The State of Non-Human Identity Security

Astrix

cloud security alliance®

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Marina Bregkou
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Graphic Designer

Claire Lehnert

Special Thanks

Danielle Guetta and Tal Skverer

About the Sponsor

Astrix Security is the first solution built to secure and manage the lifecycle of NHIs, helping enterprises like NetApp, Priceline, Figma and Agoda control their NHI attack surface and prevent supply chain attacks. The platform provides continuous discovery, posture management, threat detection and automatic remediation for NHIs across business and engineering environments.

Table of Contents

Executive Summary

Non-human identities (NHIs) such as bots, API keys, service accounts, OAuth tokens, and secrets are indispensable for automating tasks, enhancing efficiency, and driving innovation within organizations. However, these NHIs also present unique security challenges. This executive summary highlights the key findings, challenges, and recommendations derived from the survey results.

1. **High Anxiety, Low Confidence in NHI Security**
   - Only 15% of organizations feel highly confident in preventing NHI attacks, compared to 25% for human identities. This disparity is due to the vast number of NHIs, which can outnumber human identities by a factor of 20 to 1.
   - 69% of organizations express moderate to high concern about NHIs as an attack vector, indicating awareness of the risks but a lack of confidence in current security measures.
2. **Struggles with Fundamental NHI Security Practices**
   - Managing service accounts is a significant challenge, with 32% of organizations highlighting it as a major pain point.
   - Auditing and monitoring (25%), access and privilege management (25%), discovering NHIs (24%), and policy enforcement (21%) are cited as critical yet challenging areas.
   - Visibility into third-party vendors connected by OAuth apps is limited, with 38% of organizations reporting no or low visibility.
3. **Challenges with Managing Permissions and API Keys**
   - Organizations face difficulties managing permissions and API keys, particularly with existing service accounts, highlighting the issue of tech debt.
   - Only 20% have formal processes for offboarding and revoking API keys, and even fewer have procedures for rotating them.
   - Manual handling of API keys leads to delays and inefficiencies, with nearly 40% of organizations taking weeks or more to offboard keys.
4. **Fragmented Security Approaches Lead to Incidents**
   - Many organizations rely on a mix of security tools not specifically designed for NHIs, leading to a lack of cohesion and effectiveness.
   - Common causes of NHI security incidents include lack of credential rotation (45%), inadequate monitoring (37%), and overprivileged accounts (37%).
5. **Increasing Investment in NHI Security**
   - There is a promising trend towards increased investment in NHI security capabilities, with 24% of organizations planning to invest within the next six months and 36% within the next 12 months.

Key Findings

Non-human identities (NHIs) like bots, API keys, service accounts, OAuth tokens, and secrets are essential for keeping today's organizations running smoothly. They automate tasks, boost efficiency, and drive innovation. But with these benefits come unique security challenges. NHIs operate 24/7, handle sensitive data, and perform actions at lightning speed, making them prime targets for cyberattacks.

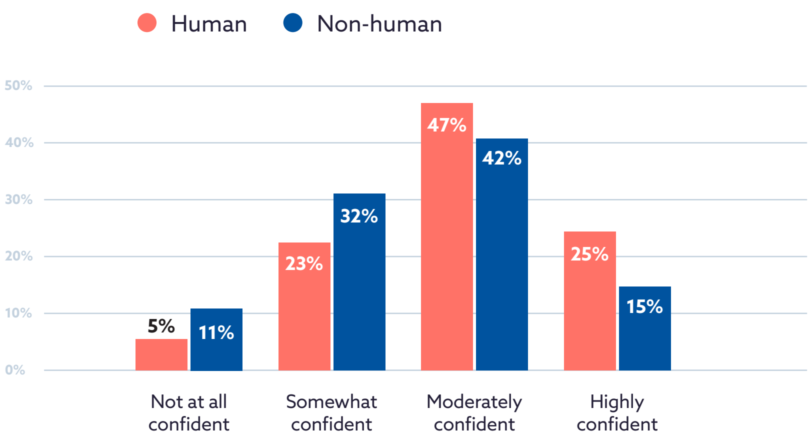
To understand how organizations are handling NHI security, a survey was conducted. The survey provides insights into their opinions about their current NHI security, the obstacles they're facing, and the strategies and tools they're using. The aim is to shed light on the current state of NHI security and identify areas for improvement. These are some of the key findings and themes from the survey results.

Key Finding 1:
High Anxiety, Low Confidence When Securing NHIs

Confidence in preventing NHI attacks

Organizations are grappling with their current NHI security strategies. Only 15% of organizations feel highly confident in their ability to prevent an attack through NHIs. In comparison, confidence in preventing an attack through human identities is higher, with 25% expressing high confidence.

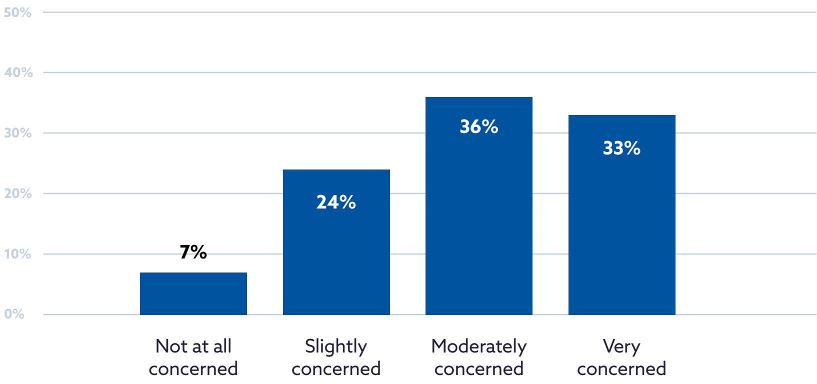
Confidence levels in human identity vs NHI attack prevention



This means that only 1.5 out of 10 organizations are highly confident about NHI security, compared to nearly 1 in 4 for human identity security. This disparity could be due to the sheer number of NHIs in their environment, which often outnumber human identities by a factor of 20 to 1.

NHI as an attack vector

Concern levels about NHI as an attack vector



The high volume of NHIs significantly amplifies the security challenges organizations face. Each NHI can potentially access sensitive data and critical systems, increasing the attack surface exponentially. Without adequate visibility and control over these NHIs, the risk of security incidents rises. Organizations' lack of confidence suggests their current NHI security methods are lagging behind their human identity security methods.

The data further reveals that 69% of organizations are moderately-to-very concerned about NHIs as an attack vector.

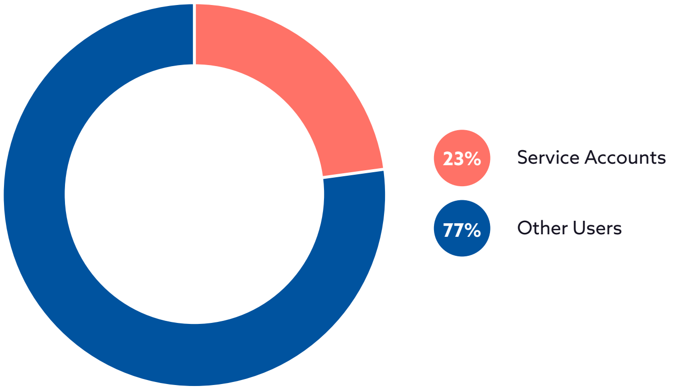
When combined with the lack of confidence in their NHI security methods, a clear picture forms. Organizations are aware of the security implications of NHI, but may not have the capabilities in place to prevent such attacks. This likely stems from issues with current strategies, insufficient tooling, and deficient processes that hinder effective NHI security management. Without the proper tools and cohesive strategies, organizations are left vulnerable and anxious while waiting for an attack. Refining their current strategy, processes, and tooling can go a long way in reducing this stress and improving their ability to secure NHIs against potential cyber threats.

Key Finding 2:

Struggling with the Basics of NHI Security

Top challenges in NHI security

Users in Snowflake Environments



With the high rates of concern regarding NHI attacks, it was important to dig deeper into the specifics. One of the biggest pain points for organizations is managing service accounts. This is a significant challenge, with

> 32% of organizations citing service accounts as one of the most challenging aspects to manage.

