claimed no such breaches.

THE ILLUSION OF PROGRESS

At first glance, the 4% decrease in reported unauthorized access incidents might seem encouraging. However, this marginal improvement belies a more complex reality:

- **Persistent Vulnerability:** Despite a year of technological advancements and increased awareness, nearly half of all organizations surveyed remain vulnerable to unauthorized access.
- **The Visibility Conundrum:** While the percentage of organizations unsure about breaches decreased slightly (from 6% to 5%), this still represents a significant blind spot in cloud security postures.

- **The Adaptation Race:** The minimal reduction in unauthorized access suggests that as organizations enhance their security measures, threat actors are evolving their tactics at a comparable pace.

IMPLICATIONS FOR SECURITY

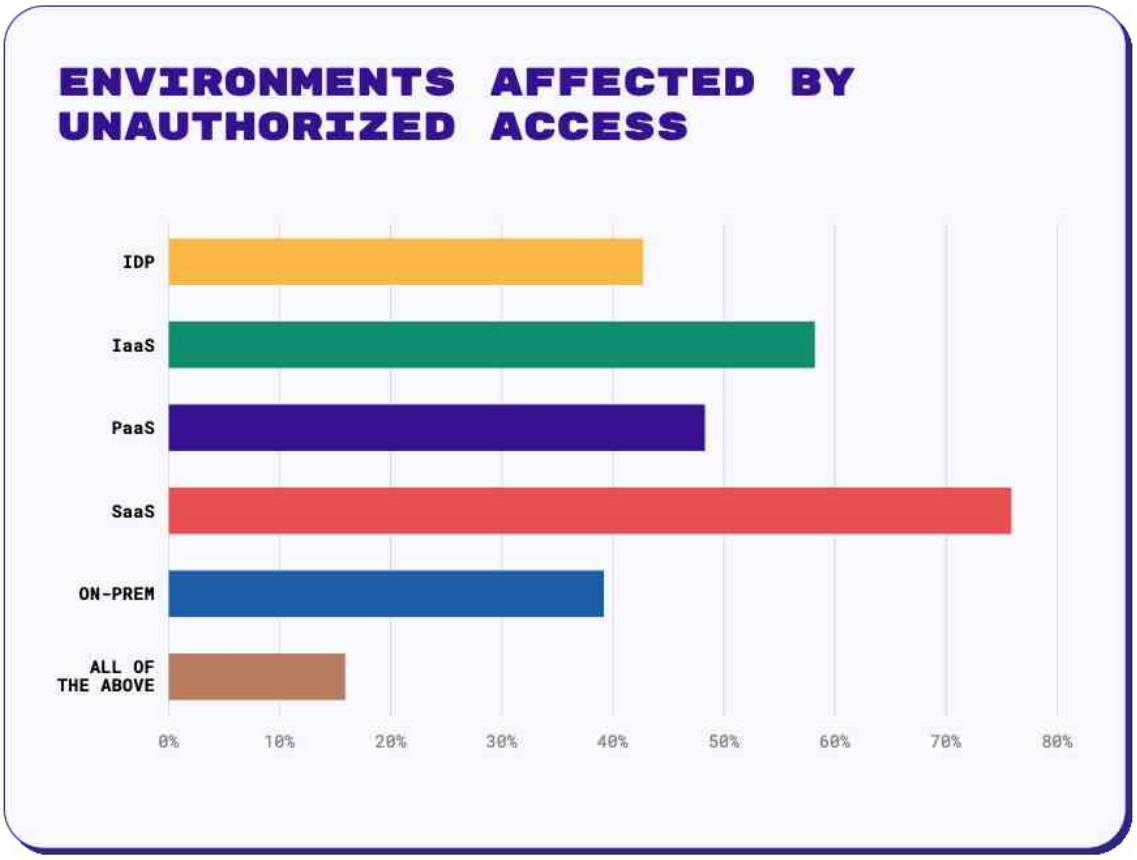
These findings raise important questions about current cloud security strategies:

1. **IAM Effectiveness:** Are current identity and access management practices adequate for complex cloud environments?
2. **Potential Overconfidence:** The increase in organizations reporting no unauthorized access might indicate improved security or a false sense of safety.
3. **Need for Better Monitoring:** The persistent uncertainty underscores the need for enhanced threat detection capabilities.

UNRAVELING THE COMPLEX WEB OF CLOUD SECURITY BREACHES

Our report examines three key aspects of cloud security breaches in 2024: affected environments, attack vectors, and resulting impacts. By studying these interconnected elements, we can better understand the full lifecycle of cloud security incidents, from initial breach to final impact. This comprehensive view allows us to identify trends, vulnerabilities, and areas where organizations may need to focus their security efforts.

1. THE MULTIFACETED NATURE OF CLOUD VULNERABILITIES



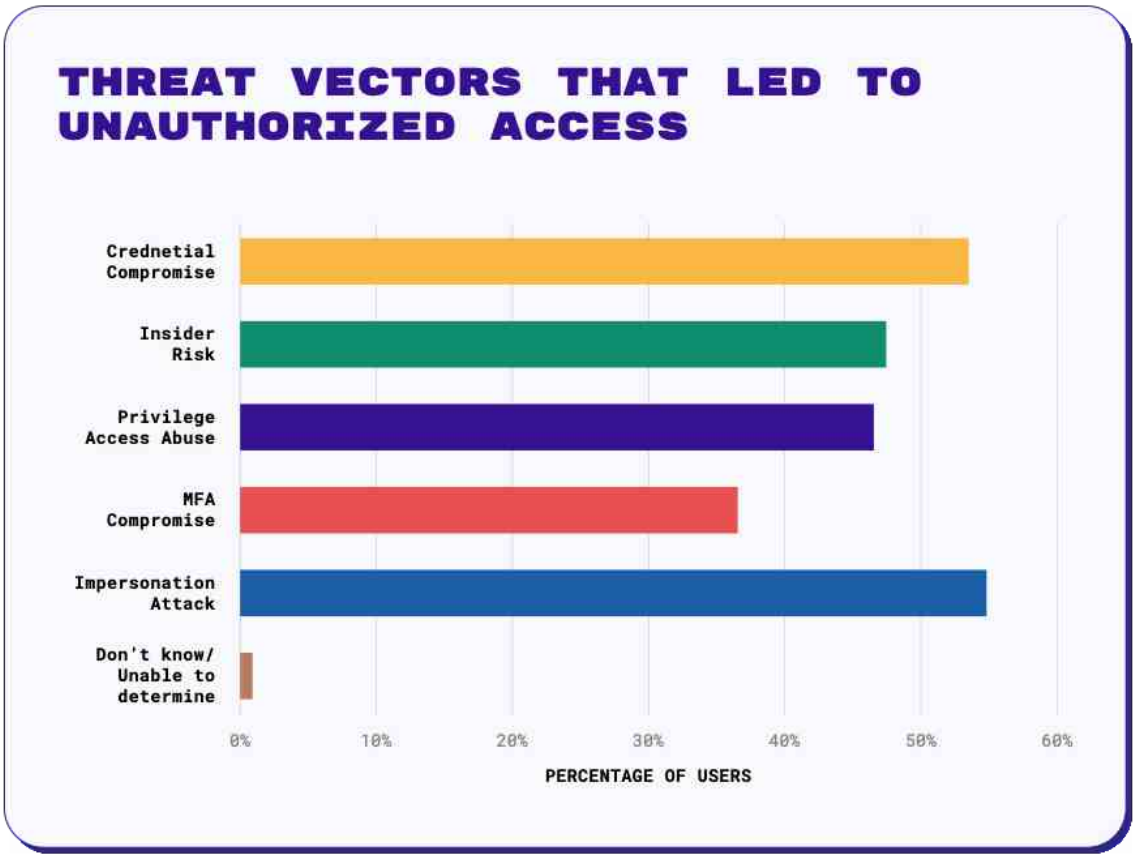
Question asked, "Please indicate which environment(s) was/were affected by the unauthorized access. Select all that apply."

