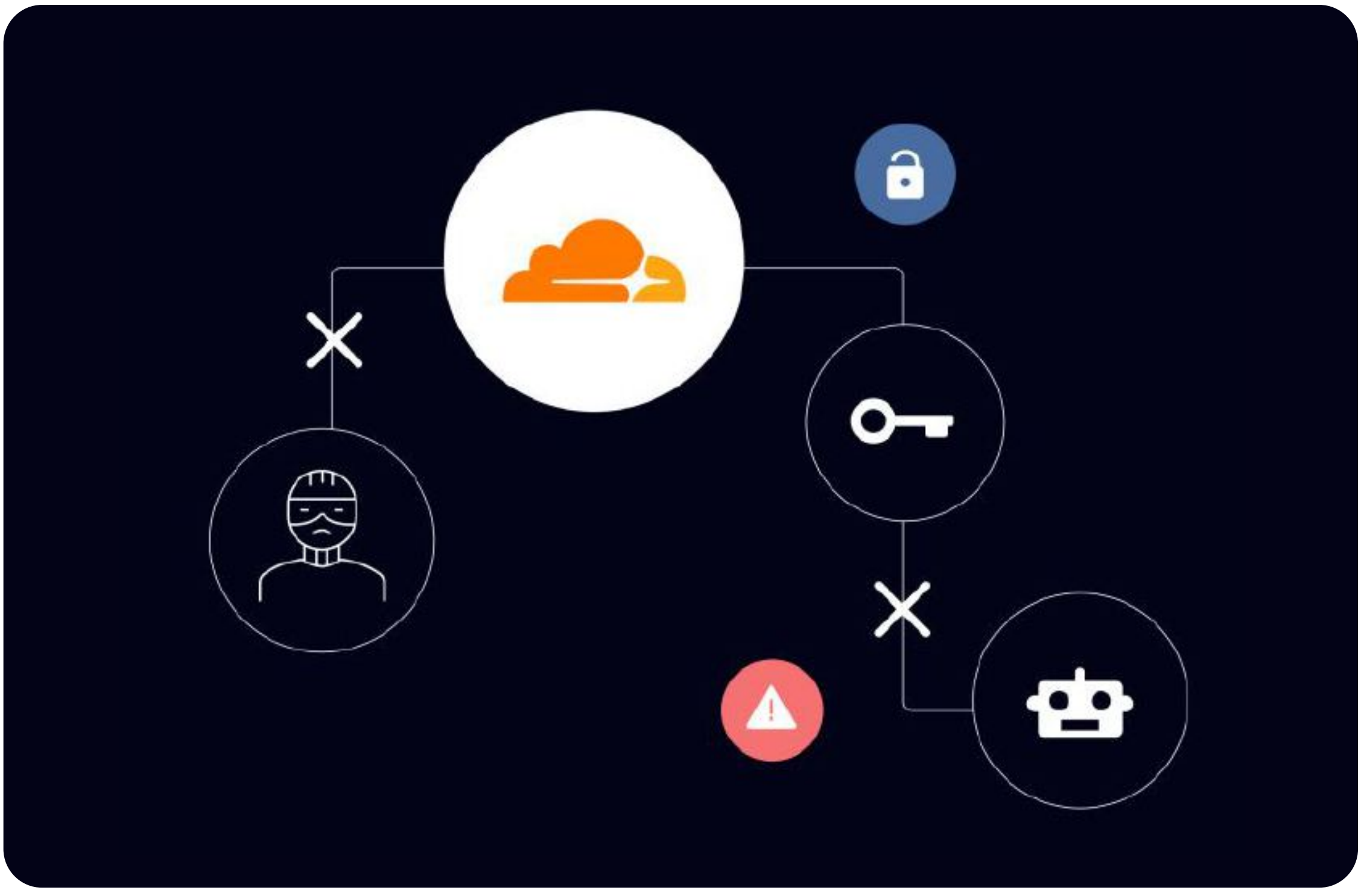
OASIS

White Paper

Lessons From Recent NHI Breaches

2024

Table Of Contents

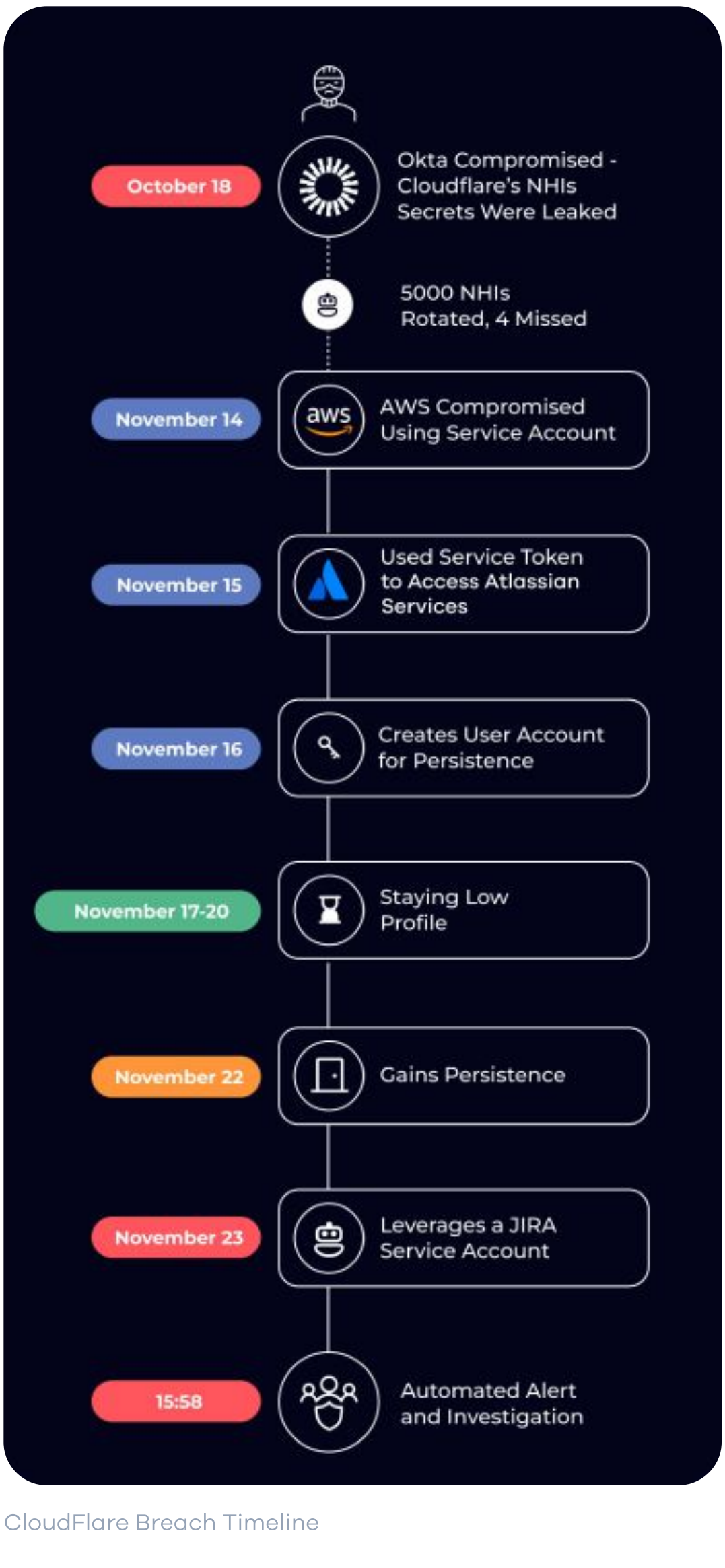


01

Securing Non-Human Identities: Lessons From The Cloudflare Breach

Cloudflare disclosed on February 2nd that it had been breached by a suspected nation-state attacker. This breach exploited multiple unrotated and exposed secrets. The chain of events began with the Okta breach in October 2023, during which the attacker gained administrative access to Cloudflare's Okta system. Although the Cloudflare team attempted to rotate all relevant credentials within Okta, they inadvertently missed one access token and three service accounts, mistakenly believing they were unused. Subsequently, the attacker utilized these four non-human identities to gain access to Cloudflare's Confluence, Jira, and Bitbucket systems. The breach was eventually detected by a detection system, prompting the initiation of a thorough investigation.

It is noteworthy that the Cloudflare team was aware of the Okta breach in October, yet they couldn't prevent the subsequent breach. Despite the awareness and the recognized need to rotate all exposed credentials, timely action was impossible to execute quickly enough and precisely due the inherent operational complexity of the task, even by an experienced team like the one at Cloudflare. Consequently, the attacker capitalized on the initial Okta access to gain further credentials, facilitating lateral movement.