In Snowflake environments, 23% of users are actually service accounts, underscoring the scale of this issue. Service accounts, due to their elevated privileges and widespread usage, represent a substantial security risk if not properly managed.

Beyond service accounts, organizations struggle with fundamental security practices related to NHIs. Auditing and monitoring (25%), access and privileges (25%), discovering NHIs (24%), and policy enforcement (21%) are all cited as major challenges. These foundational security practices are essential for maintaining a secure environment, yet many organizations are finding them difficult to manage effectively. The inability to manage these basics can lead to significant security gaps, making organizations more vulnerable to attacks.

Most challenging aspects of NHI management

32%	Service accounts
25%	Auditing and Monitoring
25%	Access and privileges
24%	Discovering NHIs
21%	Policy enforcement
21%	Managing the secrets lifecycle
20%	IAM roles
19%	Vendor-owned APIs
18%	Managing requests for third-party tools and services
16%	Managing credentials
16%	Integration and interoperability
11%	Categorizing NHIs
9%	Procuring, tracking, terminating
7%	AuthN (Authentication)
7%	AuthZ (Authorization)
6%	Scalability

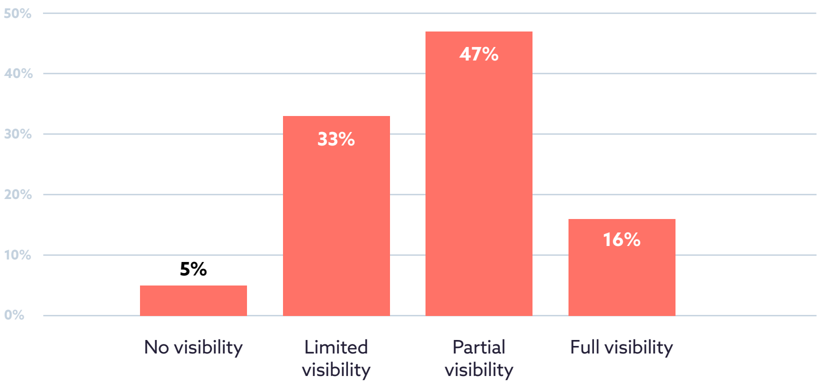
Visibility into third-party vendors

Another significant concern is the struggle to gain visibility into third-party vendors connected by OAuth apps. The survey indicates that

> 38% of organizations report no or low visibility into third-party vendors connected by OAuth apps,

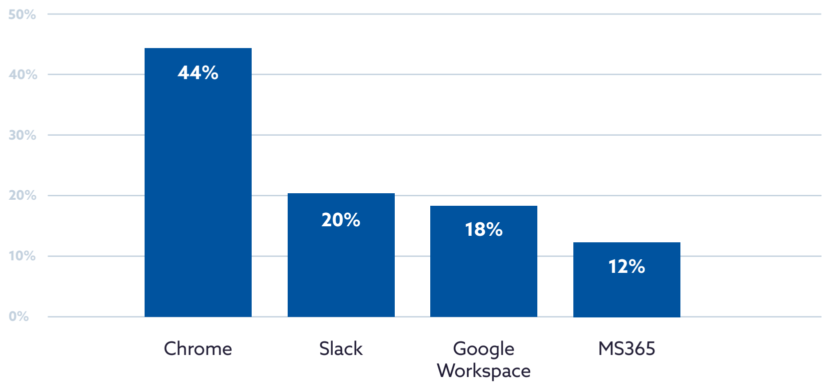
and another 47% have only partial visibility. This lack of visibility is alarming because it means that organizations cannot fully monitor or control the access and activities of these third-party applications, which is another foundational capability needed for effective NHI security.

Visibility levels into third-party vendors connected by OAuth apps



This becomes particularly important because a substantial percentage of third-party apps come from untrusted vendors. Untrusted vendors include individual developers without adequate security protocols, small companies, and those based in unconventional locations that may not adhere to standard security practices. Specifically, 44% of third-party apps found in Chrome are from untrusted vendors, 20% in Slack, 18% in Google Workspace, and 12% in MS365. Without adequate visibility, organizations are unable to effectively manage these risks, leaving them exposed.

Percentages of Untrusted Third-Party Vendors by Marketplace

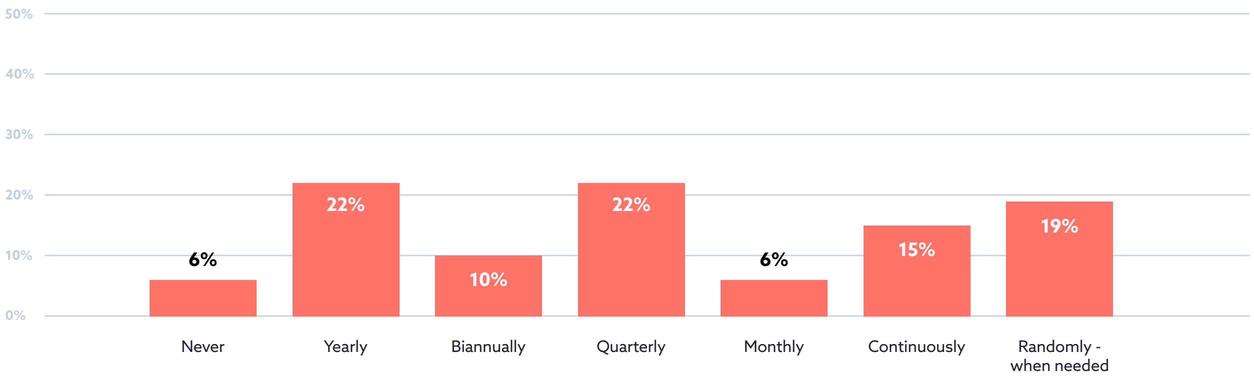


Reactive security leads to security gaps

The downstream effect is that the process of managing NHI security is reactive. Only 22% of organizations review permissions for service accounts yearly, while 19% do so randomly, when needed. This indicates that organizations are likely addressing service account permissions to prepare for an audit or upon request. The manual and tedious nature of this process further complicates proactive management, increasing the risk of oversights. Combined with the challenge of basic NHI security, it becomes clear that organizations are struggling to take proactive measures, such as continuous monitoring and automated management, which are crucial for identifying and mitigating risks promptly. This deficiency leaves organizations vulnerable to potential attacks and also means that existing security measures are likely insufficient.

Without robust, automated solutions and systematic review processes, these organizations remain vulnerable to security incidents and face significant challenges in securing their NHIs effectively. By addressing these foundational issues, organizations can enhance their overall security posture and better protect against potential threats.

Frequency of review for service account permissions

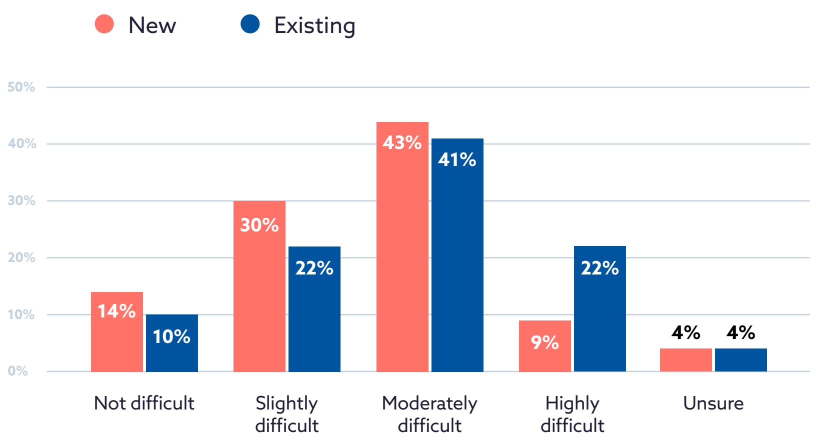


Key Finding 3:

Challenges with Managing Permissions and API Keys

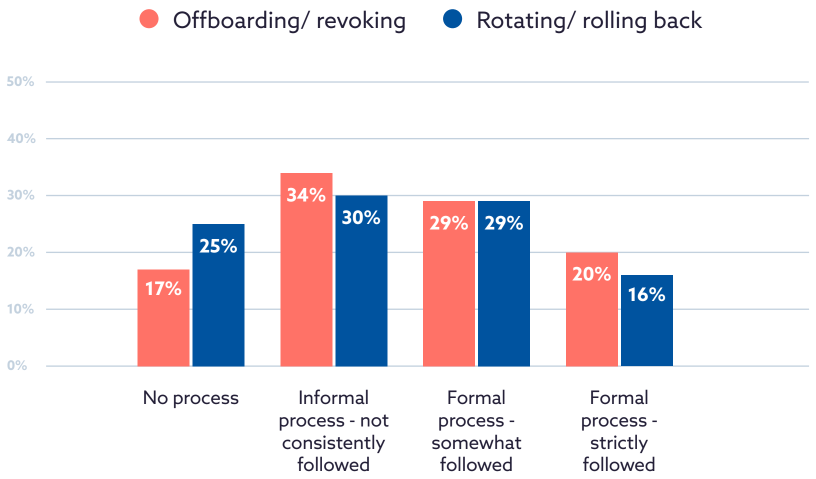
Difficulties with service accounts and tech debt

Difficulty levels of managing permissions for new versus existing service accounts



One of the significant struggles organizations face is managing permissions and API keys effectively. Survey data reveals that managing permissions is notably easier for new service accounts than for existing ones. Only 9% of organizations find it highly difficult to manage permissions on new accounts, whereas 22% find it highly difficult for existing accounts. This disparity highlights the issue of tech debt, where retroactive changes to permissions are more cumbersome and error-prone compared to initial setups. Such difficulties often lead to gaps in security as organizations struggle to keep up with evolving requirements and threats.

Type of process for API key offboarding/revoking versus rotating/rolling back



Managing and offboarding API keys

The management of API keys is another critical area where organizations falter.

> Only 20% have a formal process for offboarding and revoking API keys, and even fewer (16%) have a process for rotating or rolling back API keys.

This lack of formalized procedures means that steps are often skipped, or processes are not followed strictly, resulting in a redundant attack surface. When API keys are not properly offboarded, revoked, or rotated, they can remain active and potentially exploitable, creating significant security risks.

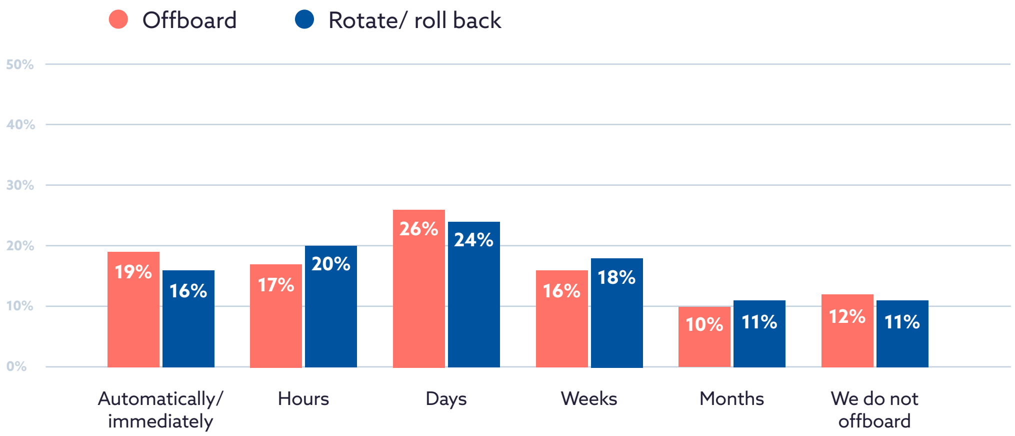
Manually offboarding API keys leads to long timelines

Only 19% of organizations have automated processes for offboarding, and 16% for rotating/rolling back API keys.

This manual handling exacerbates the issue, as organizations may not know the full impact of changes, leading to uncertainties about what might break or what systems might be affected.

Overall, these findings point to a critical need for organizations to develop and adhere to formalized, automated processes for managing permissions and API keys. Without such measures, organizations remain vulnerable to potential security breaches and inefficiencies. Implementing automated solutions can streamline these processes, reduce human error, and ensure that all necessary steps are consistently followed, thereby enhancing the overall security posture.

Timeline for API key offboarding versus rotating/rolling back



The manual nature of managing API keys leads to significant delays and inefficiencies.

The survey shows that nearly 40% of organizations take weeks or more to offboard API keys, with 26% taking days, and 10% taking months.

Similarly, 24% take days, and 18% take weeks to rotate or roll back API keys. Only a small fraction of organizations can handle these processes automatically or immediately, highlighting the need for automation. With the correct tooling, specifically designed for NHI security, these processes can be significantly streamlined, reducing both the time, manual workload, and risk involved.

Overall, these findings point to a critical need for organizations to develop and adhere to formalized, automated processes for managing permissions and API keys. Without such measures, organizations remain vulnerable to potential security breaches and inefficiencies. Implementing automated solutions can streamline these processes, reduce human error, and ensure that all necessary steps are consistently followed, thereby enhancing the overall security posture.

Key Finding 4:

Fragmented Approaches Lead to Security Incidents

Current tooling is inadequate

The reason organizations are struggling with the basics of NHI security may stem from a fragmented approach to managing NHI security. Many organizations are not using tools specifically designed for NHI security. Instead, they are relying on a mix of various security tools that are not tailored to the unique challenges NHIs present.

For instance, 58% use Identity and Access Management (IAM) systems, 54% use Privileged Access Management (PAM), 40% use API security measures, 38% employ Zero Trust/Least Privilege strategies, and 36% use Secrets Management tools. While these tools are crucial for overall security, their application to NHIs is often indirect and not comprehensive. This piecemeal strategy results in a lack of cohesion and effectiveness, contributing to their struggle with basic NHI security practices, low visibility, and proactively addressing security gaps.

Solutions and strategies currently used to manage NHIs

58%	Identity and Access Management (IAM)	**35%**	Behavioral Analytics and Anomaly detection	**20%**	Custom Scripts/Tools
54%	Privileged Access Management (PAM)	**35%**	Auditing and monitoring	**18%**	Machine identity protection
40%	API security	**34%**	Cloud Access Security Broker (CASB)	**14%**	Robotic process automation(RPA)
38%	Zero trust/least privilege	**23%**	Workload identity management	**2%**	We do not use any specific technology
36%	Secrets Management tools	**22%**	Automated Discovery and Management tools		

The result is organizations are not just looking for a couple of capabilities but need a wide array of capabilities to support their NHI management.

Key security tool capabilities being sought include visibility into third-party vendors connected through OAuth apps (26%), management of the secrets lifecycle (26%), identity discovery (25%), management of API keys (23%), managing permissions (22%), tracking access behavior/anomaly detection (22%), and automating third-party connectivity (21%).

These mirror many of the challenges that were previously identified. This broad range of capability needs further suggests that current strategies and tools are insufficient for their security needs.

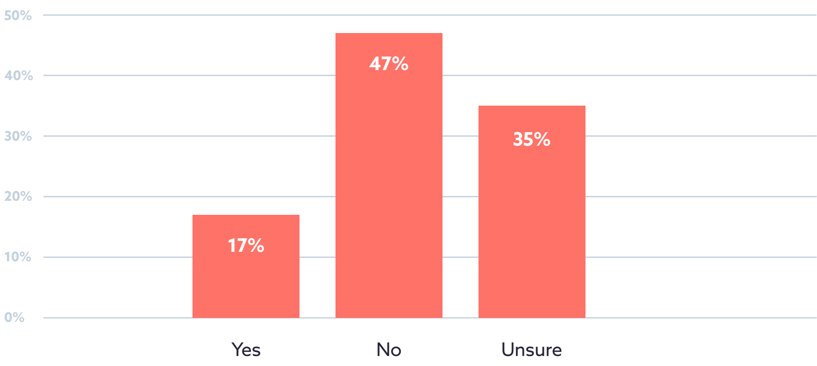
Most important security tool capabilities for NHI security

26%	Visibility into third-party vendors connected via OAuth apps
26%	Management of the secrets lifecycle
25%	Identity discovery
23%	Management of API keys
22%	Managing permissions
22%	Tracking access behavior/ anomaly detection
21%	Automate third-party connectivity
16%	Access control to sensitive information
15%	Automated provisioning and de-provisioning of identities
14%	Audit and logging of NHIs
14%	Identify owners and consumers of NHIs
13%	Policy enforcement
13%	Incident response and remediation
9%	Compliance management
7%	Scalability
1%	Use level of NHIs

NHI security incidents and causes

The security incidents experienced by organizations further highlight the inadequacies of their current strategies. While 17% of organizations were able to verify that they had an NHI-related security incident at their organization, another 35% were unsure. This means less than 50% of organizations can confidently say they have not experienced a NHI security incident.