SaaS environments emerge as the most vulnerable, with 76% of affected organizations reporting breaches in these platforms. This is followed by IaaS (58%), PaaS (48%), and

Identity Providers (43%). On-premises systems, while still vulnerable (39%), appear relatively more secure.

The Vulnerability Paradox: The inverse relationship between the adoption rate of cloud services (typically SaaS > IaaS > PaaS) and their security posture reveals a critical "security lag." This suggests that as organizations rapidly adopt new cloud services, security measures struggle to keep pace, creating a window of heightened vulnerability.

2. THE TAXONOMY OF THREAT VECTORS

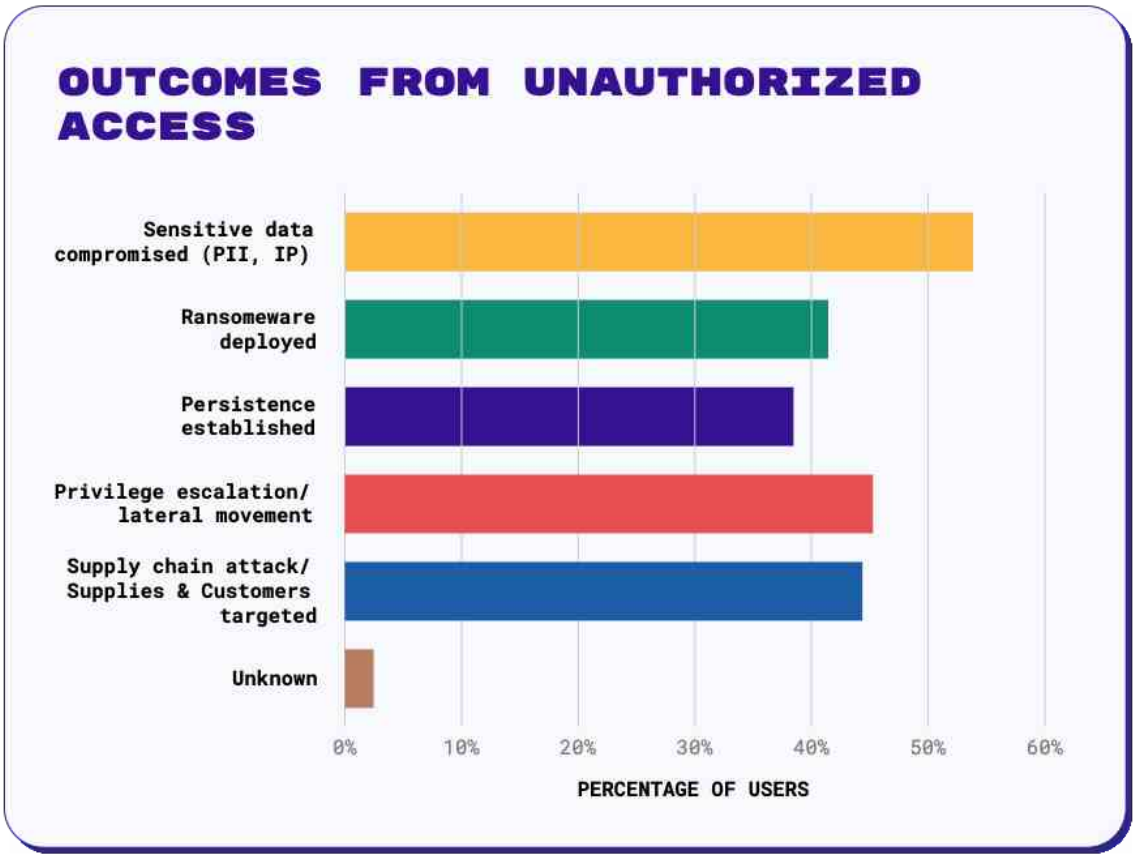


Question asked, "Please indicate the threat vector(s) that led to the unauthorized access. Select all that apply."

Impersonation attacks (54%) and credential compromise (53%) top the list of threat vectors, closely followed by insider risks (47%) and privilege access abuse (46%). The high incidence of MFA compromise (36%) is particularly alarming.

The prevalence of impersonation attacks over direct credential compromise indicates a shift towards more sophisticated, social engineering-based approaches that bypass traditional security measures.

3. THE CASCADE OF CONSEQUENCES



Question asked, "What was the outcome of the unauthorized access? Select all that apply."