CloudFlare Breach Timeline

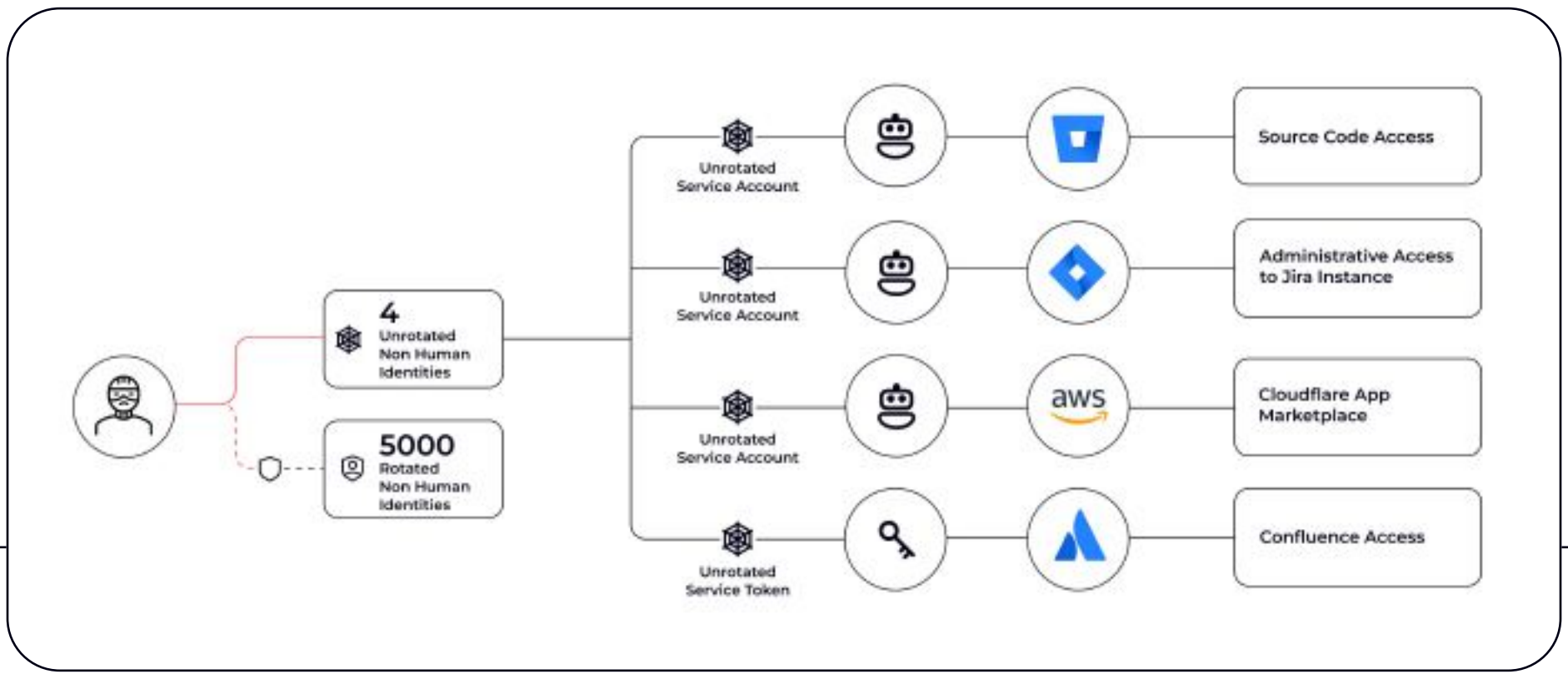
In the wake of the breach, Cloudflare's team was faced with a huge challenge that requires an incredible effort to solve: rotate all their production secrets, analyze all testing and development environments, and return data center hardware back to the vendor for analysis. A process that took them until January to complete, while developers were still working on hardening systems. As it often happens, the challenge of responding to risks is usually much greater than implementing best practices that prevent them to begin with.

The Challenge Of Secret Rotation

Rotating secrets is inherently difficult:

- They outnumber human identities by a factor 10-50x. In the CloudFlare case, they had to rotate more than 5000 of them!
- They are everywhere in the environment, making it hard to maintain an accurate and complete inventory of all identities and secrets.
- Rotating an identity without knowing what system depend on it may lead to infrastructure disruption

The lack of relevant management tools leaves most organizations struggling to perform regular rotations, especially during security incidents. Furthermore, non-human identities lack multifactor authentication (MFA) and often possess privileged access, making them prime targets for attackers seeking to execute supply chain attacks, perform lateral movement, and maintain persistence.



CloudFlare Unrotated NHI

How To Secure Non-Human Identities

The best approach for an organization to eliminate the security risk exposure from NHIs is to efficiently manage them throughout their lifecycle . This entails implementing several key best practices:

- Ensure that a non-human identity is dedicated to a single process or application.
- Rightsize the NHI privileges for its operation. No more, no less.
- Periodically rotate the identities' secrets to mitigate the risk of unauthorized access.
- Decommission stale identities that are no longer in use.

When an organization achieves this ideal state, an identity based attack becomes practically impossible. For example, after the Okta breach, this organization could trigger a wide and through rotation, thus eliminating the risk. Reaching this ideal state requires a combination of security policies and great tooling that enable the organization to follow said policies efficiently.

Oasis Makes Non-Human Identity Management Simple And Effective

The Cloudflare incident is a stark reminder of the security risks of unmanaged NHIs. It also speaks to the unique operational challenges that security teams face with NHIs, even for an experienced team like the one at Cloudflare. While most organizations today have a well defined enterprise strategy to secure human identities and the right solutions for the job, they don't for NHIs which are often left undamaged because simply too difficult to deal with existing tools for PAM, CIEM, CSPM.

Luckily, there is a solution now and it's called Oasis! We created the Oasis platform to provide security, identity and cloud teams the needed capabilities and automation to easily secure all non-human identities across that stack throughout their lifecycle.

Specifically to secret rotation, Oasis drastically simplifies the process allowing security teams to efficiently remediate existing vulnerabilities with the peace of mind that system availability won't be impacted. The Oasis platform offers several powerful capabilities to address this critical use case:

- Oasis provides the user with the full context of the identity. It shows who is accessing the identity, who manages it and what access it has. This enables the user to rotate the identity safely without disrupting operations.
- Oasis tracks all identities, showing when they were last rotated, to make sure you do not miss any identities while doing a rotation project.
- Oasis prioritizes rotation based on exposure risk and privileges.
- Finally, Oasis lets the user leverage automation and bulk operations for efficient rotation and deprovisioning. By automatically assessing and ranking posture issues, Oasis enables you to prioritize remediation efforts based on the severity of vulnerabilities.

Managing NHI is complex and involves more than just safely performing secret rotation. Without the right tool, the operational complexity and overhead of managing NHIs becomes an insurmountable barrier. Our team is here to assist you in navigating the complexities of non-human identity management and enhancing your organization's security posture.

02

Automation Is Key: DHS Report Unveils Lessons From The Microsoft Exchange Incident

Last week, the DHS Cyber Safety Review Board, established by President Biden, released a scathing report exposing critical oversights by Microsoft that enabled the targeted cyberattack by Chinese hackers on top-tier US government officials' email accounts.

This report, the third and most comprehensive review conducted by the independent board, serves as a vital resource for government officials and the broader security community to bolster the protection of their digital networks and infrastructure. Chaired by Robert Silvers, the Department of Homeland Security's undersecretary for policy, the board brings together a diverse array of government and industry experts.

TL;DR based on the report's findings:

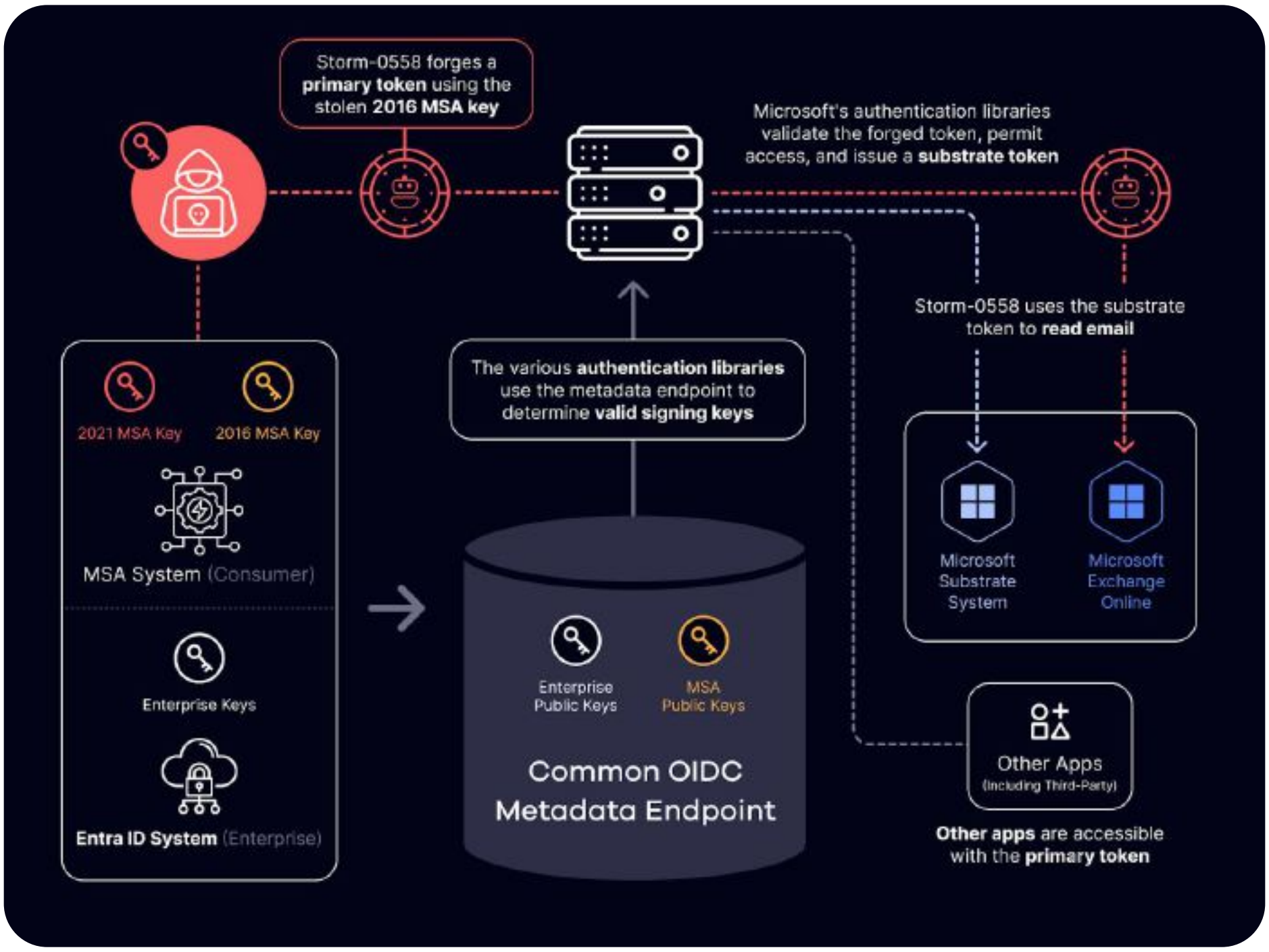
- Several "avoidable errors" in Non-human Identity Management practices led to the breach, including failure to decommission an old signing key, use of a key across business and consumer networks, and oversight in non-human identity risk assessment of acquired firms.
- A highly privileged private key that was "kind of forgotten", was left unrotated for over 6 years. This is a common toxic combination of issues that hard to detect and exponentially increases risk
- Microsoft's shift from manual to automatic key rotation is a positive step and underscores the necessity of prioritizing automation in Non-Human Identity Management.
- DHS plans to launch initiatives and meet with companies to improve security standards, emphasizing the importance of transparency and proper Non-Human Identity management.