Experienced security incidents related to NHI

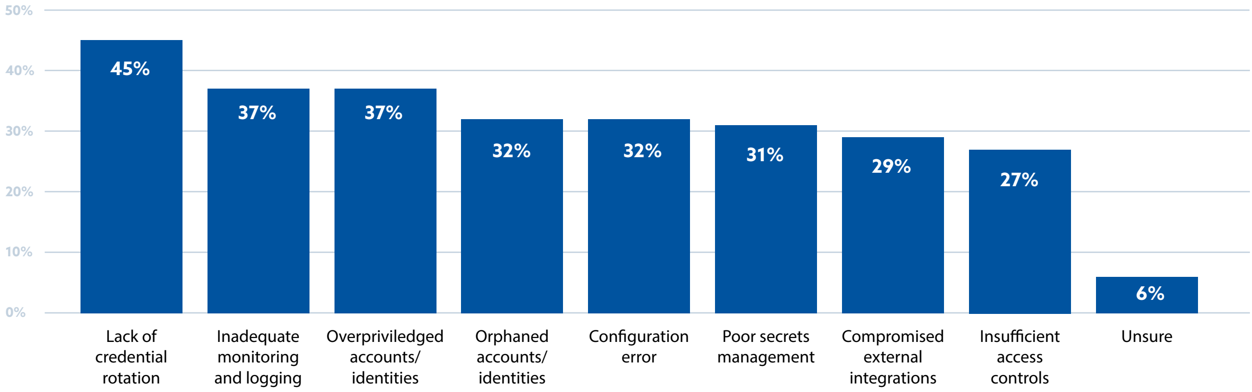


The high number of unsure responses could be a lack of insight, but could also represent further blindspots and challenges within NHI security management.

Common causes of NHI security incidents include a lack of credential rotation (45%), inadequate monitoring and logging (37%), and overprivileged accounts/identities (37%).

These issues mirror the challenges identified in the previous key finding and are exacerbated by the fragmented approach to NHI security. For example, 68% of tokens in GitHub environments have no expiry, and 64% of webhooks in GitHub are misconfigured, leaving significant vulnerabilities unaddressed.

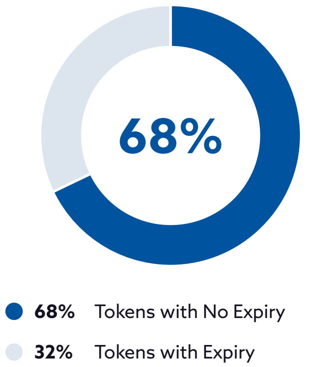
Causes of NHI security incidents



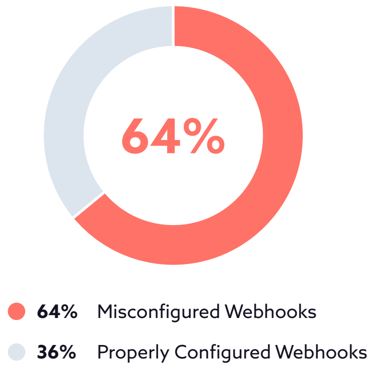
Poor secrets management (31%) is alarming, as each leaked secret is found in an average of 4.5 places, such as Slack chats and hardcoded locations.

Compromised external integrations (29%) and insufficient access controls (27%) further contribute to the risk landscape. These problems are a direct result of not having a unified, NHI-specific security strategy.

Tokens with vs without Expiry in GitHub Environments



Misconfigured vs Properly Configured Webhooks in GitHub



The implications of these findings are clear: organizations need to unify their NHI security strategies and invest in tools specifically designed for managing NHIs.

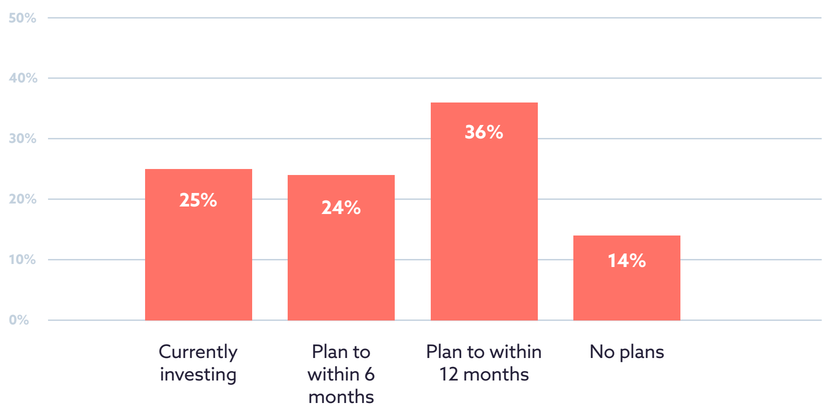
The current piecemeal approach leaves significant gaps in security coverage, making it difficult to address even the basics of NHI security. By adopting a more cohesive and targeted strategy, organizations can improve their visibility, reduce the risk of security incidents, and better manage their NHIs.

Key Finding 5:

Investment in NHI Security Capabilities on the Rise

Organizations are recognizing the critical importance of NHI security and are planning to significantly ramp up their investment in this area. The survey data reveals that only 14% of organizations currently have no plans to invest in NHI security capabilities. In contrast, 1 in 4 organizations are already investing in these capabilities, and the majority of the rest plan to do so soon, with 24% planning to invest within the next six months and 36% within the next twelve months.

Plans to invest in NHI security capabilities



This trend towards increased investment indicates that organizations are starting to take the concerns about NHI security and the struggles with basic security practices seriously. The current low levels of investment in NHI-specific tools have contributed to fragmented and inefficient security strategies. However, the planned increase in investment suggests that organizations are beginning to address these issues, moving away from piecemeal solutions towards more comprehensive, integrated strategies that effectively manage and secure NHIs.

Overall, the planned investments reflect a broader understanding of the significance of NHI security. As NHIs become increasingly integral to business operations, the associated risks cannot be ignored. By prioritizing NHI security through increased investment in the right tools and strategies, organizations can improve their security posture and better safeguard against potential threats.

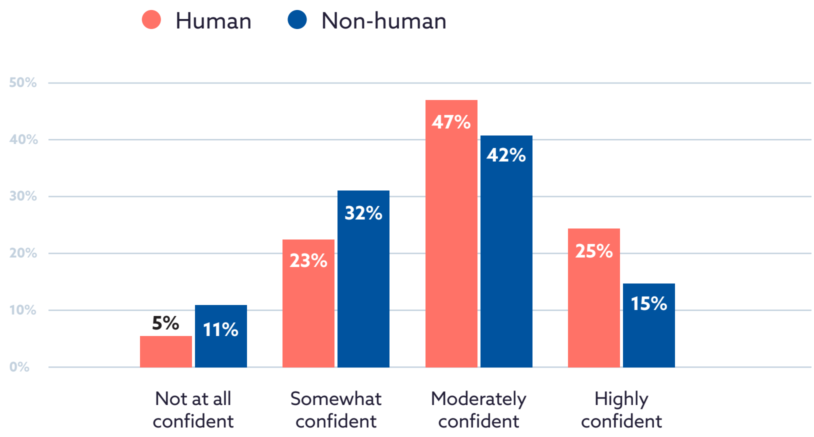
Conclusion

There is a promising shift as many organizations are planning to invest significantly in NHI security capabilities. This planned investment indicates a growing recognition of the importance of proactively addressing NHI security. By unifying their strategies, adopting NHI-specific tools, and automating critical processes, such as permission management and API key handling, organizations can enhance their security posture and better protect against evolving threats. This concerted effort will be crucial in closing the gaps identified in the survey and ensuring robust security for NHIs in the future.