The outcomes of these breaches are severe and multifaceted:

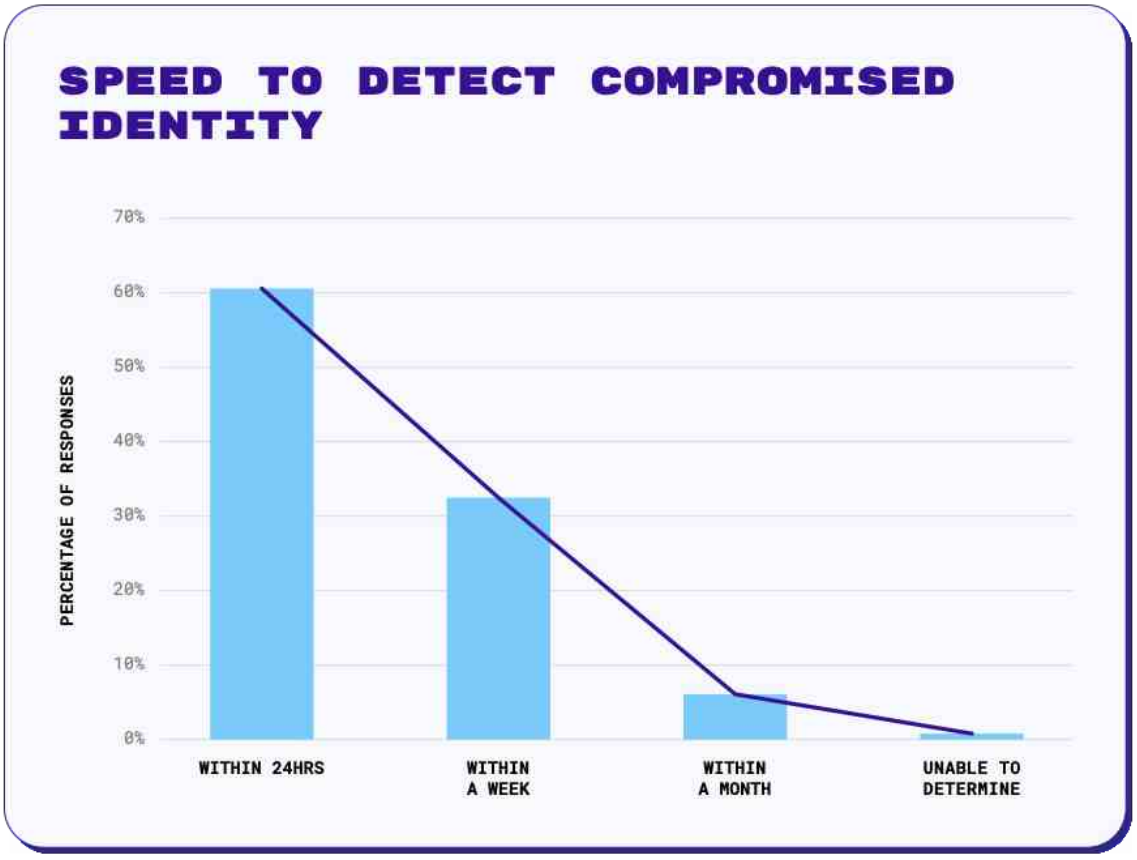
- 54% resulted in sensitive data compromise
- 46% led to privilege escalation or lateral movement
- 45% impacted supply chains
- 42% saw ransomware deployment
- 39% established persistence

SYNTHESIS AND IMPLICATIONS

1. **The Identity Crisis:** With Identity Providers being compromised in 43% of cases and impersonation attacks leading the threat vectors, we're witnessing an "identity crisis" in cloud security. Traditional perimeter-based security models are proving inadequate in this new landscape.
2. **The SaaS Security Gap:** The high vulnerability of SaaS environments (76%) coupled with their popularity presents a critical security challenge. This "SaaS Security Gap" needs urgent addressing through specialized security measures and user education.
3. **The MFA Fallacy:** The significant rate of MFA compromise (36%) challenges the perception of MFA as a silver bullet. This "MFA Fallacy" calls for a re-evaluation of authentication strategies, possibly moving towards adaptive, context-aware authentication methods.
4. **The Supply Chain Ripple Effect:** With 45% of breaches impacting supply chains, we're seeing a "Supply Chain Ripple Effect." This highlights the need for a more ecosystem-wide approach to security, extending beyond organizational boundaries.
5. **The Persistence Paradox**: The ability of attackers to establish persistence in 39% of cases, despite advancements in detection and response, reveals a "Persistence Paradox." This suggests a need for more robust post-breach detection, containment and eradication strategies.

The results underscore the need for a paradigm shift in cloud security strategies – one that emphasizes adaptive, identity-centric approaches, continuous monitoring, detection and response, and collaborative security ecosystems that extend beyond specific services boundaries.

THREAT DETECTION TIMELINES REVEAL SHIFTING CAPABILITIES



Question asked, "What best describes how quickly you would be able to detect and determine a compromised identity successfully gaining access to one of your environments?"

Our 2023-2024 survey reveals significant changes in organizations' ability to detect compromised identities in cloud environments.

24-HOUR DETECTION WINDOW

While 2023 saw 90% of organizations claiming detection within 24 hours (20% within 1 hour, 47% within 12 hours, and 23% within 24 hours), 2024 shows a more conservative but still high 61% for within 24hours. This doesn't necessarily indicate a decline in capabilities, but potentially a more over-optimistic assessment of detection timelines.

