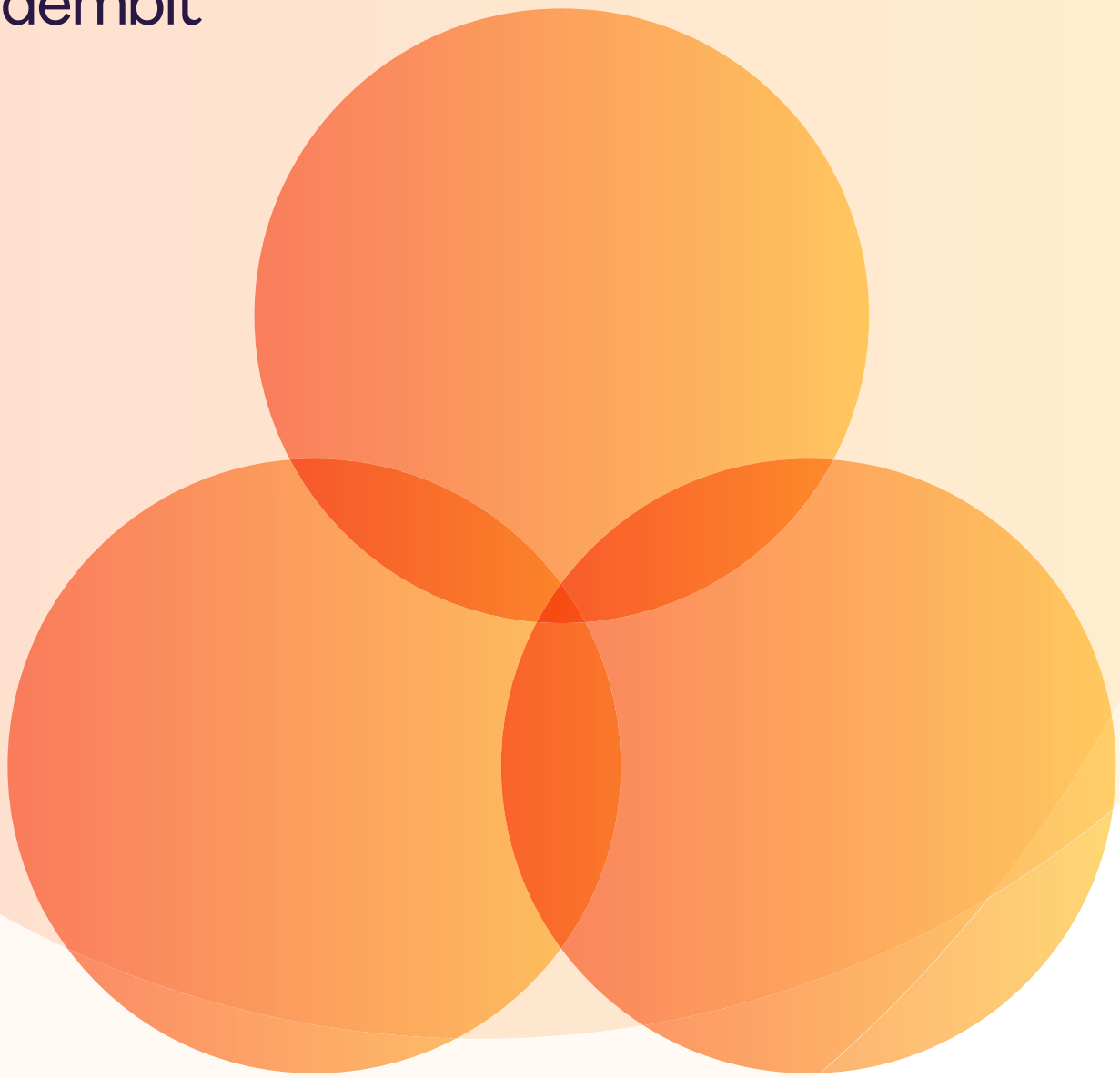
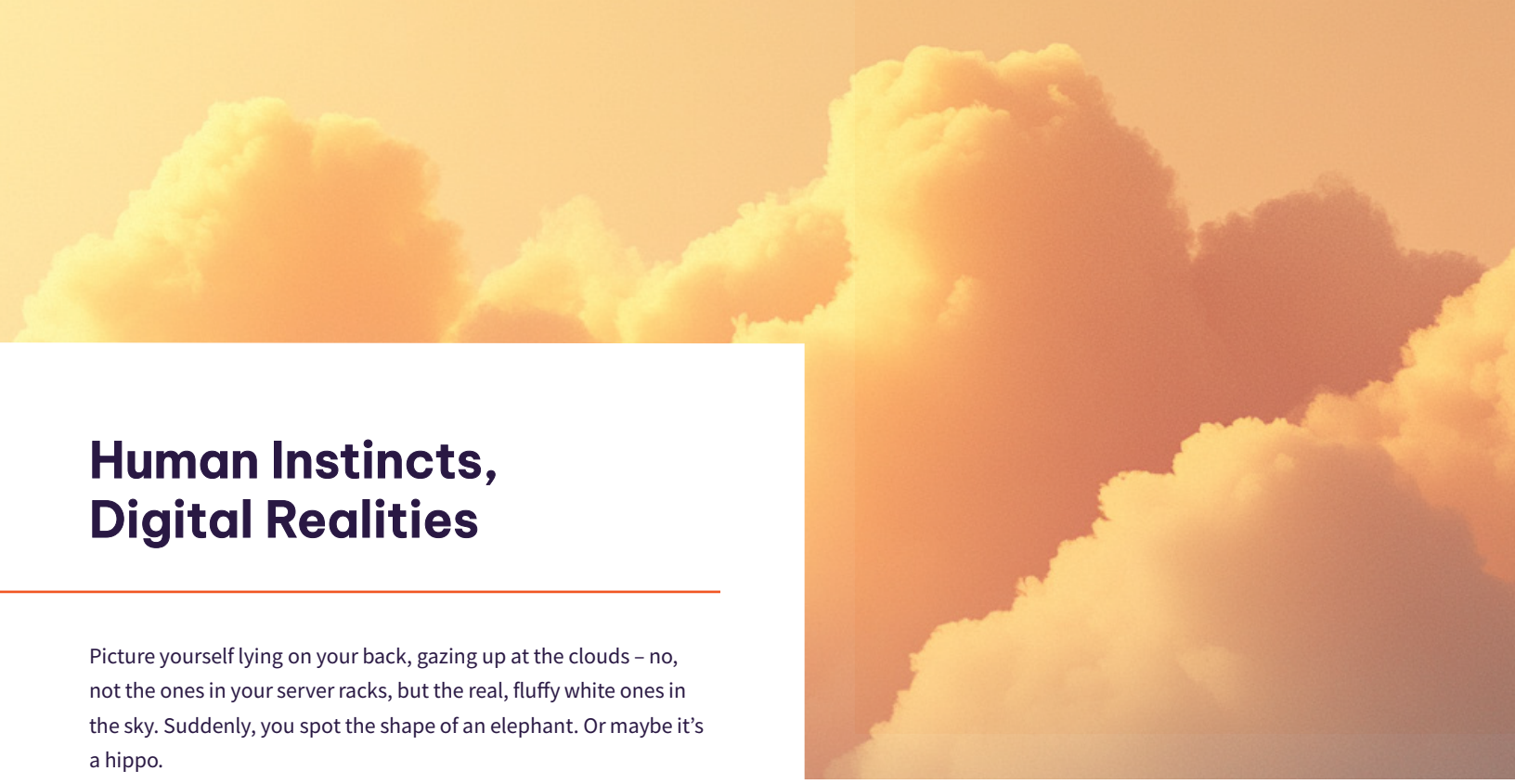
aembit