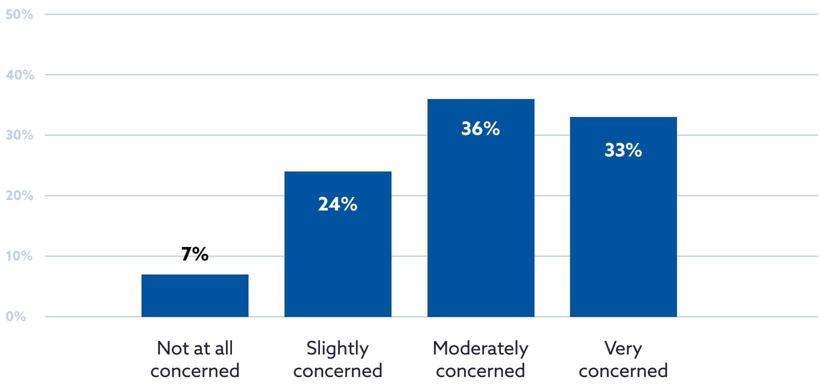
Full Survey Results

NHI Security Opinions, Concerns, and Challenges

Confidence levels in human identity vs NHI attack prevention



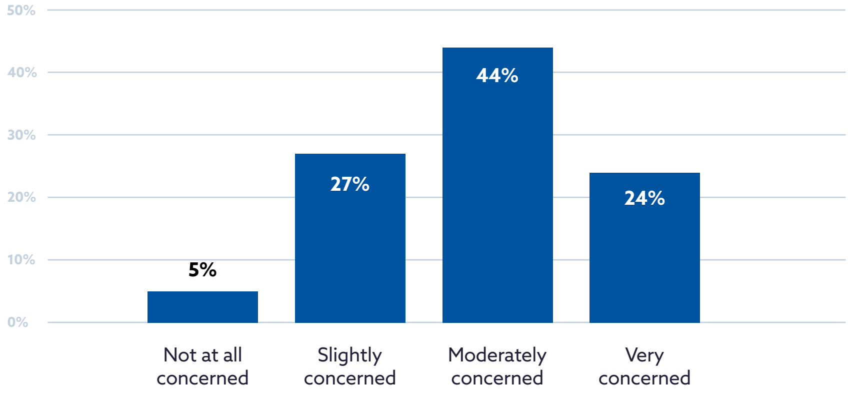
Concern levels about NHI as an attack vector



Most challenging aspects of NHI management

32%	Service accounts
25%	Auditing and Monitoring
25%	Access and privileges
24%	Discovering NHIs
21%	Policy enforcement
21%	Managing the secrets lifecycle
20%	IAM roles
19%	Vendor-owned APIs
18%	Managing requests for third-party tools and services
16%	Managing credentials
16%	Integration and interoperability
11%	Categorizing NHIs
9%	Procuring, tracking, terminating
7%	AuthN (Authentication)
7%	AuthZ (Authorization)
6%	Scalability

Concern levels about NHI access levels

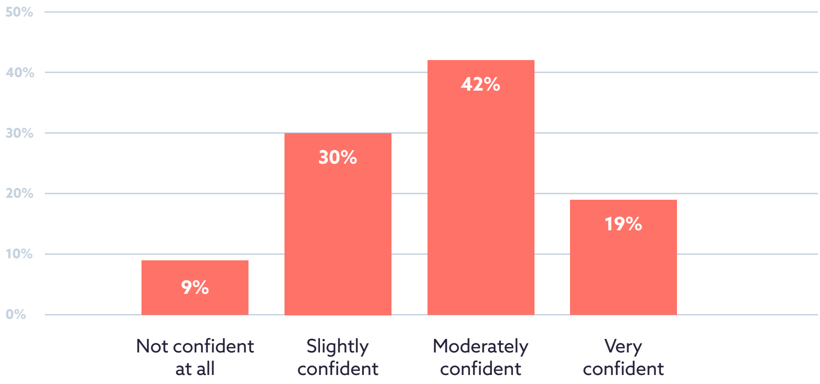


Most concerning NHI threats, risk, and vulnerabilities

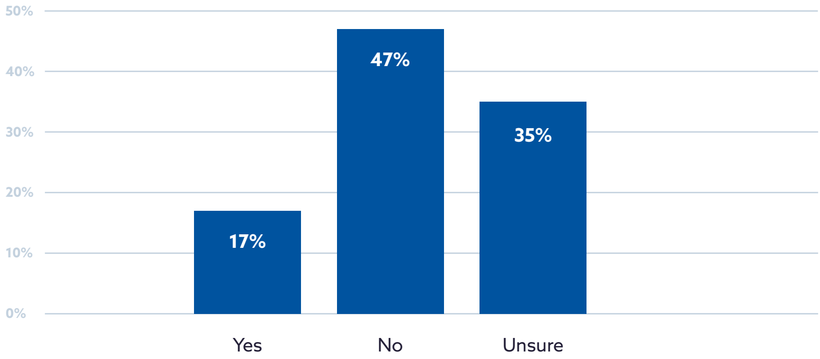
41%	Inadequate NHI Lifecycle Management
38%	Supply Chain Attacks via NHIs
33%	Overprivileged Accounts
33%	OAuth Phishing Attacks
31%	Insufficient NHI Offboarding Processes
26%	NHI Persistence, Backdoors, or Command and Control
26%	Failures in Securing and Monitoring NHIs
22%	Use of Deprecated Access Methods
16%	Malicious Suppliers
16%	Organization-Wide Access Risks

NHI Security Incidents

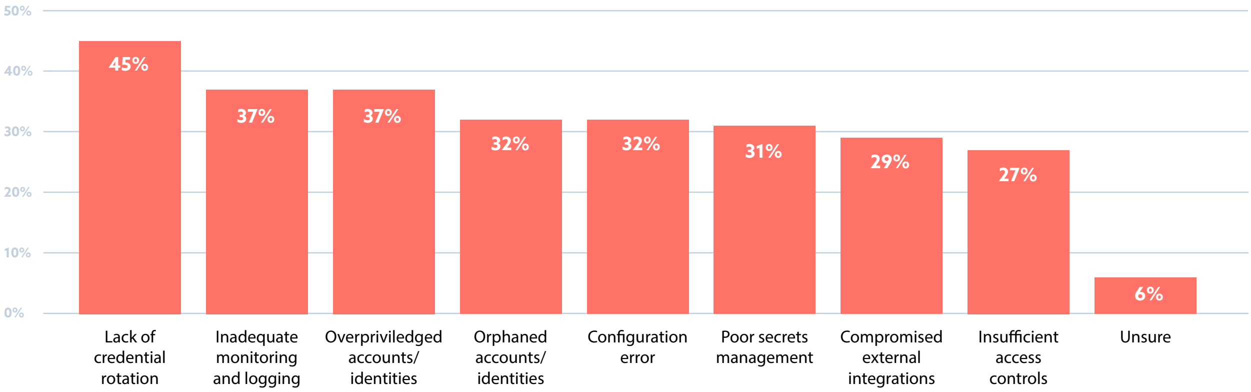
Confidence levels in responding effectively to NHI security incidents