The Breach

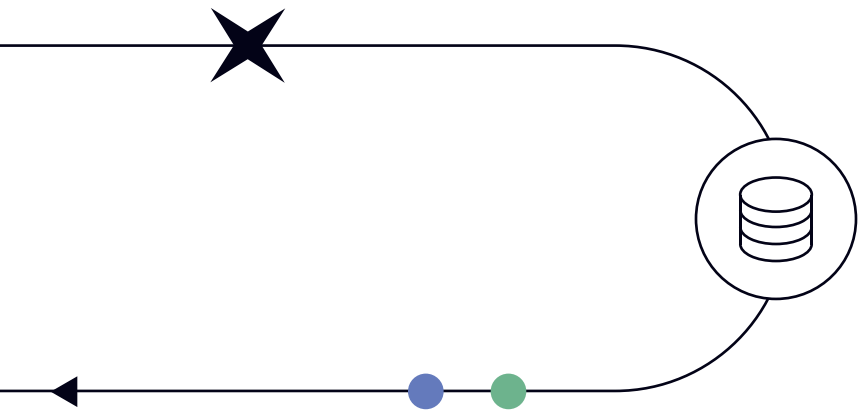
Detected in June and attributed by US intelligence agencies to China's Ministry of State Security (MSS), exploited vulnerabilities within Microsoft's cloud infrastructure. This allowed MSS hackers to manipulate credentials and gain unauthorized access to emails belonging to key figures in the US Cabinet, as well as other prominent State Department officials.

In the spring of 2023, a sophisticated cyberattack orchestrated by an entity identified as Storm-0558 compromised the Microsoft Exchange Online mailboxes of 22 organizations and over 500 individuals globally. Associated with espionage activities linked to the People's Republic of China, Storm-0558 exploited authentication tokens associated with a Microsoft key established in 2016. This intrusion had profound ramifications, affecting senior US government officials.

The compromise of these critical keys, essential for ensuring secure access to remote systems, equates to acquiring the crown jewels for any cloud service provider. In this instance, the stolen key granted the adversary unprecedented access, enabling Storm-0558 to infiltrate Exchange Online accounts worldwide and exert control over sensitive information and systems.



Storm-0558 Microsoft breach | Non-Human Identity Security



Breach Timeline

The Board's investigation reveals that the intrusion commenced in May 2023, with known adversaries' techniques addressed by the end of June 2023. Here's a high-level timeline, with a more detailed chronology provided in Appendix B.

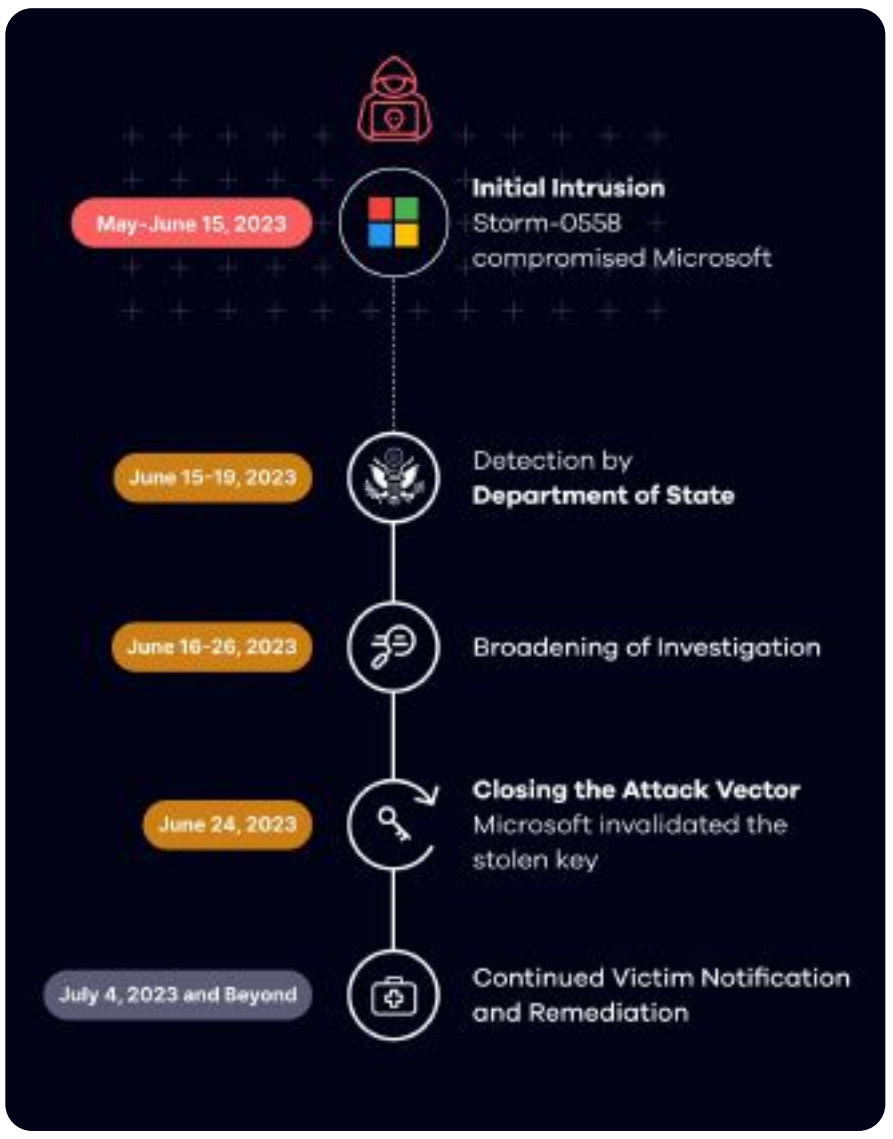
May-June 15, 2023: Initial Intrusion, Pre-Discovery Phase
Between May and mid-June, Storm-0558 compromised Microsoft Exchange Online mailboxes of certain victims in the U.S., the U.K., and other locations. However, it's noted that Microsoft's window of compromise might have begun earlier than May 15, as per standard 30-day log retention practices.

June 15-19, 2023: Detection by Department of State
State authorities detected anomalous activity on June 15, informing Microsoft on June 16. With Microsoft's support, State conducted an investigation over the holiday weekend. By June 19, it was confirmed that a threat actor had accessed six State email accounts, including those linked to the Secretary of State's upcoming trip to Beijing.

June 16-26, 2023: Broadening of Investigation; Department of Commerce Identified as Victim
State reached out to Microsoft, CISA, and the FBI. CISA personnel, already present at State, began proactive threat hunting, while the FBI shared details about the threat actor. Microsoft initiated an investigation on June 16, presuming that Storm-0558 gained entry via State's OWA. Subsequently, Microsoft notified victim organizations in the U.K. and identified the Department of Commerce as another victim by June 23.

June 24, 2023: Closing the Attack Vector
Microsoft invalidated the stolen key used by the threat actor on June 24, halting Storm-0558's access to email accounts. Following this action, Microsoft observed Storm-0558 attempting phishing and other methods to regain access to compromised email boxes.

July 4, 2023 and Beyond: Continued Victim Notification and Remediation
Microsoft commenced victim notification during its initial investigation, a process that continued for weeks. Due to the nature of the intrusion, Microsoft was primarily responsible for identifying most victims and collaborated with the U.S. government to provide necessary support



Storm-0558 Microsoft breach

Key Takeaways

#1 NHI Management needs to become an integral part of enterprise identity programs. The Microsoft breach is just the latest example in a rapidly growing trend of attacks that exploited unmanaged NHIs. Even technologically advanced and security aware organizations, such as Microsoft, can fall victim of attacks to unmanaged NHIs.