SURVEY

2024 Non-Human Identity Security Report from Aembit

As software workloads multiply, are organizations ready to secure them with the diligence they now require?



Human Instincts, Digital Realities

Picture yourself lying on your back, gazing up at the clouds – no, not the ones in your server racks, but the real, fluffy white ones in the sky. Suddenly, you spot the shape of an elephant. Or maybe it's a hippo.

Or think about that cold winter morning when you found yourself giving your road-weary sedan a pep talk, coaxing it to start with the promise of a full-detail spa day. *C'mon, baby, just this once and I swear I'll make you shine like new again.*

Not to go all scientific on you, but these moments are prime examples of how our minds naturally lean toward pareidolia, where we see familiar patterns in random stimuli, or anthropomorphism, where we assign human traits to non-human things. It's how we, as people, make sense of the world – by relating the unknown to what we know best: ourselves and our everyday experiences.

In the world of IT, a similar conceptual leap is happening with non-human identities (NHIs) – the sensitive workloads, machines, and automated processes that organizations rely on to create products and ensure everything runs smoothly. NHIs are specifically assigned to, you guessed it, entities other than humans, such as applications, scripts, microservices, APIs, databases, and, crucially, the service accounts they use.

OK, but what do sky pillows and an aging set of wheels have to do with computing resources operating within enterprises?

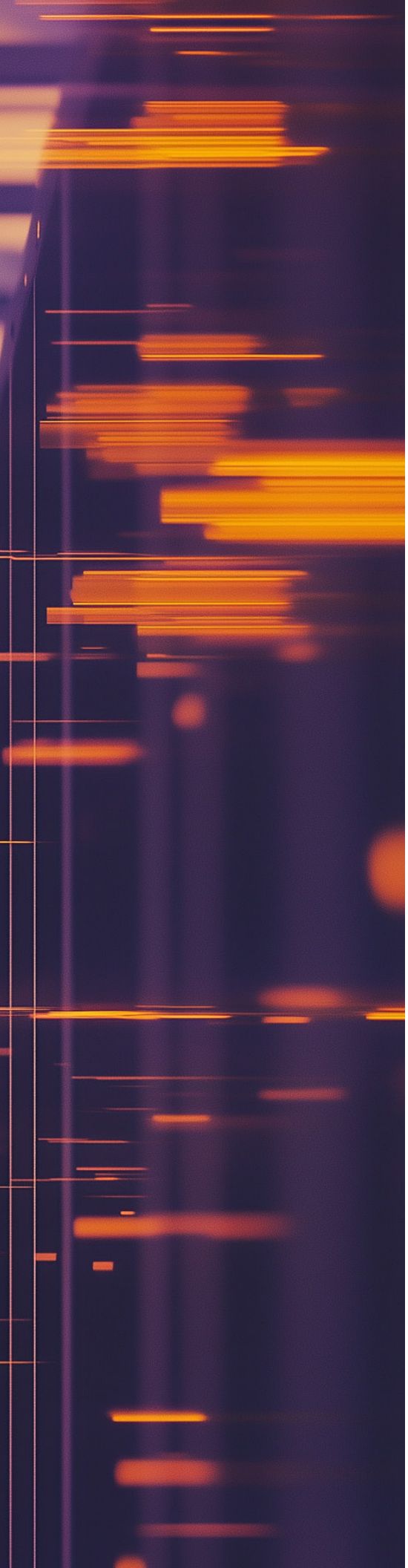
Non-human identities are no longer just tools used by employees; they are now entities in their own right. Service accounts, for example, function similarly to user profiles, providing specific identities to automated processes and applications, authorizing specific privileges within other systems.