Experienced security incidents related to NHI



Causes of NHI security incidents



NHI Security Strategy

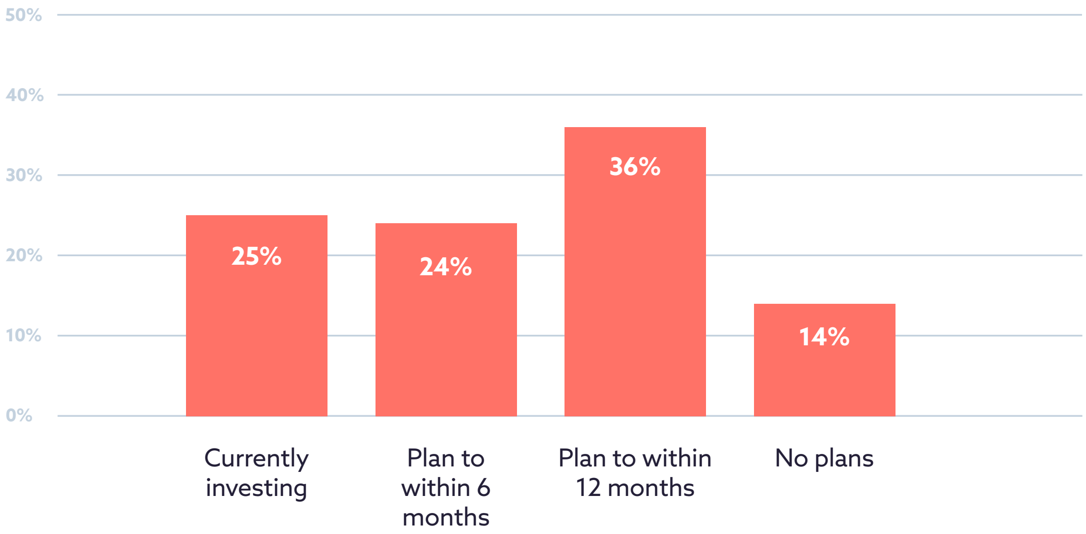
Solutions and strategies currently used to manage NHIs

58%	Identity and Access Management (IAM)
54%	Privileged Access Management (PAM)
40%	API security
38%	Zero trust/least privilege
36%	Secrets Management tools
35%	Behavioral Analytics and Anomaly detection
35%	Auditing and monitoring
34%	Cloud Access Security Broker (CASB)
23%	Workload identity management
22%	Automated Discovery and Management tools
20%	Custom Scripts/Tools
18%	Machine identity protection
14%	Robotic process automation(RPA)
2%	We do not use any specific technology

Most important security tool capabilities for NHI security

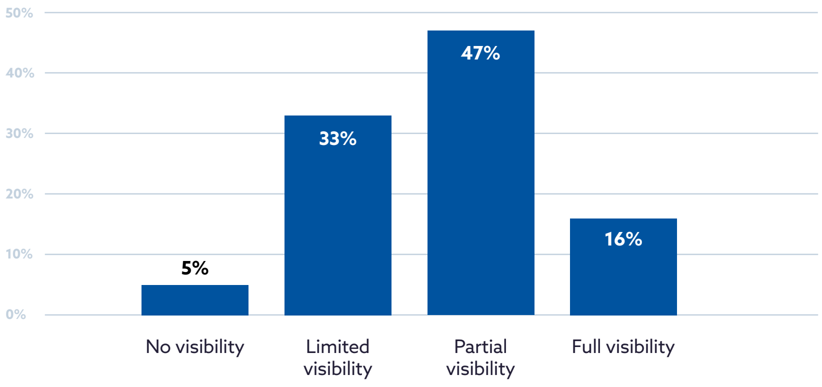
26%	Visibility into third-party vendors connected via OAuth apps
26%	Management of the secrets lifecycle
25%	Identity discovery
23%	Management of API keys
22%	Managing permissions
22%	Tracking access behavior/ anomaly detection
21%	Automate third-party connectivity
16%	Access control to sensitive information
15%	Automated provisioning and de-provisioning of identities
14%	Audit and logging of NHIs
14%	Identify owners and consumers of NHIs
13%	Policy enforcement
13%	Incident response and remediation
9%	Compliance management
7%	Scalability
1%	Use level of NHIs

Plans to invest in NHI security capabilities

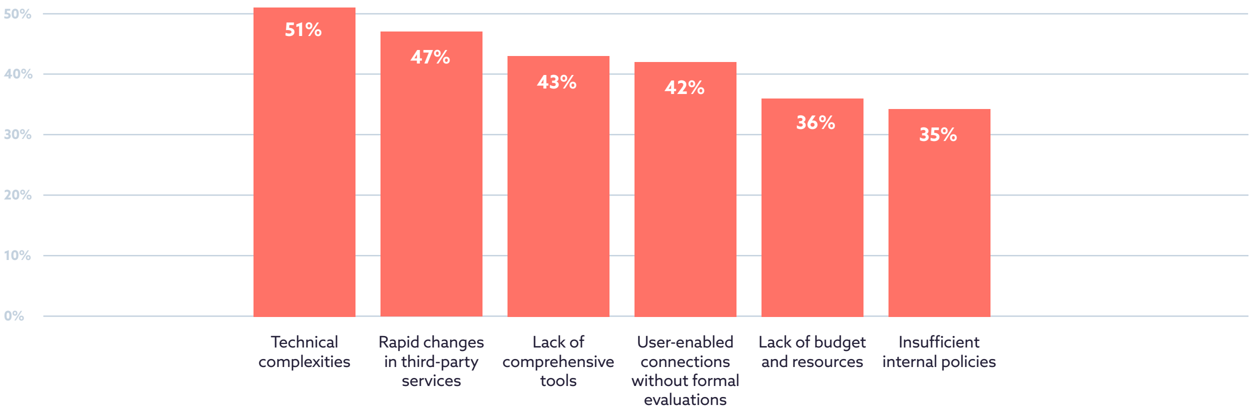


Third-Party Vendor Management

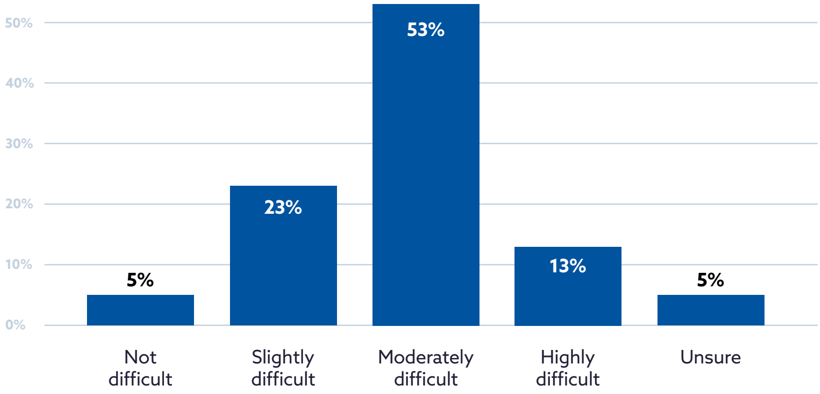
Visibility levels into third-party vendors connected by OAuth apps



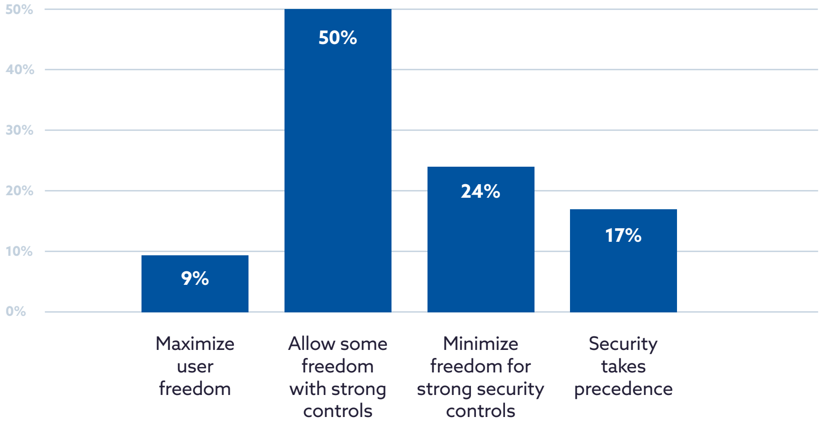
Challenges with maintaining or improving visibility into third-party vendors connected by OAuth apps