#2 Organizations should adopt practices and tools that keep both operational continuity efforts and security best practices aligned, and not in opposition.

In 2021, following a large production outage, Microsoft had stopped their manual key rotation processes, leaving the key that was later compromised, as well as many others, much more vulnerable. Prioritizing operational continuity over security posture is a very common pattern that, in most cases, is caused by lack of contextual visibility which leads to inaction. The complexity and scale of NHIs requires purpose built tools that can automatically discover NHIs, create system dependency maps and identify high risk priorities

#3 Automate, automate, automate. When it comes to NHI management, automation is key because the scale is so vast. Companies can't disregard the limitations of human driven processes, which are more prone to error and operationally expensive. While adding automating tasks like secret rotation typically requires integrating new tools and capabilities in your stack, the investment is absolutely critical for the long term success of the business. Microsoft's decision to move from manual to automatic key rotation is the right move to make and, had it been implemented sooner, it could have prevented the attack with undeniable business benefits.

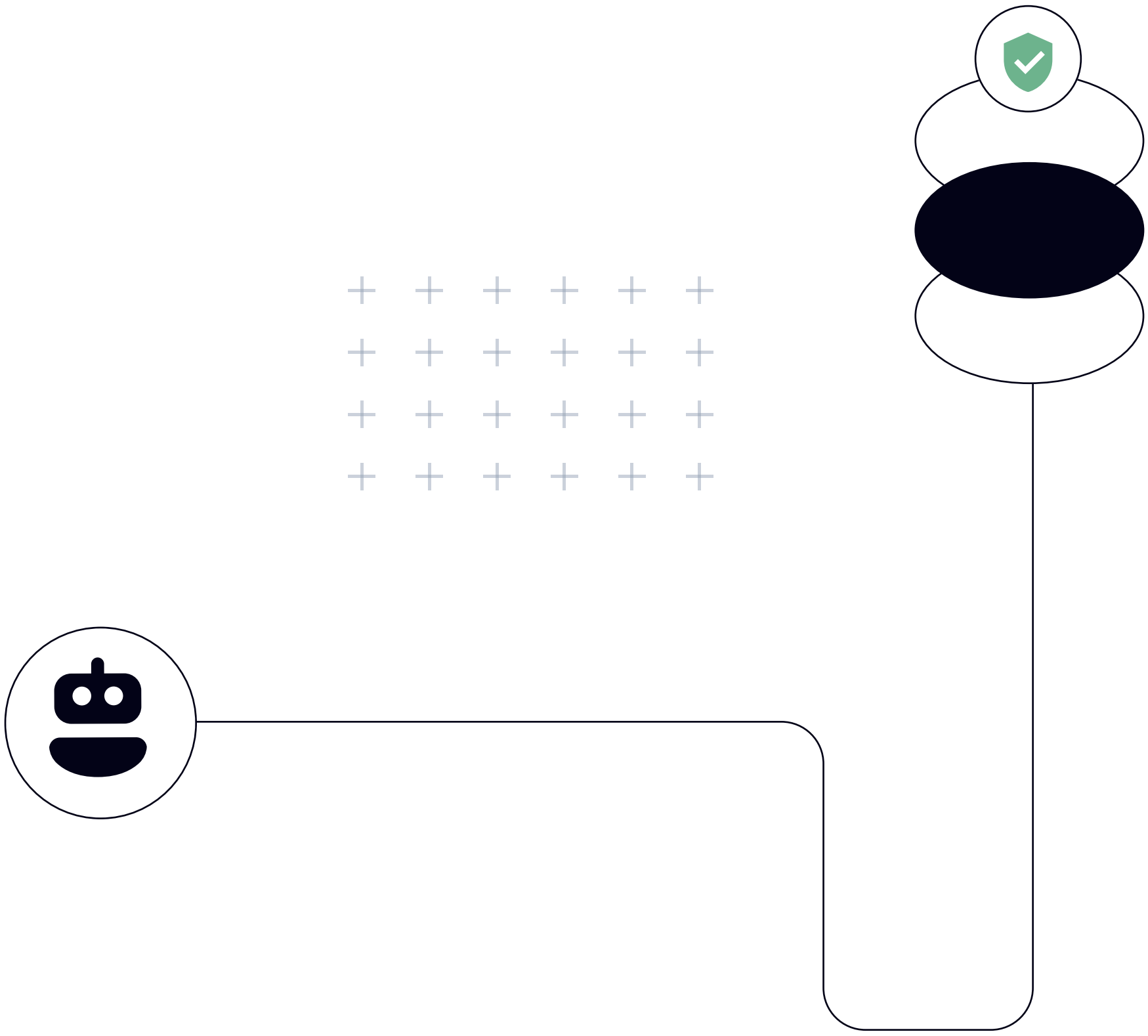
#4 Rotation of keys and secrets is only one part of the larger challenge of complete non-human identity lifecycle management. While the latest report highlights several shortcomings, cloud transformation through vendors such as Microsoft still allows organizations to improve agility and, with the right approach, security posture. As environments become increasingly distributed spanning multiple clouds and hundreds of interconnect services, Non-Human Identities grow exponentially in scale. Consequently, security and operations teams need to adopt the right tools that enable effective cooperation across every phase of the lifecycle from provisioning, to rotation and decommission.

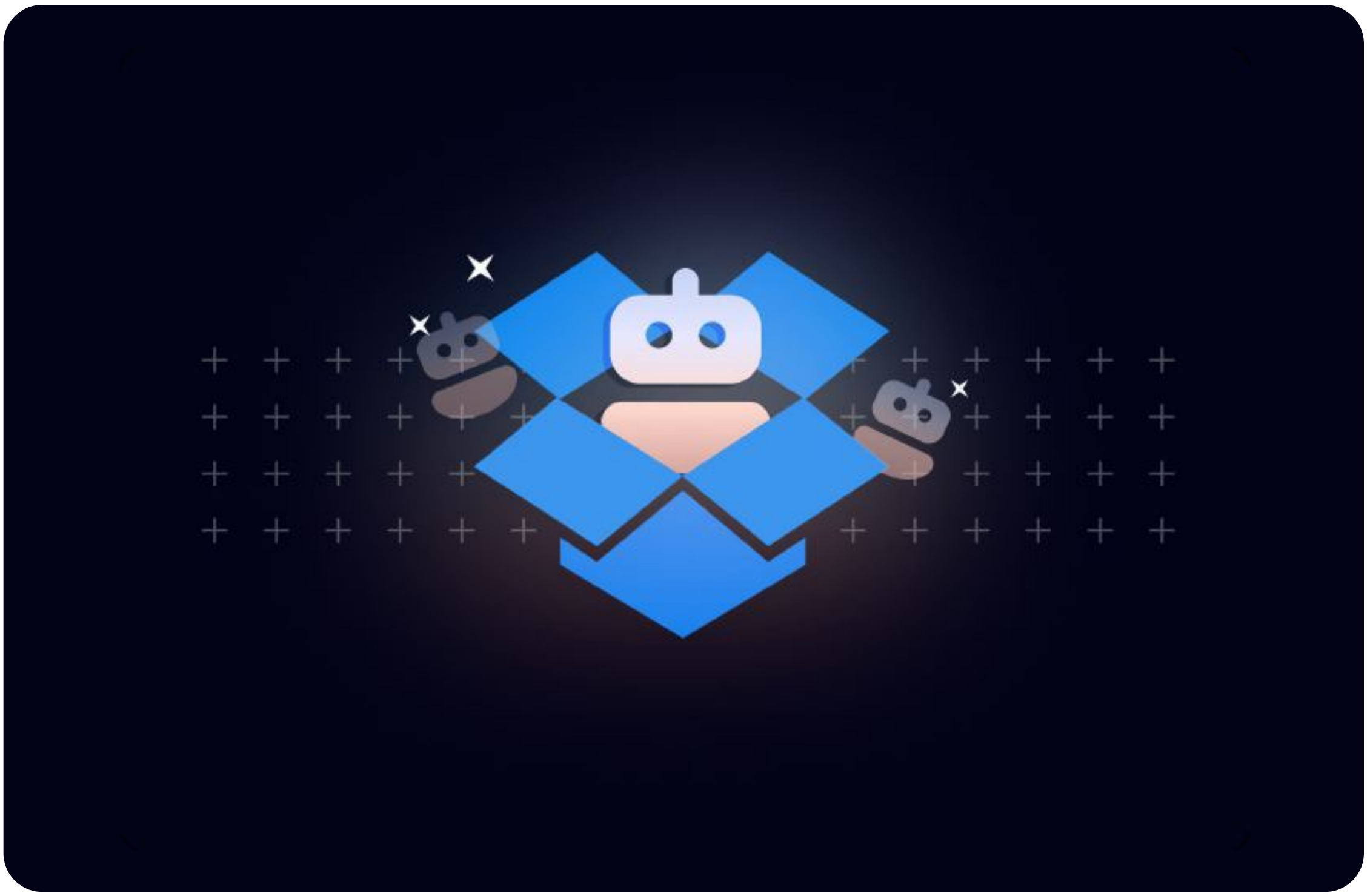
Conclusion

The revelations from this incident underscore a fundamental truth within today's intricate digital landscape: the management of non-human identities is a complex task that necessitates automation. Microsoft's breach, characterized by a series of preventable errors, starkly emphasizes the vulnerabilities associated with manual approaches to identity management.