In other words, NHIs have become active participants in our digital ecosystem, with distinct roles and responsibilities akin to human users. And while we might not be assigning them nicknames like Betsy – or imagining them in the shape of a dragon – the way we're starting to think about and address these identities shows just how much they've evolved.

To get a clearer picture of how companies are managing NHIs – and where they're hitting roadblocks – we decided to dig a little deeper. That's what led us to conduct our latest survey. Some questions allowed respondents to select multiple answers, capturing the full range of challenges, while others were more focused, requiring a single response.

In the following sections, we'll explore the survey results, examine current approaches to NHI management, and offer guidance on how to strengthen your non-human identity security.

So without further ado, onward, fellow humans.



Key Findings

IAM Maturity Gap

A striking **88.5%** of organizations admit their non-human IAM practices lag behind or are merely on par with their user IAM efforts, revealing a critical gap in focus and investment.

Outdated Methods

While **51%** of respondents use cloud provider IAM tools for non-human identities, a concerning **38.9%** still rely on less secure methods like secrets managers to authenticate and authorize non-human workloads.

Cloud Complexity

Ensuring consistent access management across hybrid and multi-cloud environments is the top non-human identity security challenge for **35.6%** of organizations.

Insecure Practices

Alarmingly **30.9%** of organizations store long-term credentials directly in code, **23.7%** share secrets through copying and pasting via email or messaging apps, and **15.5%** use manual spreadsheets to store secrets.

Low Confidence

Only one in five (**19.6%**) of respondents express strong confidence in their non-human IAM practices, while 23.7% report little to no confidence.

Rotation Risks

The lack of regular key rotation is the most significant threat to non-human identity security, identified by **29.6%** of respondents, leaving organizations vulnerable to credential compromise.

Blind Spots

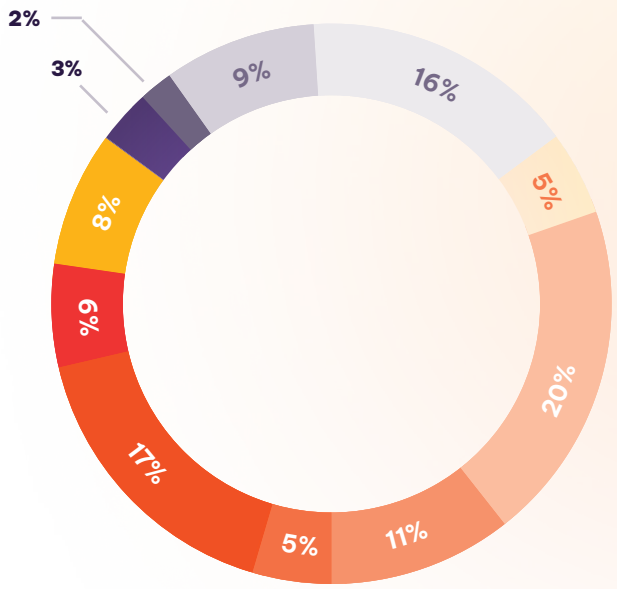
Nearly a quarter of respondents (**23.5%**) are unsure about the biggest threat to their non-human identities, indicating a concerning lack of awareness.

Demand for More

Six out of 10 (**59.8%**) respondents see value in a solution that simplifies non-human access management and introduces dynamic, ephemeral credentials.

Summary of (Human) Respondents

A total of 110 participants responded, representing a broad cross-section of roles within the IT and security sectors, including developers, IAM practitioners, security engineers, product managers, and executive-level professionals like CTOs and CSOs. The survey was distributed online, targeting professionals involved in cybersecurity, DevOps, and infrastructure operations. Respondents were asked a series of questions designed to assess their organization's maturity in managing non-human identities, the methods they employ, the challenges they face, and their confidence in current IAM practices. The results provide a comprehensive overview of how organizations are approaching non-human IAM in today's complex, multi-cloud environments.



What is your role?

- IAM Practitioner
- IS/IT Practitioner
- Developer
- Product Manager
- CSO/CISO
- Security Engineer/Architect
- Security (Individual Contributor)
- Infrastructure Operations
- CTO
- CIO
- Other

Survey Creation and Methodology

The survey was conducted to gather insights into the current state of non-human identity and access management (IAM) across various organizations. A total of 110 participants responded, representing a broad cross-section of roles within the IT and security sectors, including developers, IAM practitioners, security engineers, product managers, and executive-level professionals like CTOs and CSOs. The survey was distributed online and in person, targeting professionals involved in cybersecurity, DevOps, and infrastructure operations. Respondents were asked a series of questions designed to assess their organization's maturity in managing non-human identities, the methods they employ, the challenges they face, and their confidence in current IAM practices.

A Deeper Dive into the Big Takeaways

Key Finding 1: Non-Human IAM Maturity Lags Behind User IAM

There was a time when sticky notes and clunky spreadsheets were the go-to methods for tracking user passwords and managing permissions. Fortunately, those days are mostly behind us, with more sophisticated solutions like SSO, MFA, IAM, and Zero Trust now in place. But when it comes to non-human identities, it's a different story. Many organizations are still playing catch-up.

NHIs need to communicate securely and efficiently to do their jobs, yet today's IAM approaches are often a patchwork of systems that lead to inefficiencies and security gaps. The survey data reflects this struggle: only 11.5% of respondents believe their organizations are more mature in managing non-human IAM compared to user IAM, with 29.8% believing they are on par. Meanwhile, 19.2% of respondents aren't even sure how to gauge their maturity in this area. This uncertainty suggests that many organizations are still figuring out where they stand—or are aware they have gaps but haven't fully addressed them.