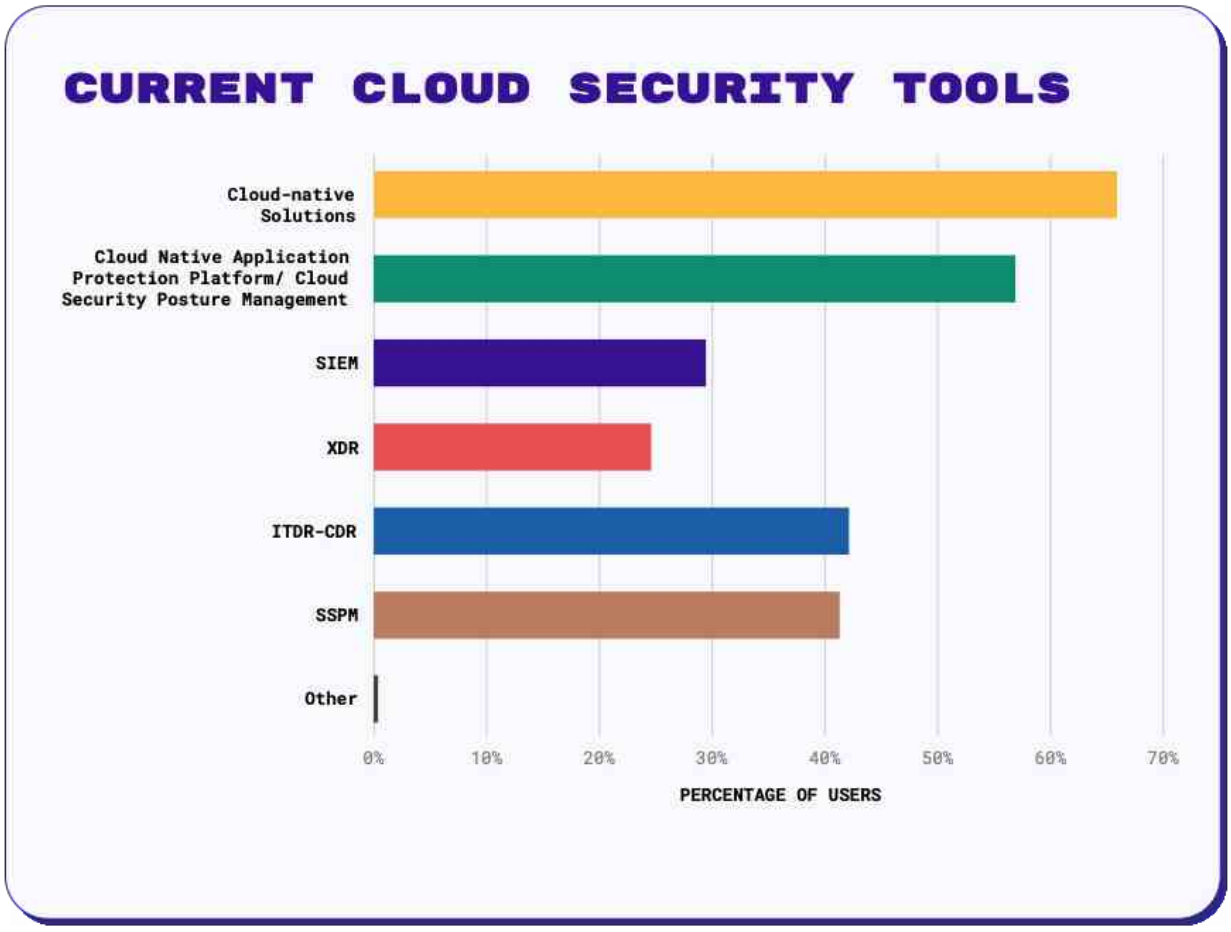
CONSISTENCY IN WEEKLY DETECTION

The ability to detect threats within a week remains relatively stable: 97% in 2023 vs. 93% in 2024. This suggests that overall detection capabilities are maintained, but with a shift in the distribution of response times.

EXTENDED DETECTION TIMES

In 2023, only 1% of respondents needed more than a week for detection of threats, while in 2024, that number rose to 6%. The emergence of a larger group needing up to a month for detection might reflect recognition of more sophisticated threats against inadequate real time threat detection capabilities.

CLOUD SECURITY TOOLS ADAPT TO A CHANGING THREAT LANDSCAPE



Question asked, "What current cloud security tooling do you utilize to secure your cloud services layers?"

SHIFT TOWARDS INTEGRATED SECURITY PLATFORMS

While cloud-native tools remain dominant at 66% adoption in 2024, their 4% decline from 2023 (70%) coupled with the significant rise of CSPM from 48% to 57% indicates a market shift towards diversified security strategies - organizations are increasingly seeking integrated platforms that offer broader visibility and control across their entire cloud ecosystem.

IDENTITY-CENTRIC SECURITY FOCUS

The consistent adoption of ITDR-CDR tools, despite a slight 4% decrease (from 46% to 42%) indicates these tools remain integral to many security strategies, underscoring the ongoing importance of identity-centric security measures. This focus on identity aligns with the zero-trust security model, which is gaining traction in cloud-first environments.

ADAPTING LEGACY TOOLS FOR THE CLOUD ERA

The modest decline in SIEM (from 32% to 30%) and XDR (from 27% to 25%) suggests a recalibration towards more cloud-specific security solutions: organizations are likely seeking ways to integrate these traditional security tools into their cloud-centric security strategies.

TOOL ADOPTION PATTERNS AND SECURITY MATURITY

→ Layered Security Approach

- 66% use cloud-native solutions
- 57% employ CSPM/CNAPP
- 42% utilize ITDR-CDR

This overlap suggests that organizations are adopting a multi-layered security strategy. We can infer that at least 22% of organizations are using all three types of tools, indicating a more mature security posture.

→ Emerging Technology Adoption Rate

SSPM adoption (41%) nearly matches ITDR-CDR (42%) in its first year, suggesting:

- Rapid recognition of SaaS-specific security needs
- Organizations may be shifting budget from identity to SaaS security

→ Traditional vs. Cloud-Specific Tools

Combined SIEM and XDR adoption (54.3%) is lower than CSPM/CNAPP (56.9%), indicating:

- A preference for cloud-specific solutions over traditional security tools
- Potential gaps in integration between cloud and on-premises security

→ Security Resources Allocation

The adoption rates might indicate where organizations are allocating their security resources:

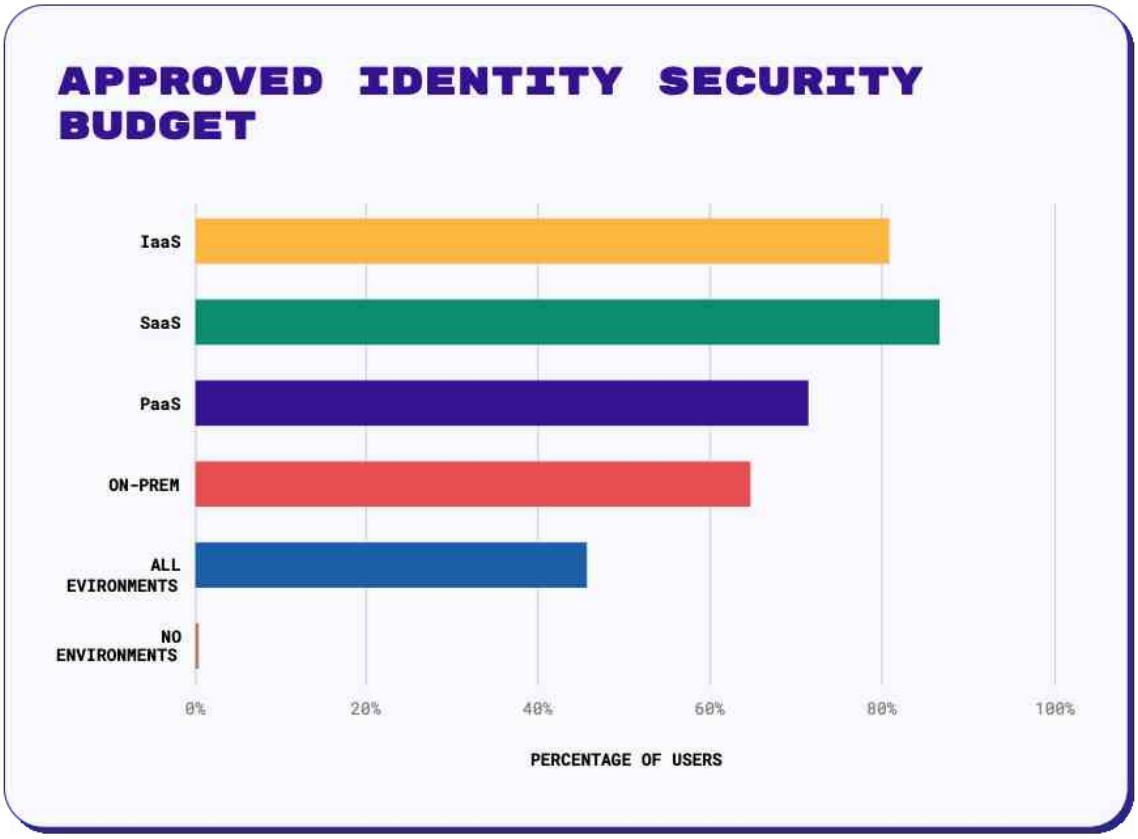
- **High priority:** Cloud-native security (66%) and posture management (57%)
- **Medium priority:** Identity and SaaS security (both around 41-42%)
- **Lower priority:** Traditional security tools (SIEM 30%, XDR 25%)