Non-Human Identities serve as keystones in ensuring secure access to vital systems and resources. However, the sheer volume and intricacy of these identities render manual oversight impractical. Without the implementation of automated solutions, organizations are left susceptible to numerous risks, including unauthorized access, compromised credentials, and systemic vulnerabilities.

At Oasis Security, we fully grasp the indispensable role of automation in effectively managing non-human identities. Our pioneering solutions harness advanced technologies to automate Non-Human identity lifecycle management, and improve enterprises NHI security posture.





03

Non-Human Identity Risks: Lessons From Dropbox's Security Incident

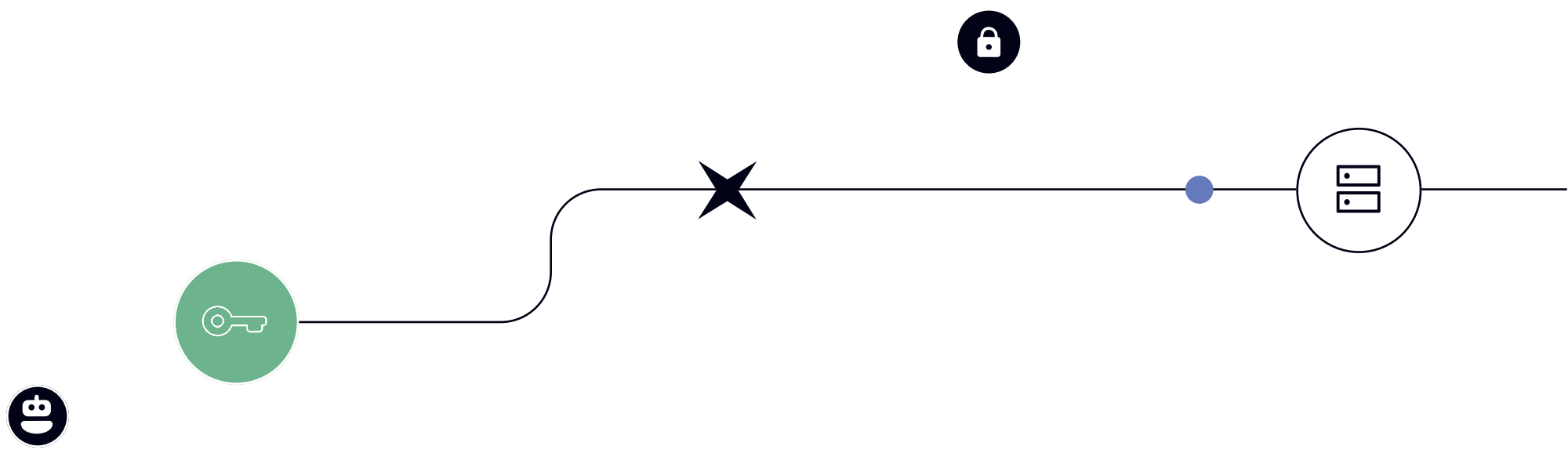
On April 24th, Dropbox became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. The Investigation revealed that a threat actor had breached the system, accessing sensitive customer information. What set this incident apart was the method of intrusion: the compromise of a **non-human identity** (NHI) used within Dropbox Sign's back-end infrastructure.

At the heart of the breach was the compromise of a vital automated system configuration tool within Dropbox Sign's infrastructure. This tool, essential for managing the system's configuration, became a target for exploitation by threat actors. Specifically, the compromised NHI was a service account—a type of non-human identity specifically designed to execute applications and automate essential services within the system.

Service accounts, often established within Microsoft Active Directory (AD), serve as conduits for various system operations, from software installations to database management. Functioning autonomously, these accounts carry out tasks seamlessly, often operating in the background without human intervention. However, their autonomy, coupled with extensive access privileges, renders them susceptible to exploitation if not adequately secured.

In the Dropbox Sign breach, the threat actor gained unauthorized access to sensitive customer data by exploiting violations within this service account. While the company assures that the breach did not extend to compromising user account contents or payment information, 'Based on what we know as of the date of this filing, there is no evidence that the threat actor accessed the contents of users' accounts, such as their agreements or templates, or their payment information,' the company said in the 8-K filing. It underscores the critical importance of fortifying non-human identities within system infrastructures.

In response to the incident, Dropbox took swift action to mitigate risks to its users. **This included resetting users' passwords, logging users out of connected devices, and coordinating the rotation of all API keys and OAuth tokens.** The company also reported the incident to data protection regulators and law enforcement authorities. However, the incident illuminates a broader issue within cybersecurity practices—the often overlooked security measures concerning non-human identity management.



Lessons Learned And Future Outlook

The Dropbox Sign security incident serves as a stark reminder of the critical importance of effectively managing non-human identities like service accounts throughout their lifecycle. Organizations must prioritize robust practices for the creation, assignment, governance, rotation of secrets, and decommissioning of stale service accounts to mitigate risks and enhance cybersecurity posture.

Prioritize Comprehensive Visibility For Effective Service Account Management

Achieving a complete view of the service account landscape is crucial. Organizations should strive for holistic visibility, enabling them to identify all service accounts within their infrastructure. This visibility should extend to various aspects such as account usage, permissions, and associated resources, empowering administrators to track and manage service accounts efficiently.

Ensure Safe Secret Rotation For Non-Human Identities

While regular password/secret rotation is standard practice for human identities, it is often overlooked for non-human identities. Concerns about potential disruptions to critical operations lead to the neglect of secret rotation, allowing compromised service accounts to maintain prolonged access to an organization's network undetected.

Rotating passwords in outdated environments, especially those heavily dependent on Microsoft Active Directory (AD) service accounts, presents a significant challenge. An illustrative example of this challenge is the Cloudflare breach, where despite a rotation attempt of approximately 5000 accounts, four service accounts remained unrotated. This incident highlights the need for automation solutions to address this issue effectively. Unlike modern systems that allow for simultaneous rotation of multiple passwords, older systems often impose restrictions, permitting only one password rotation at a time. This limitation not only complicates the rotation process but also heightens the risk of credential exposure due to delayed updates.

To mitigate these risks, organizations must invest in dedicated tools designed to automate the rotation of non-human identity secrets. By leveraging automation solutions, such as specialized platforms, organizations can streamline the rotation process, enhance security measures, and effectively safeguard their systems against evolving cyber threats. Moreover, streamlining non-human identities lifecycle management is paramount for both efficiency and security. Automated workflows enable seamless provisioning, enforce role-based access controls (RBAC), and conduct regular audits, ensuring consistent and policy-compliant management of service accounts. Through automation, organizations can minimize manual efforts, mitigate the risk of errors or oversights, and uphold robust security standards across their infrastructure.

Context Is Key To Solve Security Challenges Without Business Disruption

When Dropbox asked its customers to rotate all API keys and OAuth tokens following the security incident, it highlighted the importance of contextual understanding. Without a comprehensive view of how these non-human identities were being used within their systems, customers may find it challenging to determine the appropriate course of action for rotation.

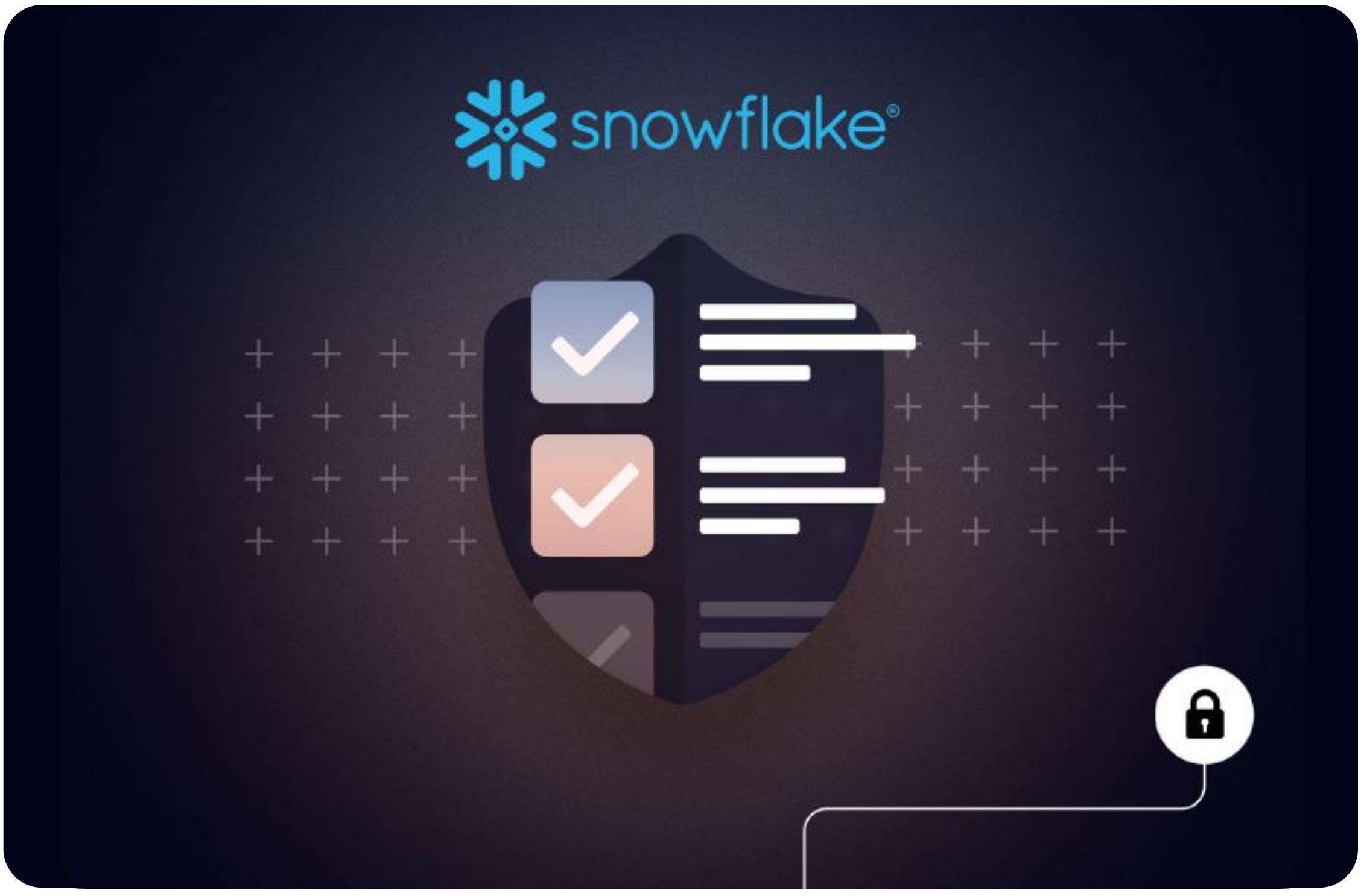
For instance, some API keys or OAuth tokens may be associated with critical integrations or applications essential for business operations. Rotating these tokens without understanding their usage context could potentially disrupt crucial workflows or services, leading to operational downtime or service interruptions. Think of it like this: some of these keys and tokens are like the keys to your office building or your home – if you change them without knowing who's using them and why, you could accidentally lock out important services or cause disruptions in your day-to-day operations.