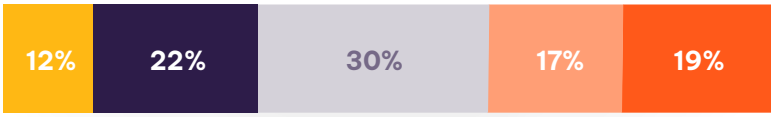
This isn't just a minor oversight. NHIs often interact with an enterprise's most sensitive data and critical systems. As businesses expand their digital ecosystems, the number and complexity of these identities are growing rapidly. This makes it even more crucial to close gaps and ensure non-human IAM is as robust as user IAM.

The challenge is compounded by the fact that non-human identities operate across a variety of environments – cloud, on-premises, SaaS, and more. Each environment has its own set of tools, standards, and IAM practices, making it difficult to maintain a consistent security posture across all platforms. This fragmentation can lead to security gaps, where certain non-human identities may be over-privileged, under-protected, or simply unmonitored.

The survey results make it clear: there's a lot of work to be done. It's becoming increasingly imperative for organizations to move beyond ad hoc solutions and develop comprehensive strategies for managing non-human IAM.

As we explore the next findings, we'll see how these gaps in non-human IAM maturity play out in other critical areas. The following findings will delve deeper into these issues, revealing where organizations are struggling, where they're making progress, and what needs to happen next to bridge these gaps.

> “Many organizations are still figuring out where they stand—or are aware they have gaps but haven't fully addressed them.



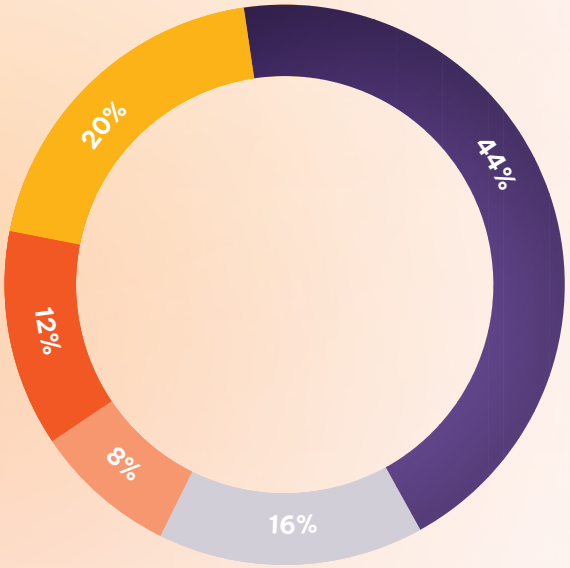
How would you compare your organization's maturity of Non-Human/ Workload Identity and Access Management (IAM) compared to User IAM?

- More mature in Non-Human IAM
- More mature in User IAM
- Equally mature in both Non-Human IAM and User IAM
- Insufficient maturity in both Non-Human IAM and User IAM
- Not sure

7 Common Places Where Non-Human Identity Credentials Are Exposed

1. Environment Variables
2. Configuration Files
3. Log Files
4. Container Images
5. Application Memory
6. Backup Files
7. Temporary Files

Key Finding #2:
Confidence in Current IAM Methods is Limited



How confident are you in your current methods to securely manage non-human workload identities and ensure that only authorized workloads are accessing your data and services?

- Somewhat confident
- Not at all confident
- Very confident
- Not sure
- Not very confident

Confidence in current methods of managing non-human identities and access is surprisingly low, according to recent findings. Only 19.6% of respondents express a high level of confidence in their organization's ability to securely manage non-human workload identities. This lack of confidence highlights a critical issue: organizations are aware of the vulnerabilities but are uncertain about how to effectively address them. The majority of respondents – over 80% – indicated some degree of uncertainty or lack of confidence.

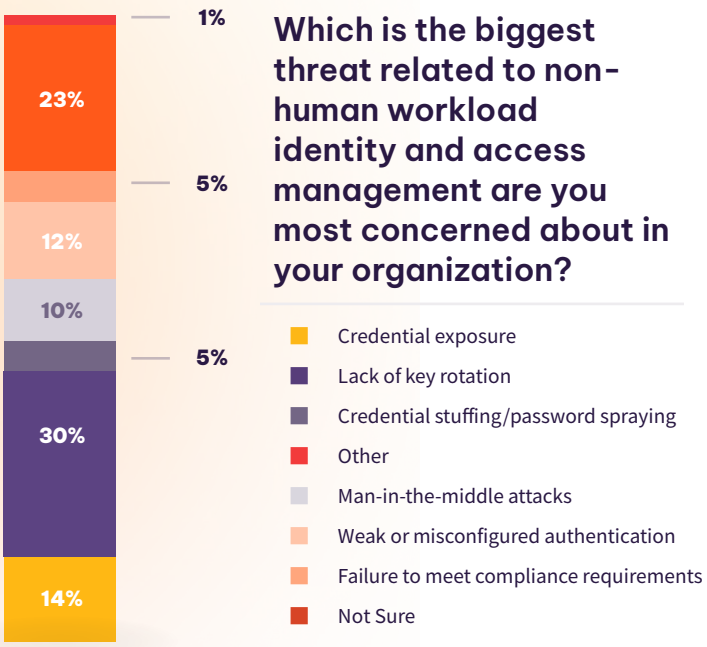
This limited confidence is not without reason. Managing non-human identities, which include applications, services, and automated processes, presents unique challenges that differ markedly from user IAM. These identities are often more dynamic, with frequent changes in access needs, making them harder to monitor and secure.

Additionally, the widespread use of static credentials, such as hard-coded API keys and tokens, adds another layer of risk. Since these credentials often have long lifespans and are stored in multiple locations, they become prime targets for exploitation.