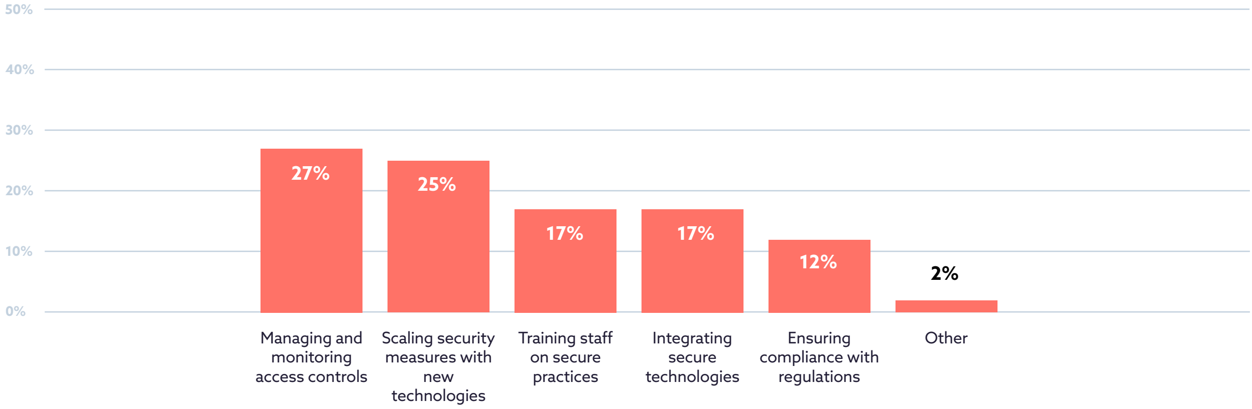
Difficulty levels for managing requests to add third-party tools and services



Balancing user freedom and security for business integrations

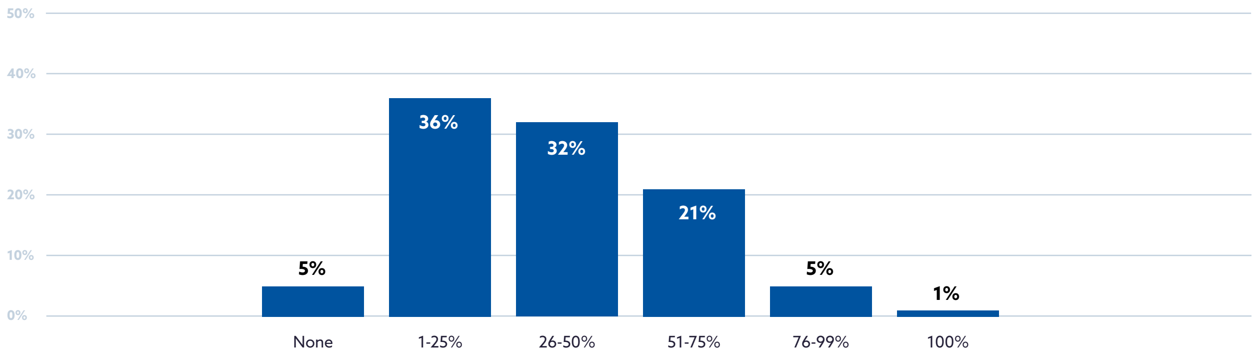


Challenges for implementing secure automation and connectivity

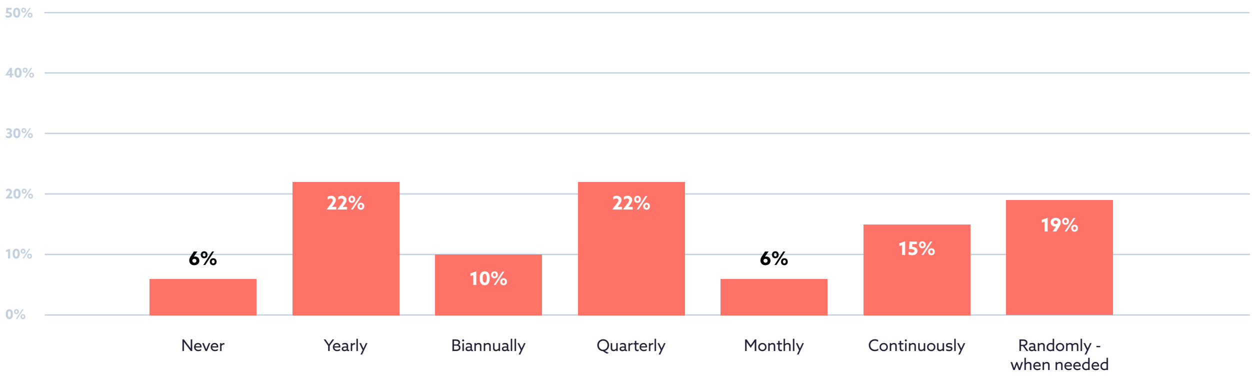


Service Account Permissions Management

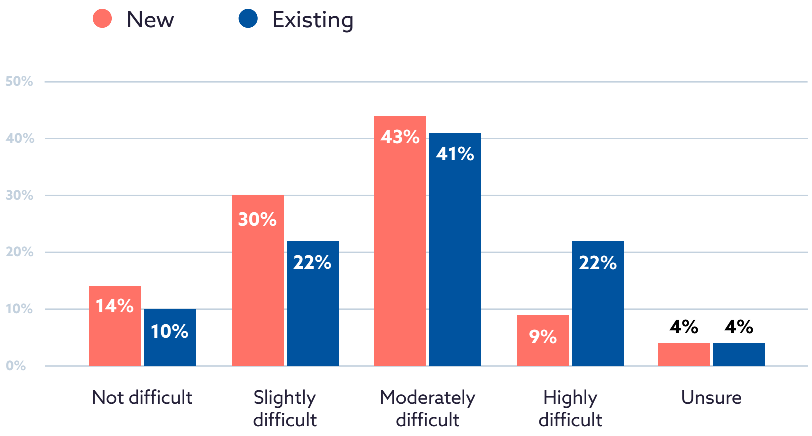
Estimated % of Over-Permissive Accounts in Organizations



Frequency of review for service account permissions

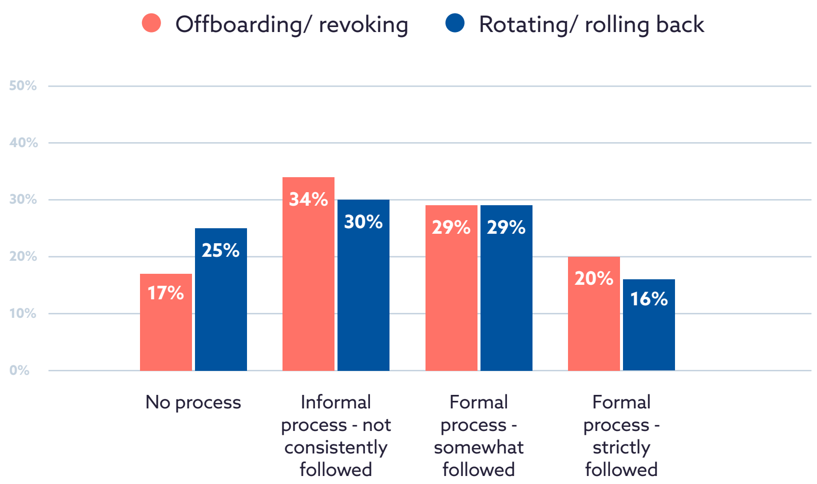


Difficulty levels of managing permissions for new versus existing service accounts