Detailed insights into the context surrounding each service account are essential. Contextual mapping capabilities provide information about service account configurations, access controls, and usage patterns. By understanding the context in which service accounts operate, administrators can make informed decisions regarding their management and access privileges.

Proactive Posture Assessment Is Key To Strengthening Security Measures

Assessing the security posture of service accounts is paramount. Organizations should conduct automated posture assessments, evaluating factors such as secret rotation, access permissions, and compliance with security policies. This proactive approach helps identify vulnerabilities and prioritize remediation efforts to enhance the overall security of service accounts.

In conclusion, the Dropbox Sign security incident highlights the critical need for organizations to enhance their management of service accounts throughout their lifecycle. By adopting robust practices for visibility, contextual understanding, proactive posture assessment, streamlined lifecycle management, and security and compliance enforcement, organizations can significantly improve their cybersecurity posture and effectively mitigate risks. As we all adapt to the ever-evolving cybersecurity landscape, it's essential for organizations to invest in comprehensive approaches to non human identity management. If you're a Dropbox user looking to better assess your non-human identity risk in light of this incident, reach out to Oasis Security today for expert assistance and guidance. Safeguard your sensitive data and maintain trust with stakeholders by taking proactive steps towards better security practices.



04

Best Practices To Secure Data Access In Snowflake

In the last few days, there has been a lot of noise about an alleged Snowflake breach that impacted several companies' supply chains. While the details remain unconfirmed, it appears that the attack is once more identity-based. It is important to remain vigilant and ensure we are doing everything in our power to maximize the security posture of mission-critical systems that store sensitive data. In this article, we want to share best practices for implementing secure data access to Snowflake by humans and machines.

Access Control In Snowflake

Snowflake uses various authentication methods for user accounts, including passwords combined with multi-factor authentication (MFA), client certificates, and OAuth2 tokens. An important aspect to be aware of is that Snowflake doesn't use different types of accounts for humans and machines - in Snowflake, a user is a user regardless if human or not. It is a common best practice for organizations to follow a standardized naming convention for service accounts, a type of non-human identity (NHI) used for integrations and automated processes such as sfdc_svc_connector or api_usr. These accounts typically authenticate using certificates or OAuth2 tokens and, in some legacy systems, a password.
Snowflake recommends the following security measures:

1. Enforce Multi-Factor Authentication on all accounts;
2. Set up Network Policy Rules to only allow authorized sources or only allow traffic from trusted locations;
3. Reset and rotate Snowflake credentials.

Furthermore, we recommend taking an additional step and disabling Snowflake password authentication for human users if your company has implemented a single sign-on (SSO) solution.

Best Practices To Secure Program Access To Snowflake

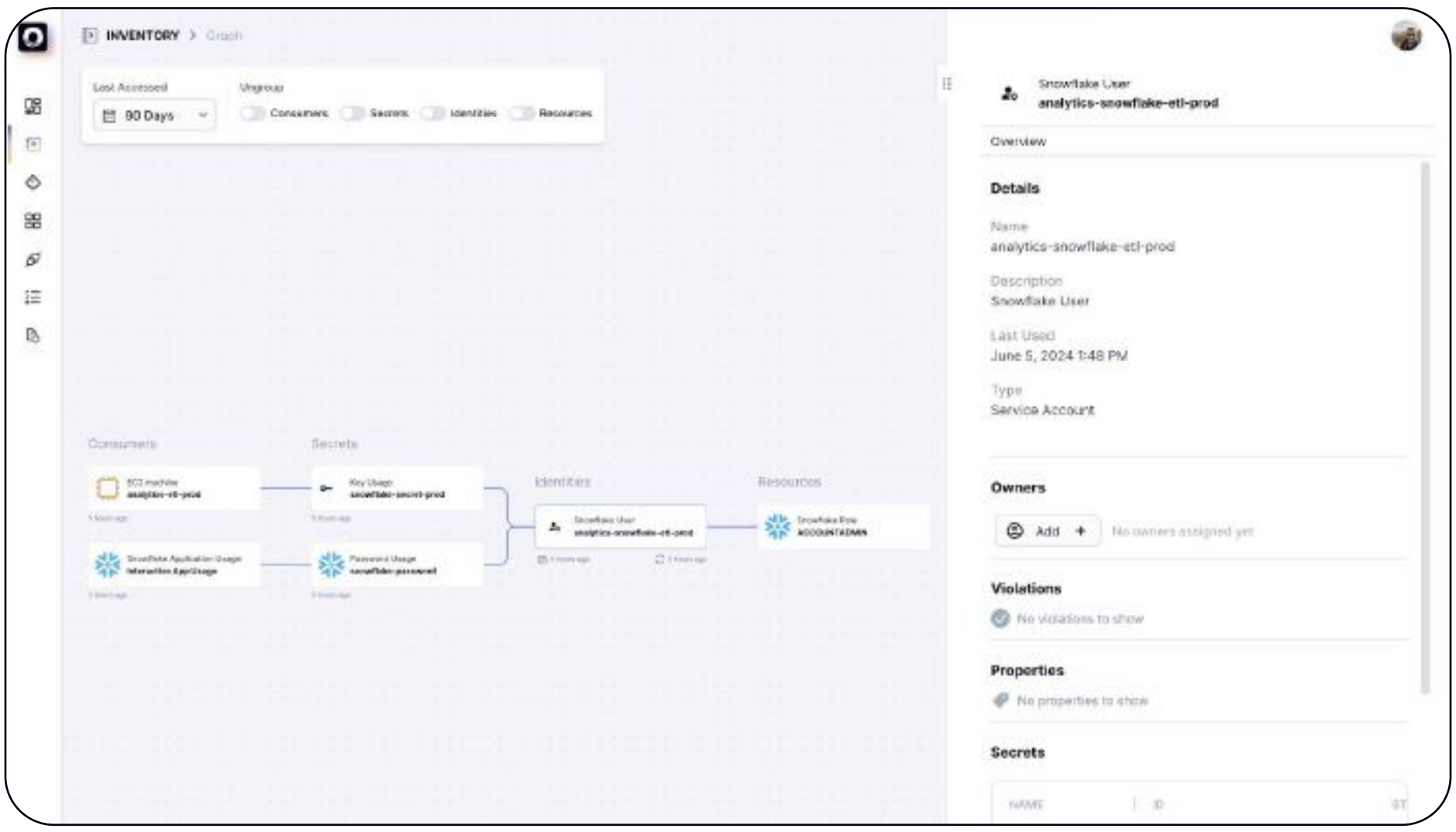
Securing Snowflake user accounts used by programs and presents a unique challenge. These user accounts that often have wide-ranging privileges, but, like other Non-Human Identities, can't rely on smartphones or other devices to support MFA. So, while employees enter codes from their mobile apps, these non-human users can't and therefore are at higher risk.

To account for the different nature of NHIs, we recommend implementing the following security best practices:

1. **Contextual Visibility:** Create and maintain a real-time inventory of NHIs with contextual information about consumers, owners, and access patterns. This helps identify unusual or unauthorized activities quickly.
2. **Rotate Credentials Regularly:** To minimize the risk of unauthorized access, rotate credentials and secrets associated with NHIs regularly.
3. **Right-Size Privileges:** Ensure that NHIs have the right level of necessary privileges required for their purpose. Overprivileged accounts increase the attack surface.
4. **Remove stale accounts:** Ensure that accounts that are no longer in use, for example, user or program accounts previously owned by an offboarded employee, are properly and promptly decommissioned.