An operational challenge also emerges concerning non-human IAM: determining which team should have stewardship. While this survey didn't specifically address personnel and operational oversight, anecdotally, we've heard of ambiguity regarding who should own NHI security – with both the cloud security team and the traditional IAM team being viable candidates. Each group has a case for taking ownership, which could lead to confusion and inefficiencies if not clearly defined.

The ambiguity in leadership, coupled with reliance on outdated practices like manual credential management and a general lack of awareness, likely contributes to the overall lack of confidence reported by respondents. The absence of stringent compliance requirements that address non-human identities with the same rigor as human identities may also be playing a role, as we'll explore later.

Key Finding #3:
Lack of Key Rotation is the Top Threat



Among the various threats related to non-human workload identity and access management, the lack of key rotation emerged as the top concern, with 29.6% of respondents identifying it as their primary worry. In today's IT environments, static, long-lived credentials can become significant vulnerabilities if not regularly rotated or replaced with short-lived tokens that initiate just-in-time access.

Key rotation in IT environments is complex. For NHIs – like applications, scripts, and services – keys are often deeply embedded within automated processes, making the rotation process delicate. A poorly executed key rotation can disrupt critical services, leading to downtime or leaving systems temporarily unprotected.

Consider a large enterprise managing hundreds of APIs and services across multiple cloud environments. Each service uses keys or tokens to authenticate and communicate securely. If even one of these credentials remains unchanged for too long, it could be discovered and exploited by attackers, granting them access to sensitive systems. Regular key rotation is crucial to minimize the window of opportunity for potential breaches.

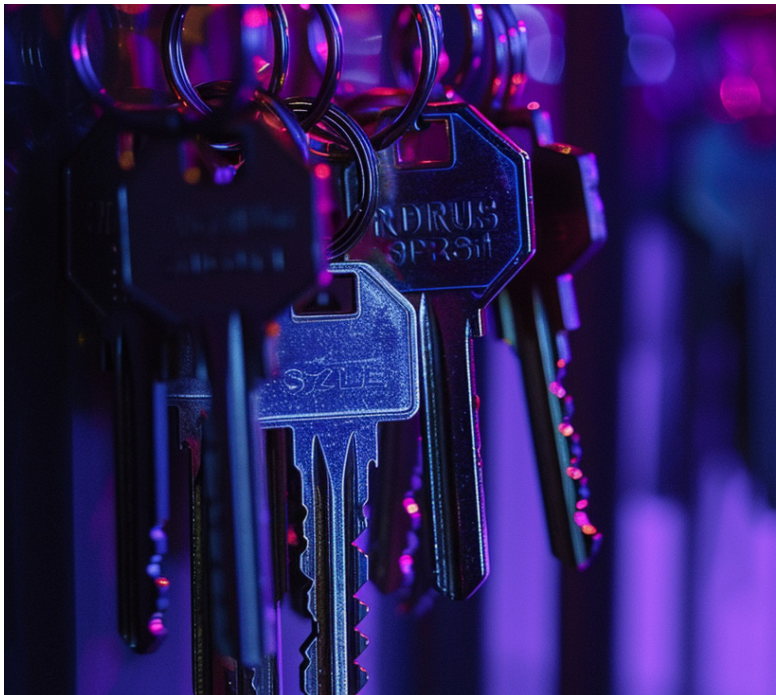
However, key rotation isn't the only concern. The survey also highlighted other significant threats, such as credential exposure, cited by 13.6% of respondents. Credential exposure occurs when keys or tokens are inadvertently shared, stored insecurely, or intercepted by malicious actors.

Weak or misconfigured authentication, identified by 12.3% of respondents, was another concern. This issue arises when strong credentials or secure token-based authentication aren't consistently applied, leaving non-human identities, like service accounts or APIs, vulnerable to unauthorized access and lateral movement within a network.

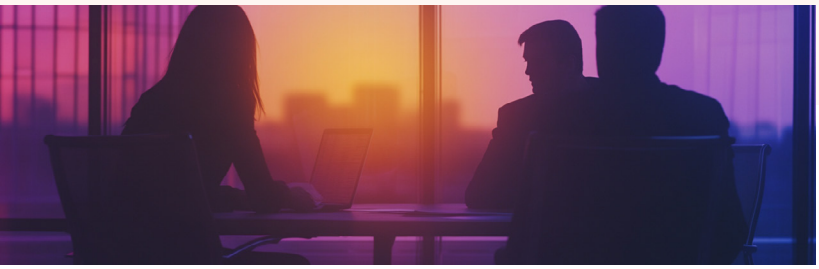
Meanwhile, 5% of respondents pointed to growing compliance pressures. Although not yet as influential as human identity regulations, this concern is gaining traction as industry standards increasingly recognize non-human identities. Updated guidance from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, for example, now emphasizes the need for comprehensive identity and access management (IAM) that includes non-human identities, reflecting their critical role in secure environments.

As these standards evolve, compliance-related concerns around non-human identities are likely to rise significantly. Organizations will need to demonstrate robust mechanisms for securing non-human identities, not just human ones.

It is worth noting that the second-highest percentage of responses (23.5%) indicated uncertainty about the biggest threat to their non-human workload identities. This highlights a significant lack of awareness around potential risks such as credential exposure, weak authentication, and key management failures, leaving organizations vulnerable to overlooked security gaps.