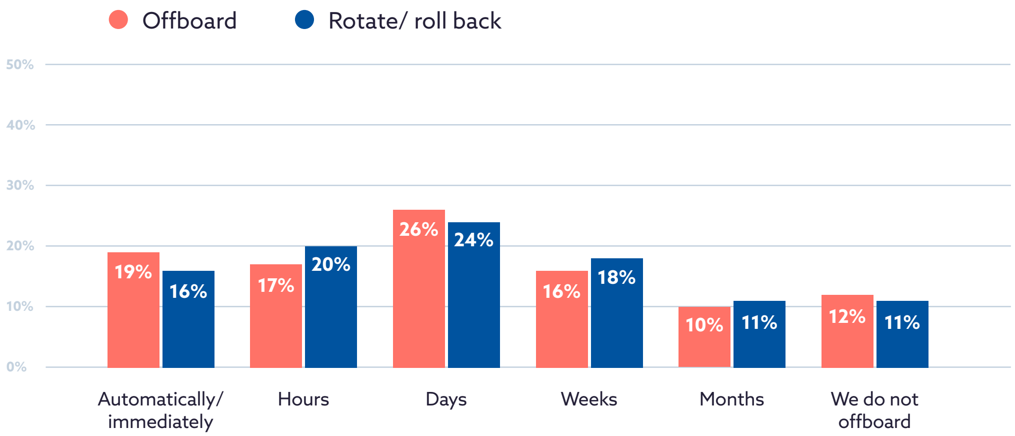


API Key Management

Type of process for API key offboarding/revoking versus rotating/rolling back



Timeline for API key offboarding versus rotating/rolling back

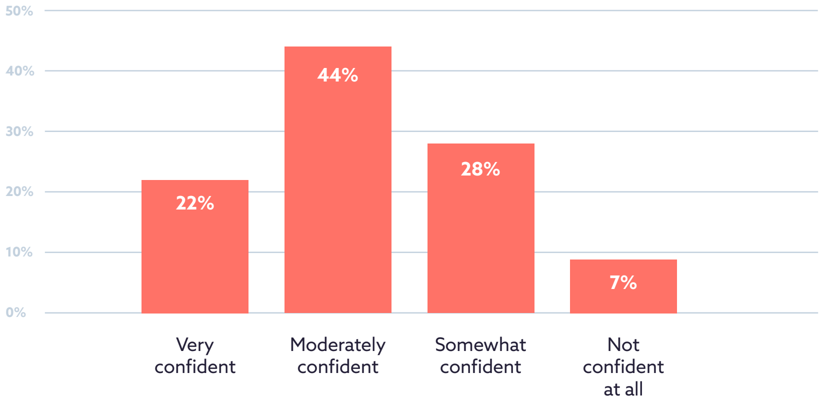


Secrets Management

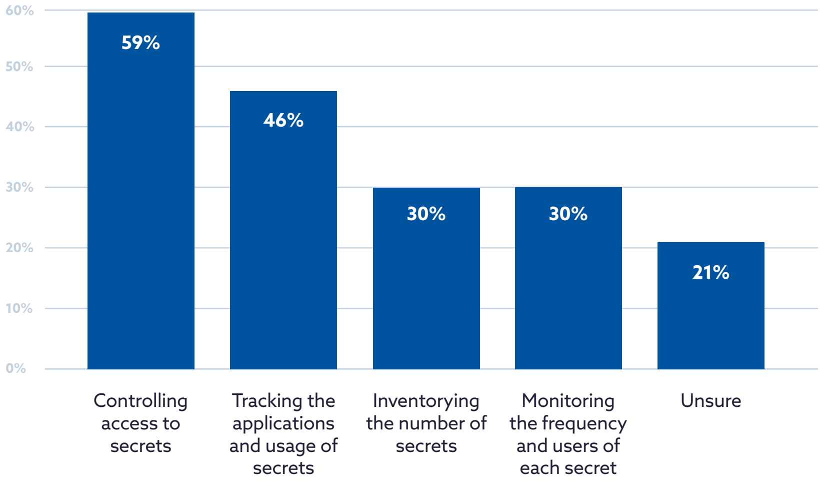
Methods for storing and managing secrets

46%	Encrypted databases
45%	Dedicated secrets management tools
41%	Access Controls
41%	Cloud vault
31%	Auditing and Monitoring
31%	Rotation and Expiration Policies
28%	Hardware Security Modules (HSMs)
22%	Zero-Trust Architecture
21%	Environment variables
16%	Hard-coded in application code
1%	Other

Confidence levels in storing and managing secrets



Capabilities used for secrets management in application development

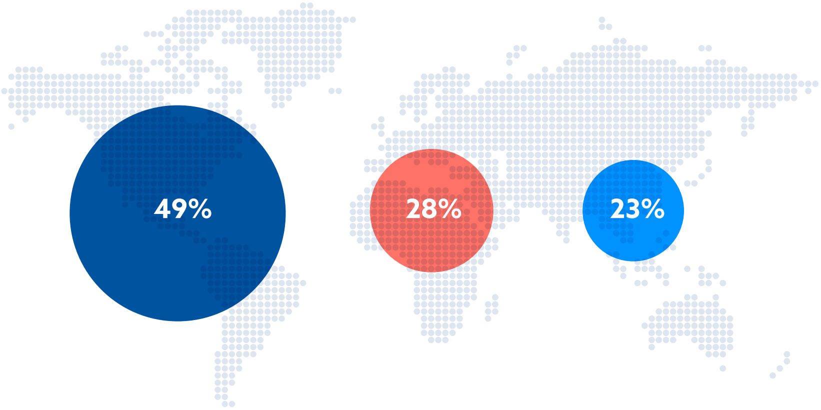


Demographics

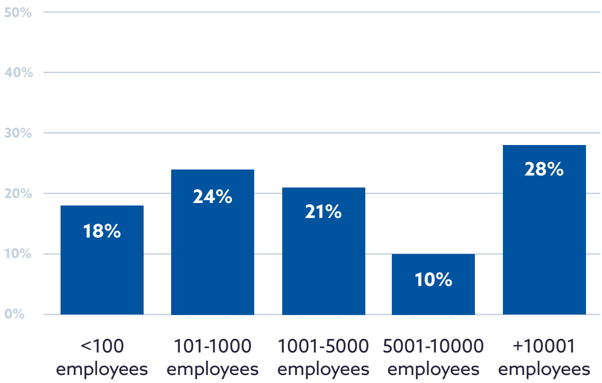
The survey was conducted online by CSA in June 2024 and received 818 responses from IT and security professionals from organizations of various sizes and locations.

What region of the world are you located in?

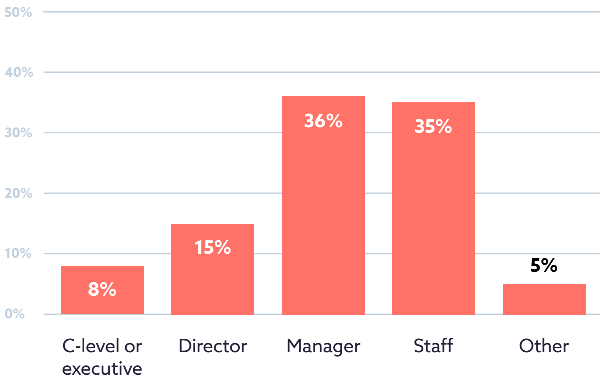
- ● Americas
- ● Europe, Middle East, Africa (EMEA)
- ● Asia-Pacific (APAC)



What is the size of your organization?



What best describes your job level?



Which of the following best describes the principal industry of your organization?

33%	Telecommunications, Technology, Internet & Electronics	3%	Retail & Consumer Durables	1%	Entertainment & Leisure
18%	Finance & Financial Services	3%	Business Support & Logistics	1%	Food & Beverages
6%	Prefer not to answer	2%	Utilities, Energy, and Extraction	1%	Transportation & Delivery
5%	Healthcare & Pharmaceuticals	2%	Construction, Machinery, and Homes	1%	Agriculture
5%	Education	2%	Automotive	1%	Real Estate
4%	Government	2%	Nonprofit	1%	I am not currently employed
4%	Manufacturing	2%	Advertising & Marketing	0%	Health & Fitness
3%	Insurance	1%	Airlines & Aerospace (including Defense)		

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices and ensure cybersecurity in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Astrix commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding non-human identity (NHI) security and its challenges. Astrix financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in June 2024 and received 818 responses from IT and security professionals from organizations of various sizes and locations. CSA's research analysts performed the data analysis and interpretation for this report.

Goals of the Study

The primary objectives of the survey were to gain a deeper understanding of several critical aspects of NHI, such as:

- The perceptions and concerns around non-human identities
- Current security efforts, policies, and management of non-human identities
- Challenges with connecting to third-party vendors
- Current management and policies for API keys