Oasis makes it easy to protect Snowflake non-human user accounts with a seamless integration

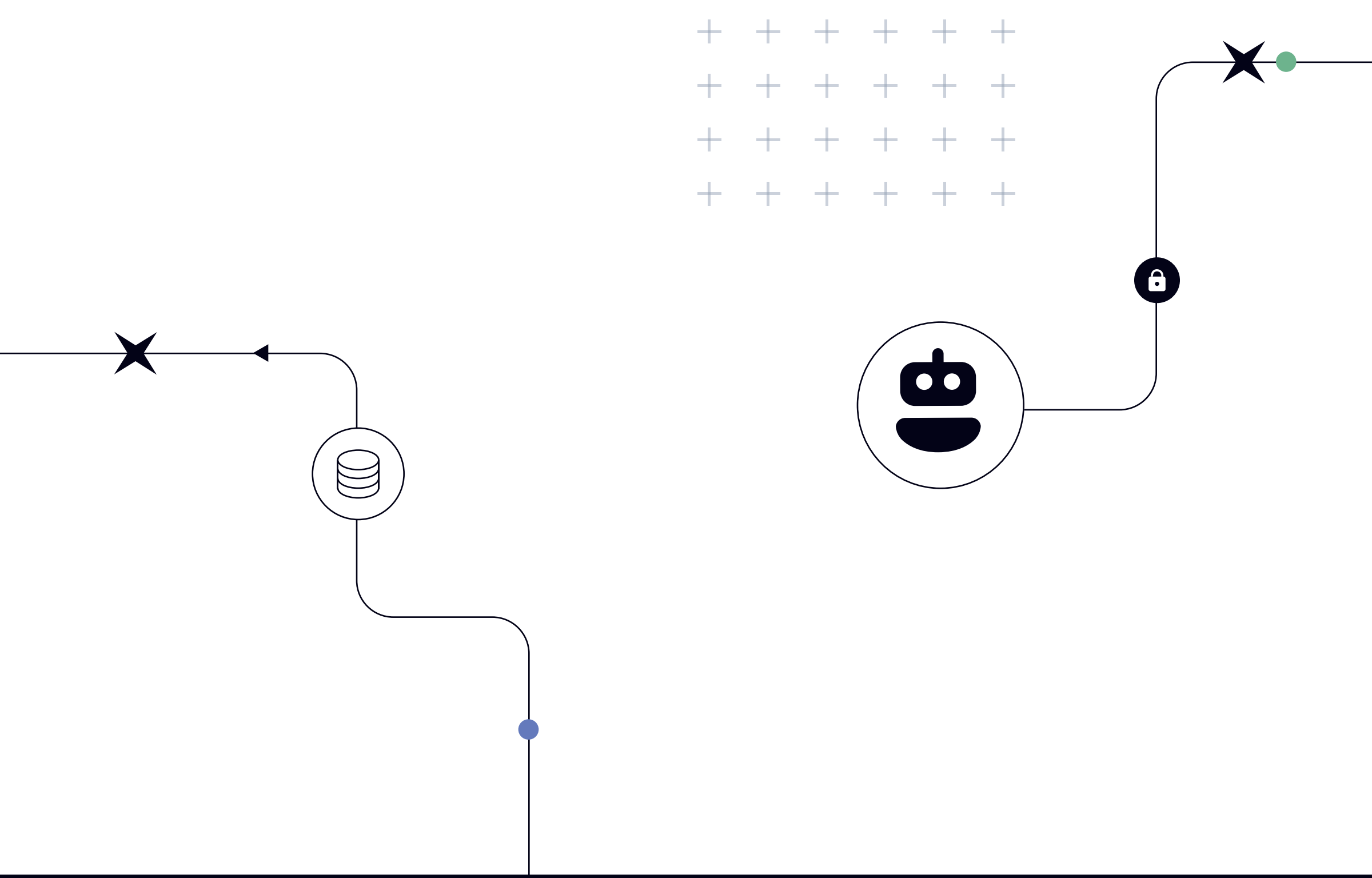
At Oasis, we understand the unique challenges of managing non-human identities. Our platform is designed to secure all NHIs throughout their lifecycle, providing visibility, automation, and robust security measures to protect your organization. Oasis integrates with Snowflake to make it easy to implement security best practices that will drastically reduce the risk of breaches from identity attacks. Simply set up a dedicated user and role in Snowflake, and share the details with Oasis.



Snowflake User in Oasis

This integration provides the following benefits:

- Comprehensive NHI inventory: Oasis takes away the overhead of manually maintaining an accurate inventory of your NHIs within Snowflake. Once connected, Oasis automatically and continuously discovers all your Snowflake NHIs providing critical real-time visibility with detailed information about each identity.
- Critical contextual information: Oasis facilitates auditing activities and ensures accountability for actions performed by NHIs in Snowflake by providing insights into which consumers (users, applications, services) are utilizing each NHI and what resources these identities have access to.
- Posture violation detection: The integration continuously monitors and flags NHIs in stale or unrotated credentials, as well as other basic posture violations, enabling proactive risk mitigation.
- Efficient credential rotation: As part of regular operations or in the event of a security breach, Oasis allows for efficient and automated rotation of credentials across all affected NHIs, minimizing operational disruptions.
- Enhanced incident response: Oasis provides a comprehensive view of all NHIs, their access patterns, and interactions during an incident, enabling security teams to quickly identify potentially compromised identities and take immediate action to mitigate risks.



05

The Future Of Identity Security: Lessons From The Change Health Breach

UnitedHealth Group confirmed that in February, the BlackCat/**ALPHV** ransomware group breached Change Healthcare by exploiting compromised credentials for a Citrix remote access portal that lacked multi-factor authentication (MFA).

"On February 12, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later," UnitedHealth Group declared in the prepared statement.

UnitedHealth Group CEO Andrew Witty confirmed that the company paid a $22 million ransom. “The decision to pay a ransom was mine,” Witty said. “This was one of the hardest decisions I’ve ever had to make, and I wouldn’t wish it on anyone.”

Change Healthcare's payment of $22 million into a ransomware gang, following a crippling attacks on numerous healthcare entities nationwide, not only established one of the largest ransomware payment precedents but also triggered a vicious cycle, encouraging a surge of new cyber attacks on similarly vulnerable targets across the US healthcare system.

The Importance Of MFA In Securing Identities

This recent breach at Change Health serves as a stark reminder of the evolving threat landscape in the digital age. As cyber attackers become more sophisticated, the focus has increasingly shifted towards identity-centered breaches. This incident underscores the urgent need for robust Multi-Factor Authentication (MFA) and a comprehensive strategy to secure both human and non-human identities. In a time where organizations often have 50 times more non-human identities than human ones, it's time for a paradigm shift in our approach to identity security.

MFA has long been recognized as a critical component in securing human identities. By requiring users to provide two or more verification factors, MFA significantly reduces the risk of unauthorized access due to compromised credentials.

The benefits of MFA include:

Enhanced Security: Adding an extra layer of security makes it significantly harder for attackers to gain access to sensitive information.

Compliance: Many regulatory frameworks mandate the use of MFA to protect sensitive data.

Trust and Confidence: MFA helps build trust with customers and partners by demonstrating a commitment to security.

MFA Alone Is Not Enough

However, while MFA is essential, it is not a magic pill. The breach at Change Health highlights that securing human identities alone is insufficient. The broader and more complex challenge lies in protecting the entire identity fabric, which includes a vast array of non-human identities.

Non-human identities, such as service accounts, APIs, and tokens, play a crucial role in modern IT environments and now constitute the bulk of the identity fabric outnumbering human identities by 10x-50x. These identities often have access to sensitive data and critical systems, making them attractive targets for attackers.

Non-human identities, however, can't be protected with MFA making them a primary target for undetected **lateral movement and access to critical data sources**

The challenge in securing non-human identities arises from several factors:

Scale: Organizations typically have exponentially more non-human identities than human ones. Managing and securing such a large number of identities is inherently more operational complex and time consuming without the proper automation

Lack of MFA protection: Non-human identities are associated with resources and programs, not a human. As a result they can't leverage MFA to limit the potential blast radius of an attack. NHIs leverage a wide spectrum of authentication methods, such as certificates, tokens, keys and secrets, which are difficult to efficiently to rotate and decommission at scale due to their sensitive nature. .

No authoritative source: Non-human identities are created by multiple stakeholders for various purposes across the company's infrastructure. This decentralization adds complexity to identity management and makes it challenging to ensure consistent security practices. It complicates ownership assignment, which eventually hinders the remediation process for non-human identity-related violations. Attempting to rotate a credential without proper context of usage and ownership is nearly impossible and prone to disrupting critical business workflows.

Highly Dynamic: Non-human identities are often created, modified, and deleted dynamically, making it difficult to maintain an accurate inventory, understand who owns them, and apply consistent security policies.

The Paradigm Shift: Securing The Entire Identity Fabric

To address the growing risk of identity-centered breaches, the security market must undergo a paradigm shift. Organizations need to recognize that protecting their identity fabric (human and non human identities) requires a comprehensive and integrated approach that includes:

Recognizing Non-Human Identities as Targets: Hackers are increasingly targeting non-human identities as their "golden ticket" for successful breaches. Identity teams must not only bridge the gap in their identity security posture but also take a leading role in understanding that identities have become the new security perimeter, and the attack surface is larger than perceived.

Adopting dedicated Solutions for Non-Human Identity Challenges: Traditional identity access management solutions weren't designed to handle the complexities of non-human identities. We require dedicated solutions tailored to address these challenges effectively. These solutions should support various critical capabilities and ecosystem requirements. To tackle issues like the absence of MFA and the lack of contextual visibility, an NHIM solution should include automated secret rotation functionality.