Key Finding #4:
Risky Practices Persist



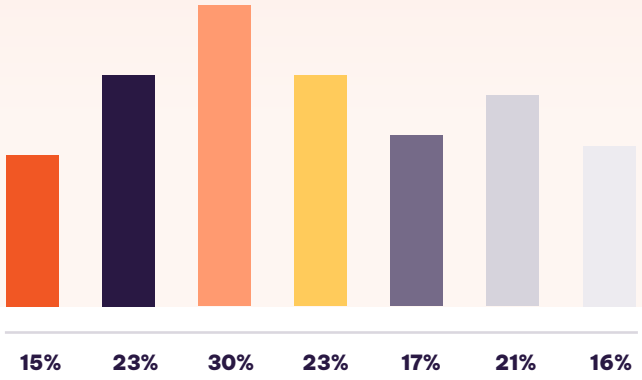
Despite the growing awareness around securing non-human workload identities, many organizations are still clinging to risky practices that leave the door wide open for attackers. These habits, often born out of convenience or the comfort of legacy systems, create gaping vulnerabilities that could easily compromise the entire IT environment.

One particularly concerning practice revealed in our survey, where respondents could select all that applied, is storing long-term access secrets in code, reported by 30.9% of respondents. While hard-coding credentials into scripts or environment variables may streamline deployment, it also introduces a significant risk. If the code is compromised, perhaps through a breach of the source code repository, attackers could gain access to critical systems. This practice not only increases the likelihood of credential exposure but also complicates the process of rotating secrets, potentially disrupting important services.

Additionally, 23.7% of respondents acknowledged sharing keys through less secure methods, such as copying and pasting via emails or messaging apps. This practice poses a risk because unencrypted credentials could be intercepted, leading to unauthorized access and potential data breaches.

The survey also highlighted that a similar percentage of respondents lack a systematic approach to tracking and rotating secrets. Without a structured process, organizations may lose visibility into who has access to critical systems, creating potential vulnerabilities. The absence of regular key or secret rotation can leave organizations exposed to threats that could have been mitigated.

Another area of concern is the reliance on manually updated spreadsheets to track access information, mentioned by 15.46% of respondents. While spreadsheets may seem like a practical solution, they are prone to human error, lack version control, and may not be adequately secured. This can lead to outdated or incorrect information and, in some cases, unmonitored exposure of sensitive systems.



Does your organization currently rely on any of the following practices for managing non-human workload identity and access? (Select all that apply)

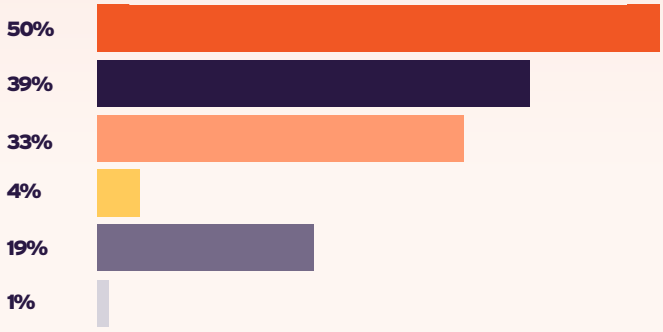
- Using manually updated spreadsheets to track access information
- Sharing keys through copying and pasting, possibly via emails or messenger
- Storing long-term access secrets in code (i.e., environment variables)
- Lacking a systematic approach to secrets tracking and rotation
- Insufficient access analytics or visibility
- None of the above
- Not sure

SLIDESHOW

Breach Files: Non-Human Identity Edition

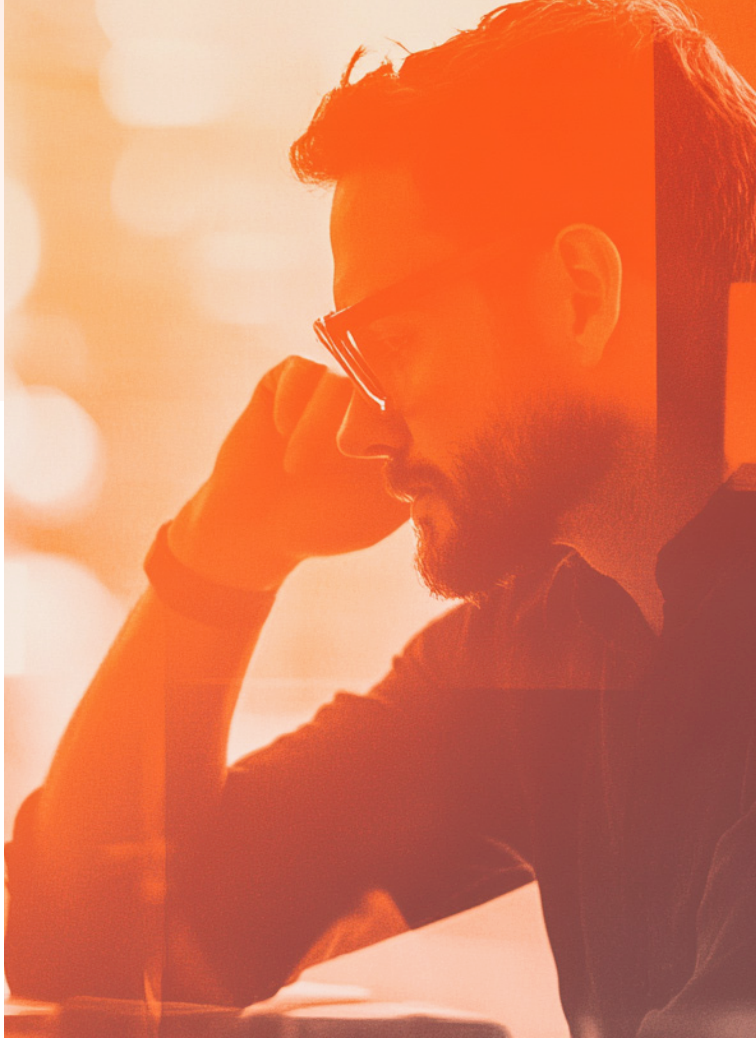
Identity management has traditionally focused on human users — understandably so, as people have long been considered the biggest security risk and are responsible for many of the largest data breaches in history. But as digital transformation has advanced, non-human identities have rapidly grown in both scale and importance — becoming a significant source of data-loss incidents themselves.