→ Potential Security Gaps

- 34% of organizations not using cloud-native solutions may be relying solely on third-party tools, potentially missing out on platform-specific security features
- The 43% not using CSPM might lack continuous assessment of their cloud security posture, a critical component in maintaining robust security

We're seeing that organizations are not abandoning their cloud-native foundations but are increasingly supplementing them with specialized tools, CSPM, SSPM and ITDR designed to maintain secure configurations and address the unique security challenges posed by cloud and SaaS environments.

IDENTITY SECURITY BUDGETS REVEAL ORGANIZATIONAL PRIORITIES AND CHALLENGES



Question asked, "Which of the following, if any, do you have approved identity security budget for? Select all that apply."

FINDINGS	DATA POINT	IMPLICATIONS
THE SAAS-FIRST MENTALITY	SaaS leads with 87% budget allocation, surpassing IaaS (81%).	• A shift towards decentralized IT • Potential security gaps as traditional perimeter-based security becomes obsolete • Dedicated security focus for SaaS as a major attack vector
THE HYBRID REALITY	65% still allocating budget to on-premises security alongside cloud investments	• Persistence of legacy systems in most enterprises • Challenges in maintaining consistent security posture across hybrid environments • Potential for security silos and blind spots between on-prem and cloud systems
THE PAAS PUZZLE	71% budgeting for PaaS security	• Increasing adoption of container and serverless technologies • Potential security risks as traditional IaaS and SaaS security tools may not suffice
THE HOLISTIC MINORITY	Only 46% report budgeting for “All environments“	• A concerning lack of comprehensive security strategy in over half of organizations • An opportunity for security vendors to offer more integrated, cross-environment solutions

Budget Allocation Patterns: The descending order of budget allocation (SaaS > IaaS > PaaS > On-Prem) mirrors the typical cloud adoption journey, suggesting:

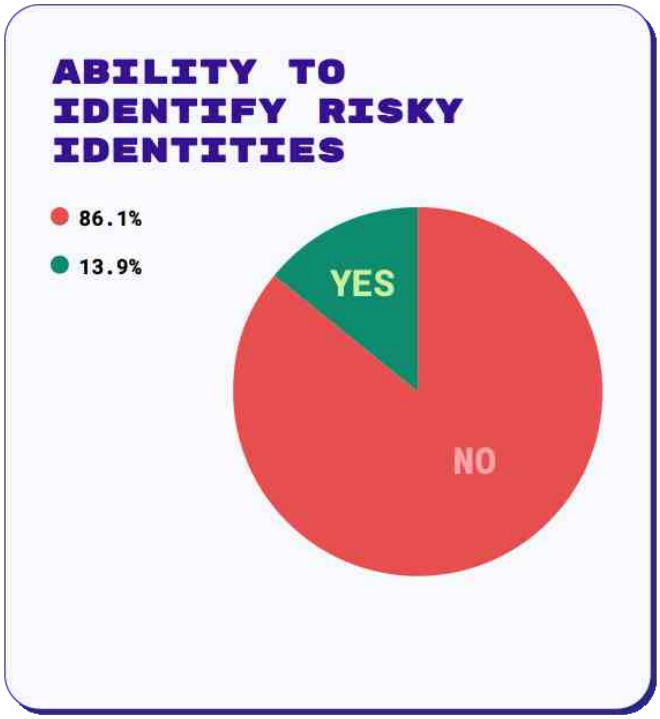
- Security investments closely follow technology adoption trends
- A reactive rather than proactive approach to security in many organizations
- Potential gaps in emerging technologies that don't fit neatly into these categories (e.g., edge computing, IoT)

The Multi-Cloud Imperative: High percentages across IaaS, SaaS, and PaaS indicate widespread multi-cloud strategies, implying:

- Increased complexity in managing identities across diverse environments
- A need for cloud-agnostic identity security solutions
- Potential for inconsistent security practices across different cloud platforms

IDENTIFYING HIGH-RISK IDENTITIES BECOMES A CRITICAL SECURITY CAPABILITY

Our 2024 survey introduces a new question that probes organizations' ability to pinpoint their most vulnerable identities across all environments. The results reveal a strong trend towards advanced identity risk management.



Question asked, "Are you able to identity the top 10 riskiest identities across all of your environments?"

A significant 86% of organizations report they can identify their top 10 riskiest identities across all environments. This high percentage suggests that most companies have implemented sophisticated identity analytics and risk assessment tools.

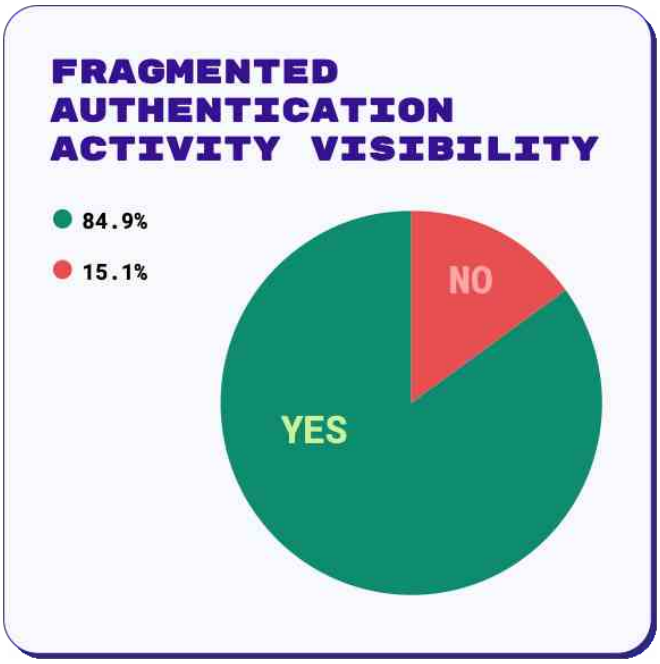
However, the data also highlights a potential blind spot in the industry. 14% of organizations admit they cannot identify their riskiest identities. This gap represents a considerable security vulnerability, as these organizations may struggle to focus their defensive efforts effectively.