Leveraging Automation at scale: Given the large number and dynamic nature of non-human identities, automation is essential across their lifecycle—from provisioning to rotation and decommissioning. Human processes are prone to errors and can lead to misconfigurations, especially considering the high privileges granted to non-human identities for performing their business-critical tasks. Therefore, there is no room for mistakes.

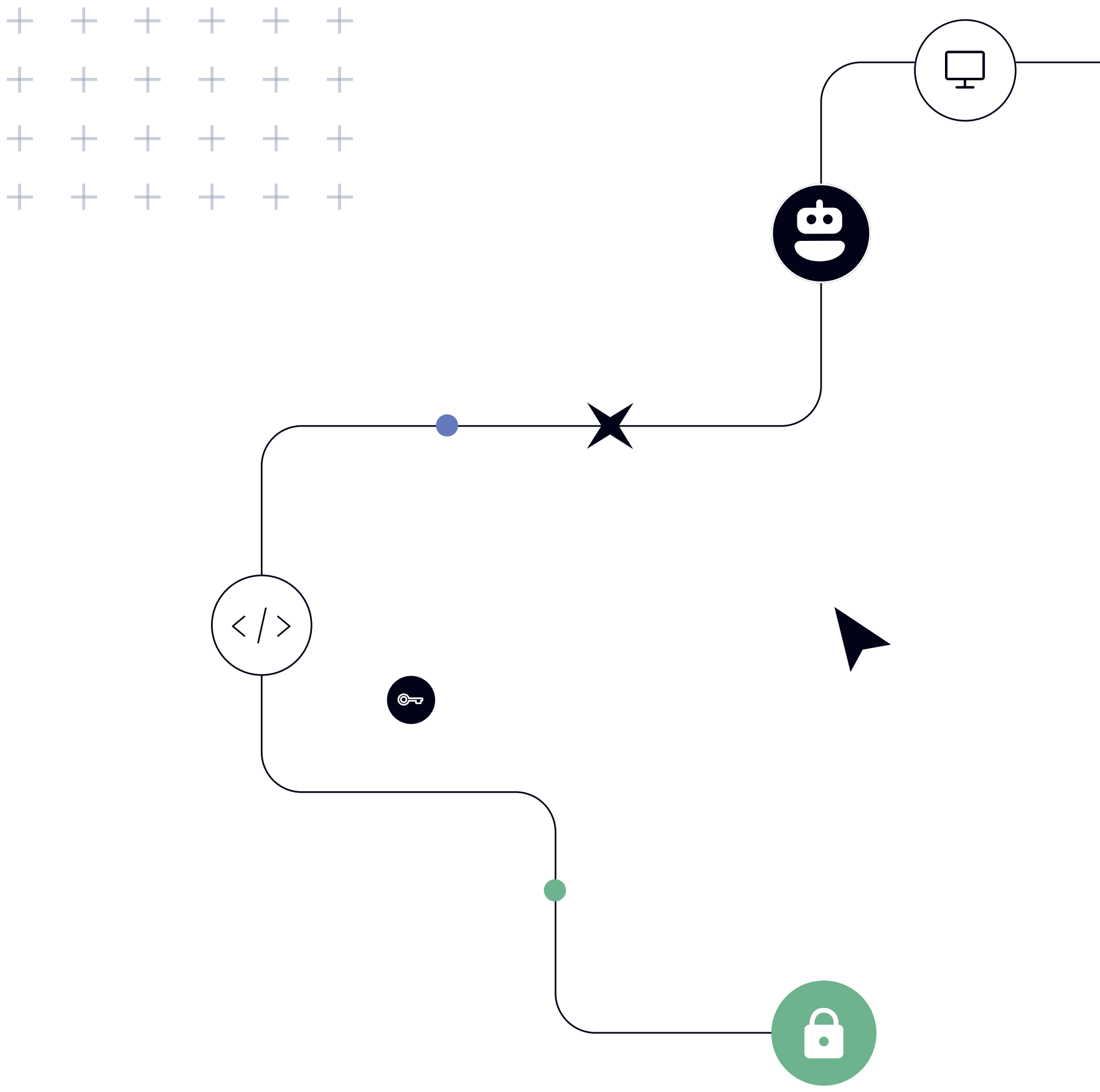
The breach at Change Health is a wake-up call for organizations to rethink their approach to identity security. While MFA remains a cornerstone of securing human identities, it is clear that a broader and more complex challenge exists in protecting non-human identities. By adopting a unified and integrated approach to identity management, organizations can better defend against identity-centered breaches and safeguard their critical assets. The time to act is now, and the path forward requires a comprehensive strategy that addresses the unique challenges of both human and non-human identities.

Oasis: Managing Non-Human Identities

With Oasis, organizations can effectively manage their entire identity fabric, both human and non-human, mitigating the risk of identity-centered breaches and safeguarding sensitive data.

Oasis provides solutions that help enforce identity security measures, including compensating controls for non-human identities where traditional methods like MFA may not be applicable.

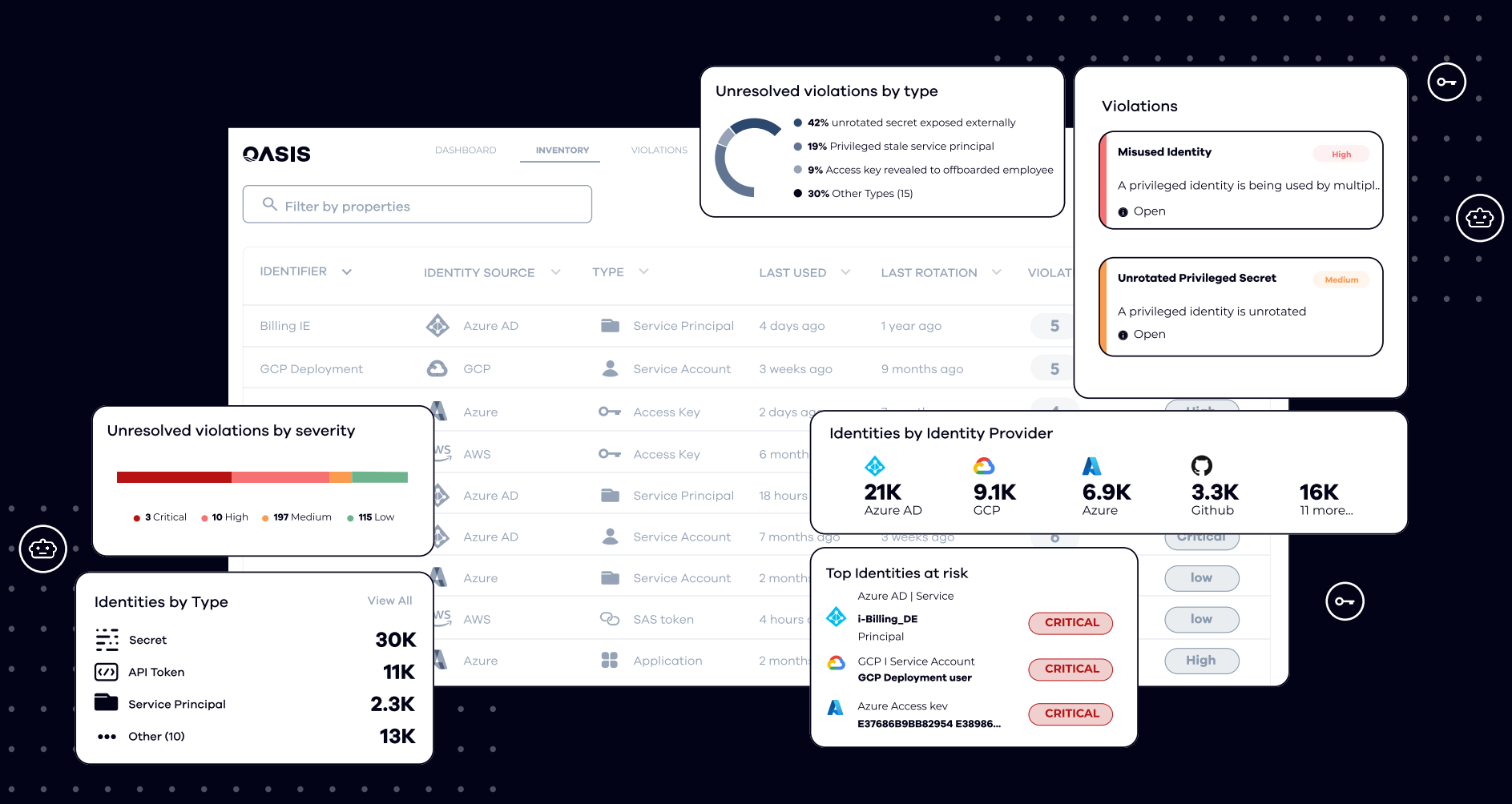
Curious to discover how Oasis is revolutionizing identity security? Schedule a demo today to experience top-notch Non-Human Identity Management firsthand!



About Oasis Security

Oasis Security is the leading provider of Non-Human Identity Management (NHIM) solutions. NHI Management is a huge and unresolved security weakness that is constantly exploited by malicious cyber attackers.

By enabling control over Non-Human Identities, we bridge the gap between devops/R&D and security ensuring our customers elevate their security posture while maintaining highly efficient operations.



Secure All Identities, NHIs First

Don't leave your business vulnerable. Contact Oasis today for a free security assessment and to learn more about how we can protect your assets and reputation

Get a Free Assessment

OASIS