SEE REAL-LIFE EXAMPLES OF NHI COMPROMISES



How do you currently manage the authentication and authorization of non-human workloads [aka applications, scripts, and services] in your organization? (Select all that apply)

- Using cloud provider IAM (e.g., AWS/Microsoft Azure/Google Cloud, or similar)
- Password manager
- Not sure
- Spreadsheet/document
- Other
- Using secrets managers (e.g., HashiCorp Vault, Akeyless, or similar)



Key Finding #5: Mixed Methods for Managing Non-Human Identities

While the previous finding highlighted ongoing risky practices, this survey also reveals that organizations are attempting to tackle these challenges, albeit with mixed results. As companies recognize the importance of securing non-human identities, they're experimenting with various methods – some more effective than others.

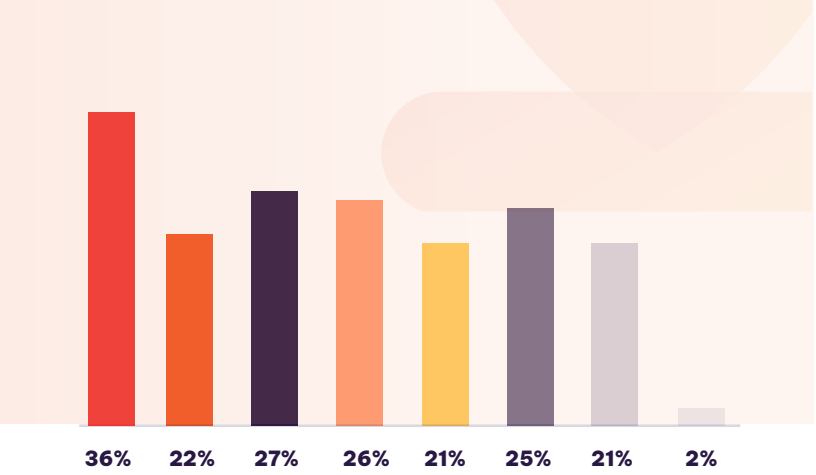
Over half of organizations (50.5%) are leveraging cloud provider IAM tools like AWS IAM, Azure AD, or Google Cloud IAM to manage non-human identities. These tools, while powerful within their respective ecosystems, often struggle with cross-platform integration, as we'll discuss in the next section, potentially leading to inconsistent security practices across hybrid and multi-cloud environments.

Interestingly, a significant portion of respondents (38.8%) reported using secrets managers, such as HashiCorp Vault or Akeyless, to manage authentication and authorization of non-human workloads. While secrets managers provide a more secure alternative to older methods, they are not without risks. Without proper configuration, regular updates, and vigilant oversight, secrets managers can become a single point of failure, exposing sensitive credentials if compromised.

However, the survey also uncovered that some organizations are still relying on less secure methods. For instance, one-third of respondents are using password managers. While typically designed for human identities, some organizations may be using them to manage credentials for non-human identities as well. This approach, while better than manual tracking, may not be sufficient for the complex and dynamic nature of non-human identities, which require more specialized tools and operate across a different tech stack.

Additionally, 3.9% admitted to managing these critical identities using spreadsheets or documents – a method fraught with risks, including human error, lack of version control, and inadequate security measures. (Editor's note: This percentage differs from the previous finding, where 15.4% reported using spreadsheets to manage NHIs. The discrepancy likely stems from how the questions were asked – one focused on general risky practices, while this one specifically references current management methods.)

Lastly, the fact that 19.4% of respondents are unsure about how their organizations manage non-human identities suggests that non-human IAM may not yet be a top priority. This lack of clarity highlights the urgent need for more robust, unified solutions that can elevate non-human IAM to the same level of focus and control as user IAM.



What are the main challenges you face with managing non-human workload identities, secrets, and access across different environments (e.g., on-premises, cloud, SaaS services, and third-party APIs)? (Select all that apply)

- Achieving consistent access management in hybrid or multi-cloud environments
- Vendor lock-in from cloud provider's Workload IAM tools
- Over-reliance on static or long-lived credentials
- Requiring developers to code auth to company standards
- Moving to just-in-time credentials or ephemeral access
- Auditing access
- Not sure
- Other

Why Traditional Secrets Management Falls Short and What Organizations Are Doing About It

As organizations work to improve their confidence levels in managing non-human identities, they're exploring alternative approaches. Key points from Gartner's recent research report, Innovation Insight: Secrets Management Tools, highlight why these changes are necessary:

Long-Lived Credentials Are Risky

API keys, tokens, service account passwords, and other long-lived credentials pose significant security risks if not managed properly. Organizations are urged to seek alternatives that minimize the reliance on these static secrets.

Secrets Managers Have Gaps

Traditional secrets management tools often don't cover the entire lifecycle of workload identities and accounts. Organizations need additional tools to fill these gaps, ensuring a more secure and comprehensive approach to non-human identity management.

Consider Secretless Methods

Gartner recommends that organizations "evaluate alternative mechanisms that keep secrets away from workloads entirely." Moving toward secretless, just-in-time access methods is becoming a key strategy for reducing risk.

Disclaimer: Gartner does not endorse any vendor, product, or service mentioned in its research publications, and it does not recommend that technology users select only those vendors with the highest ratings or other designations

Key Finding #6: Challenges in Multi-Cloud Environments

As more organizations expand into hybrid and multi-cloud environments, they're discovering that managing non-human workload identities, secrets, and access across these diverse platforms is no easy task. In our survey, 35.7% of respondents identified maintaining consistent and secure access management as their top challenge in these environments.