The ability to identify high-risk identities is particularly important given the evolving threat landscape. As attackers increasingly target privileged accounts and leverage identity-based attack vectors, understanding which identities pose the greatest risk becomes a critical component of a robust security strategy.

This new data suggests that many organizations are moving beyond traditional perimeter-based approaches to focus on the identities that access their critical systems and data. Looking ahead, closing the gap for the 14% of organizations that lack this capability should be a priority.

THE "WHO" AND "WHAT" ACROSS COMPLEX AUTHENTICATION BOUNDARIES

The example provided in the question (Okta -> GitHub -> Terraform -> AWS) represents a highly intricate authentication chain. The ease (almost 85%) with which organizations claim to navigate this complexity may indicate:



Question asked, "Are you currently able to easily answer "who" is doing "what" across fragmented authentication boundaries (example: Okta-> GitHub-> Terraform-> AWS)"

1. **Advanced identity management systems in place** - Organizations have prioritized advanced identity management as a cornerstone of their security strategy, enabling them to maintain visibility in increasingly complex digital ecosystems.

2. **Potential underestimation of the true complexity of environments** - This could reflect a focus on surface-level tracking without fully grasping the deeper complexities of identity propagation and transformation across disparate systems, potentially leaving blind spots in security coverage.

3. **A gap between perceived and actual visibility capabilities** - What organizations believe they can track and what their current tools are actually capable of. The 15% acknowledging difficulty in tracking across boundaries may paradoxically be in a stronger position:

- More realistic assessment of their capabilities
- Likely to invest more in robust identity monitoring solutions
- Potentially more alert to the risks of fragmented authentication

Questions for Further Consideration

- How is this visibility being measured or validated?
- Are organizations truly able to track actions in real-time, or is this retrospective analysis?
- What's the depth of visibility – surface-level tracking or deep, contextual understanding?

Implications for Vendors and Solutions:

- A need to educate the market on the true complexities of cross-boundary identity tracking
- Opportunities to provide more sophisticated, real-time analytics and anomaly detection
- The importance of solutions that can validate and test the actual effectiveness of cross-boundary visibility

UNPACKING THE SPECTRUM OF ORGANIZATIONAL SECURITY CONFIDENCE

Question asked, "On a scale of 1 to 5 (with 1 being 'Not mature' and 5 being 'Advanced maturity') please rate the maturity of your cloud security

CLOUD SECURITY MATURITY IS AT A HIGH POINT

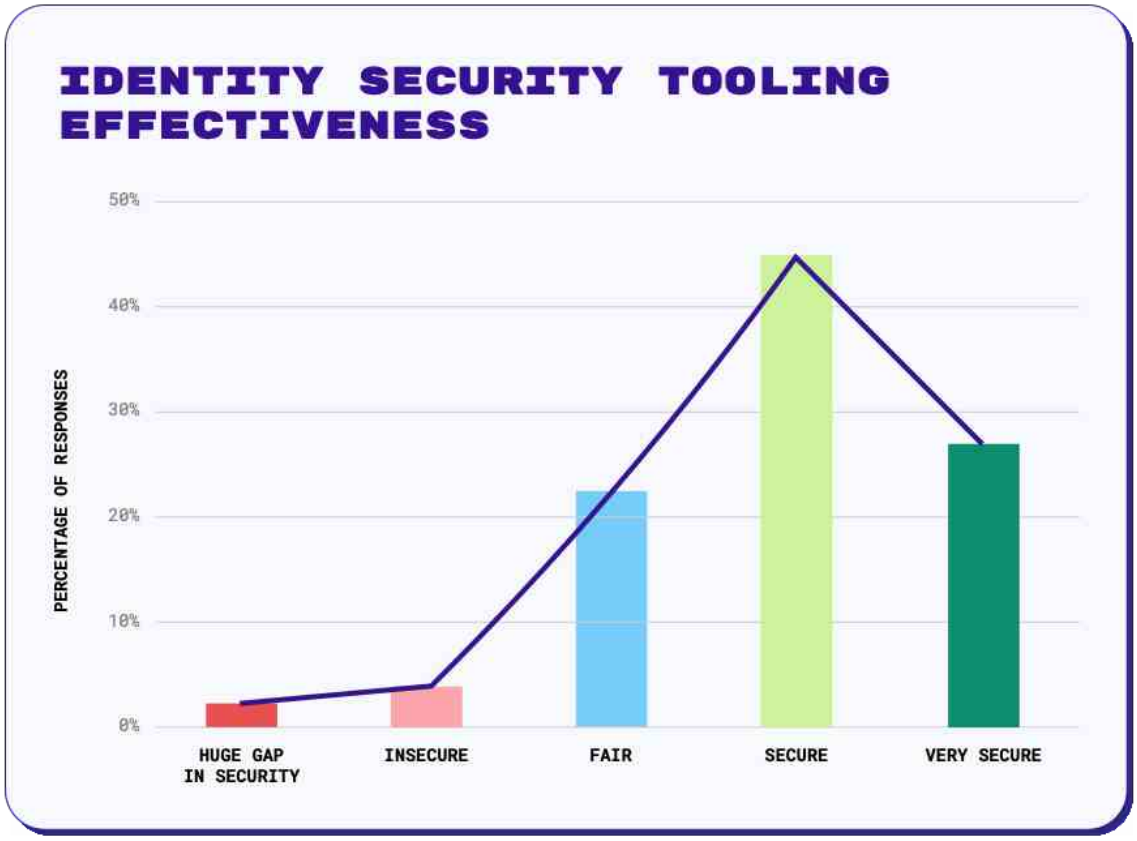
- Nearly half (45%) rate their cloud security maturity at an "advanced" level
- Another 29% believe they are "Above Average"
- Combined, nearly 3 in 4 organizations are extremely confident about their cloud security maturity

These findings could point to a belief that existing cloud security investments translate into improvements in cloud security maturity. Although this may be valid, it could also infer that majority of organizations are fixating security efforts on tackling known risks. Given

that for most organizations cloud majority is still in its developmental phase, these results must be viewed with some degree of caution.

JUST OVER A QUARTER ARE SOBER MINDED ON RISK

- 23% of organizations rate their maturity as average with an additional 3% falling into the below average, not mature category.



Question asked, "On a scale of 1 to 5 (with 1 being 'Huge gaps in security' and 5 being 'Very secure') please rate how you feel your current tooling is protecting your organization from a well-orchestrated identity-based attack on your organization."

CONFIDENCE DOMINATES THE SECURITY LANDSCAPE (72%)

- A whopping 45% feel "Secure"
- Another 27% believe they are "Very Secure"
- Combined, nearly 3 in 4 organizations exude confidence in their identity security defenses

Such confidence in today's complex threat environment raises a crucial question: Is this confidence based on robust security measures, or could it indicate a potential blind spot?

CAUTIOUS REALISM CHARACTERIZES THE MIDDLE GROUND (22%)

- These realists acknowledge their security as merely "Fair"
- They're neither overly confident nor excessively worried

This group's balanced view might reflect a more nuanced understanding of the threat landscape. Their cautious stance could drive continuous improvement in security measures.

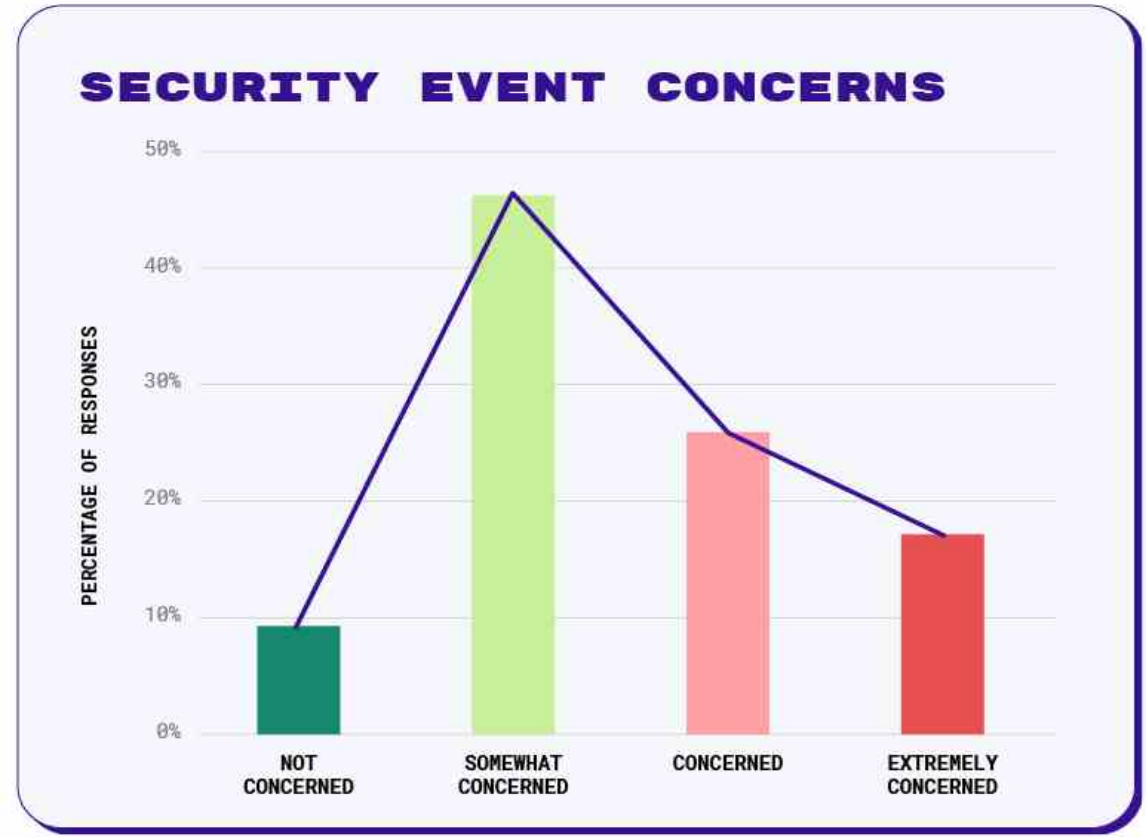
A SMALL FRACTION RECOGNIZES SIGNIFICANT VULNERABILITIES (6%)

- 4% admit to feeling "Insecure"
- A concerning 2% recognize "Huge gaps in security"

While a small percentage, this group's awareness of their vulnerabilities is crucial. Their concerns could stem from recent security incidents, limited resources, or a more acute understanding of emerging threats.

Confidence without competence is a recipe for disaster. The question isn't just "How secure are we?" but "How accurately do we perceive our security?" And the answer may be the difference between genuine resilience and a house of cards waiting to fall.