The challenge stems from juggling various identity and access management (IAM) tools like AWS IAM, Azure AD, and Google Cloud IAM. While each tool works well within its own ecosystem, they don't always play nicely together, leading to potential security gaps where workloads might be over-privileged or under-protected.

Another significant concern, raised by 26.7% of respondents, is the reliance on static, long-lived credentials. Though easy to implement, these credentials are risky, as they become prime targets for attackers over time. Shifting toward dynamic, short-lived credentials that rotate automatically is increasingly seen as essential for reducing these risks.

Additionally, just over a quarter (25.7%) of respondents noted the burden on developers to code authentication according to company standards. This responsibility often pulls developers away from innovation, forcing them to focus on managing credentials – a task that's better suited to security teams, ideally with automation in place to maintain strong credential hygiene.

Finally, roughly one in four respondents (24.8%) highlighted the difficulty of auditing access across multi-cloud environments. Without comprehensive auditing, organizations struggle to detect suspicious activities or ensure compliance, leaving them exposed to preventable breaches.

Key Finding #7: High Demand for Simplified Non-Human IAM Solutions

As organizations wrestle with the growing complexity of managing non-human identities across diverse environments, it's no surprise there's a strong push for streamlined, comprehensive solutions. Our survey reveals that 59.8% of respondents see clear value in a solution that simplifies non-human access management across cloud, SaaS services, and third-party APIs. When you add in the 33.7% who are unsure, it becomes clear that 93.5% of respondents recognize the need for a better approach, even if they're still figuring out exactly what that looks like.

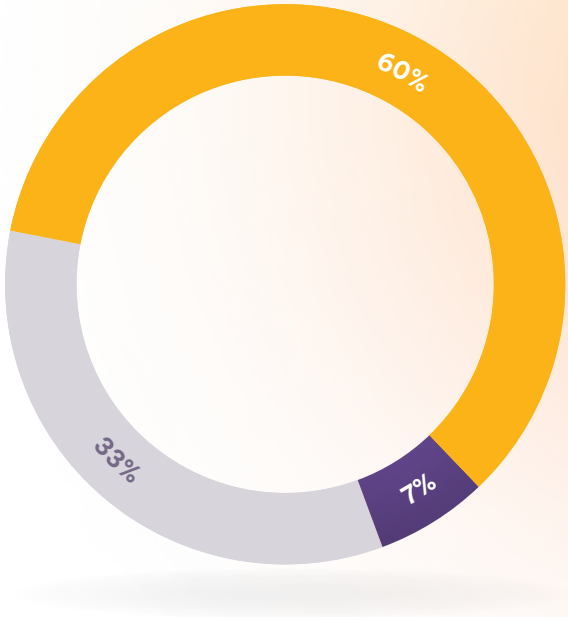
Remember when you cajoled your car into starting up with the promise of a little TLC? IT and DevSecOps teams are, slowly but surely, having a similar moment with their non-human identities. They're starting to understand these digital assets are more than just background support – they're critical components of their IT ecosystems, requiring more than surface-level security.

The data makes it clear that traditional methods of managing non-human identities – such as using long-lived credentials or relying on manual processes – are no longer sufficient in today's fast-paced, multi-cloud environments. These approaches are increasingly viewed as cumbersome and prone to errors, especially when it comes to maintaining consistent security across various platforms with different tools and standards.

The survey results point to a growing consensus: Businesses need a more streamlined and secure way to manage non-human identities that can keep up with the dynamic demands of modern IT infrastructure. This is where a comprehensive platform like Workload IAM can step in, offering a new and mature way forward.

By moving beyond traditional approaches, such a solution integrates best practices into a unified system that simplifies management and enhances security. It offers real-time policy enforcement, secretless access tokens, and automated credential management, all of which work together to minimize the attack surface and reduce operational overhead. Additionally, identity-based logging provides comprehensive visibility into the actions of non-human identities, which is essential for detecting and responding to security incidents promptly.

If you're not quite ready to dive into a full-fledged platform, there are still practical steps you can take right now to start improving your non-human identity management.



Would you see value in a solution that simplifies non-human access management across different environments (clouds, SaaS services, third-party APIs), handles workload authentication, authorization, and logging for you, and ensures dynamic, short-lived credentials for secure access?

Yes No Not sure

"

59.8% of respondents see clear value in a solution that simplifies non-human access management.

Conclusion: Bridging the Identity Divide

You can take actionable steps immediately to ensure your non-human identities get the same care and attention as your human ones. Here are some quick ideas to close out the survey:

Implement Automated Credential Rotation

Start automating the rotation of your most critical credentials to reduce the risk associated with static, long-lived credentials.

Enhance Inventorying, Logging, & Monitoring

Set up comprehensive logging for all non-human identities and ensure you have real-time monitoring to detect unusual activities.

Tighten Access Controls

Audit existing non-human identities and reduce over-privileged accounts to ensure they only have the access necessary for their tasks.

Educate and Align Teams

Make sure both your security and development teams understand the risks associated with non-human identities and are trained on best practices for managing them.

Experiment with Secretless Authentication

Begin piloting secretless authentication methods in lower-risk environments to see how they can fit into your broader security strategy.

Think you might be ready to dip your toes in workload IAM to help you secure your non-human identities and more efficiently manage workload-to-workload access? Give Aembit a try for free today.

Manage Access, Not Secrets.

Aembit is the Workload Identity Platform that lets every business safely build its next generation of applications by inherently trusting how it connects to partners, customers, and foundational services. Aembit provides seamless and secure access from your workloads to the services they depend on, like APIs, databases, and cloud resources, while simplifying application development, delivery, compliance, and audit. For more information visit aembit.io


aembit