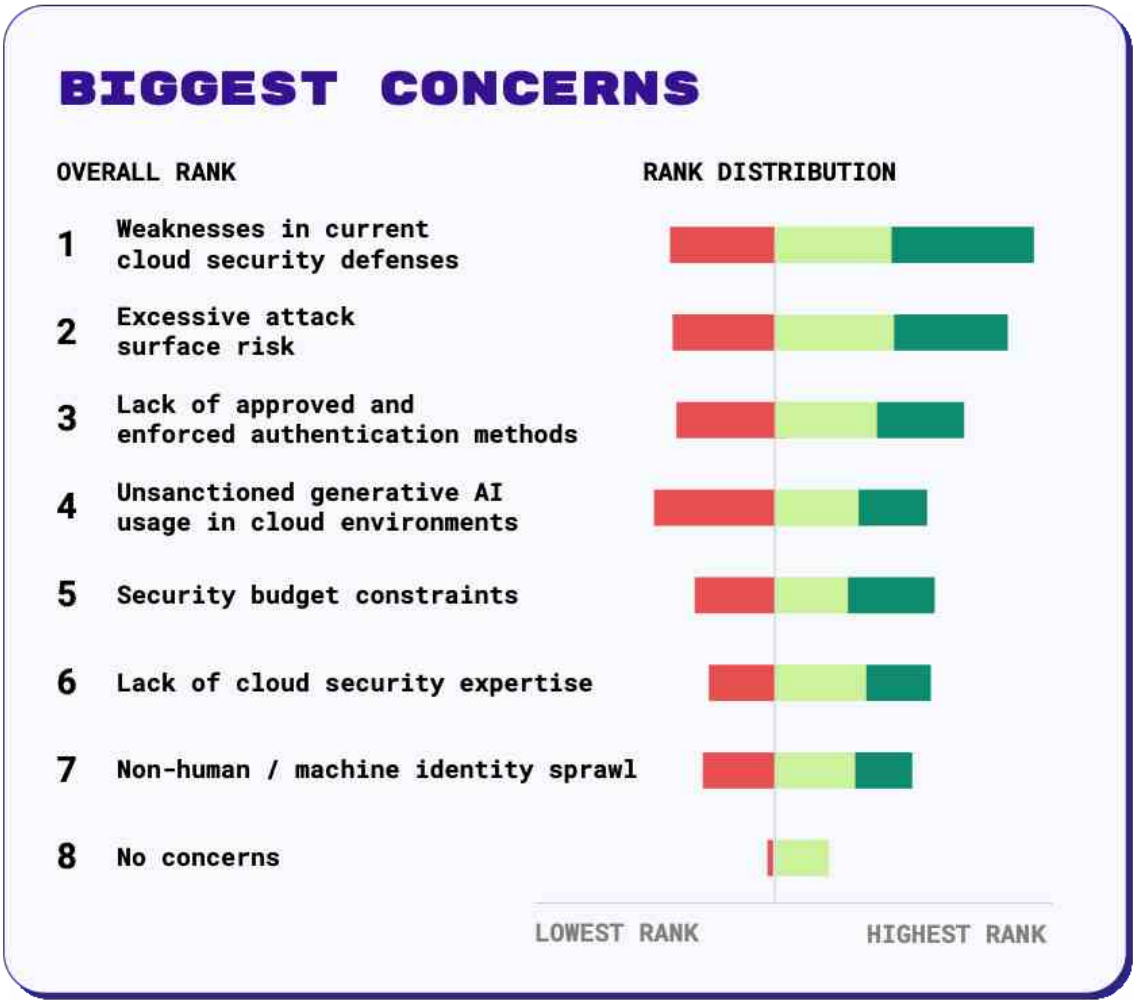
CLOUD SECURITY CONCERNS EXPOSING A HIERARCHY OF RISKS



Question asked, "How concerned are you that your current tools and teams may not be able to detect and respond to a security event in your environments"

DESPITE CONFIDENCE, CONCERN IS PALPABLE (45%)

Nearly half (45%) of respondents reported being "concerned" or "extremely concerned" that their current tools may not be able to detect and respond to a security event in their environment. Given that an equal number of respondents, 45%, reported suffering an identity related breach might point to a scenario of organizations that have had their security controls tested understand their true degree of cybersecurity resilience and ability to respond to an actual incident.



Question asked, "What are you most concerned about? Select top 3 and rank them in order with most concerned being the top ranking."

Our final question reveals a clear pecking order in cloud security concerns, highlighting where organizations are focusing their attention—and where potential blind spots may lurk.

TOP-TIER CONCERNS: TRADITIONAL THREATS STILL REIGN SUPREME

1. Weaknesses in Current Defenses: Taking the Top Spot

- Credential compromise, account takeovers, and insider threats remain the primary bogeymen
- Organizations are acutely aware of their vulnerability to these classic attack vectors

2. Excessive Attack Surface: A Close Second

- Zombie accounts, identity sprawl, and privilege creep form a triad of concern
- The complexity of modern cloud environments is clearly keeping security teams on their toes

3. Authentication Woes: Rounding Out the Top Three

- MFA and Security Tokens are recognized as critical, yet implementation lags
- A gap between knowing what's needed and actually deploying it is evident

MID-TIER PRIORITIES: EMERGING THREATS AND RESOURCES CONSTRAINTS

1. AI in the Shadows: A New Entrant

- Unsanctioned generative AI usage is raising eyebrows
- Organizations are waking up to the double-edged sword of AI in cloud environments

2. Budget Blues: The Eternal Struggle

- Security teams continue to grapple with limited resources
- The relatively low ranking suggests other concerns are overshadowing financial constraints

THE LOWER RANKS: OVERLOOKED OR UNDERESTIMATED?

1. Expertise Shortage: A Surprising Low Rank
    - The lack of cloud security expertise is not top-of-mind for many
    - This could indicate overconfidence or a lack of awareness about skill gaps
2. Machine Identity Sprawl: The Sleeper Threat
    - Non-human identities are proliferating, yet concern lags
    - This low ranking could be a significant blind spot as automation increases

What This Tells Us

- Traditional threats still dominate the security landscape
- Emerging risks like AI and non-human identities are on the radar but not yet priority
- There's a potential misalignment between perceived and actual threats
- The low ranking of expertise shortage could be a ticking time bomb

The data paints a picture of an industry still grappling with fundamental security challenges while new threats emerge on the horizon. The question remains: Are organizations looking in the right direction as the identity security landscape evolves?

CONCLUSION

The Permiso Security State of Identity Security Report (2024) underscores the pivotal role of identity security management in the current cloud security landscape. As organizations continue to embrace multi-cloud strategies and witness the proliferation of human and non-human identities, the complexity of managing and securing identities has reached unprecedented levels.

The data reveals a mixed picture of progress and persistent challenges. While many organizations report advanced capabilities in identity management and threat detection, there are concerning gaps in visibility, particularly across different access methods and cloud environments. The high incidence of unauthorized access, despite increased security measures, indicates that threat actors are evolving their tactics as rapidly as defenses are being fortified.

Perhaps most tellingly, the report highlights a significant disconnect between perceived security capabilities and actual vulnerabilities. This "confidence-capability gap" poses a substantial risk, potentially leaving organizations exposed to sophisticated, identity-based attacks.

Looking ahead, several key areas demand attention:

1. Bridging the gap between cloud adoption and identity security implementation
2. Developing more comprehensive identity security strategies for managing human and non-human identities across multiple environments
3. Implementing truly comprehensive, real-time all entity identity monitoring across all environments
4. Shifting towards more proactive, identity-centric security models
5. Addressing the organizational divide and responsibility misallocation for identity security responsibilities

As we move forward, the ability to adapt to this changing landscape will be crucial. Organizations must strive for a balance between leveraging the benefits of cloud technologies and maintaining robust identity security postures. This will require not just

technological solutions, but also a fundamental shift in how we approach identity and access management in the cloud era.

The path forward is clear: identity must be at the center of cloud security strategies. Only by placing identity at the core of security architectures can organizations hope to navigate the complexities of modern cloud environments securely and effectively.

These findings underscore the complex challenges organizations face in securing identities across increasingly diverse and distributed cloud environments. The report highlights a critical need for more integrated, identity-centric security and risk management strategies that can adapt to the rapidly evolving threat landscape while providing comprehensive visibility and control across all cloud platforms and services.

PERMISO

THANK YOU

QUESTIONS? CONTACT US AT HELLO@PERMISO.IO