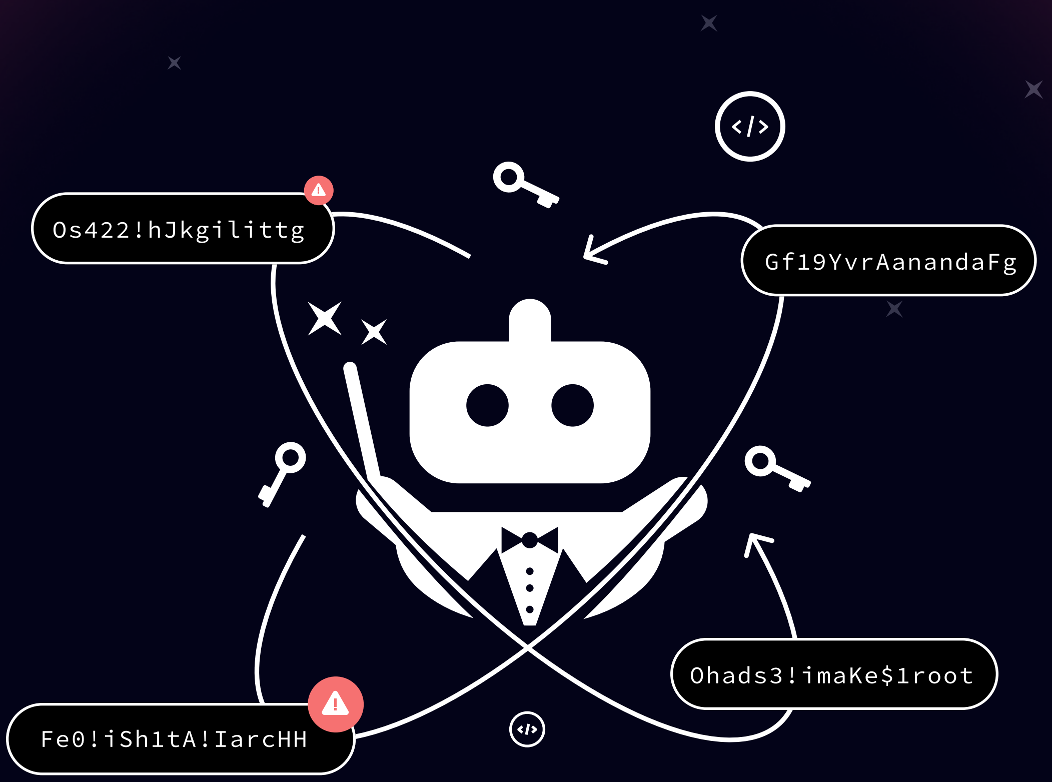
OASIS

White Paper

The Guide To Safe Secret Rotation



Secret Rotation: What It Is and Why It Matters

Secret rotation is the process of periodically updating sensitive values, such as API keys, security credentials, encryption keys, or any other secret necessary to authenticate and allow connections between resources or machines on-premises, in the cloud, or SaaS applications.

Respond to Security Breaches

When Cloudflare discovered that Okta had been compromised, their immediate priority was to rotate all credentials to prevent further exposure. Secret rotation helps mitigate the impact by ensuring that compromised credentials are quickly rendered useless.

Compliance and Audit Readiness

Auditors require proof that organizations manage their identities securely and adhere to necessary standards. While the focus is often on privileged identities, managing all secrets ensures compliance and prevent issues such as lateral movement and maintain overall security hygiene across the organization.

Managing Organizational Changes

When employees join, move within, or leave the company, their permissions must be reassessed and reassigned. This review should include users and roles within specific applications and consider any privileged information and secrets the employee had access to.

Maintaining Business Continuity

Expired secrets can cause applications to break or fall out of sync, necessitating the creation of new secrets and updating configurations to maintain functionality.

Common Pitfalls and Misconceptions

01

I have my secrets vaulted!
Even though most organizations implement processes to ensure everyone uses vaults, these processes are not always enforceable.

Therefore, a tool that shows all secrets, how they are being used, and by whom, is necessary. Regular rotation ensures that even if a secret is compromised, its usability is limited, maintaining overall system security.

02

I have CSPM to manage risk exposure!
Cloud Security Posture Management (CSPM) tools are helpful but they do not replace the need for secret rotation. These tools might detect anomalies, but responding to alerts often requires rotating and managing secrets to mitigate risks. This process can be time-consuming and labor-intensive.

03

I use threat detection tools!
Detection tools like secret scanners can identify shared secrets on platforms like Slack, but they can't cover all possible avenues, such as WhatsApp or email. It's unrealistic to assume that all environments can be completely scanned.

Hence, rotating and managing secrets remains essential, regardless of the detection tools in place. Proactive management ensure that secrets remain secure and minimize the risk of exposure through unmonitored channels.

04

I closed my former employee’s account!
Decommissioning or deleting the account in the authoritative source or Identity Governance and Administration (IGA) system may not stop the former employee's access to a Non-Human Identity (NHI). NHIs, represent resources that can be on-premises or accessible directly from the internet through cloud services. In such cases, NHIs act as the perimeter. If the former employee knows the resource and its secret, they could still gain access from their home.

Challenges of Secret Rotation

Manually updating secrets across multiple applications and services can be labor-intensive and time-consuming, especially as the number of non-human identities grows. The potential for errors is significant.

Mistakes such as forgetting to update a secret in one location or misconfiguring a service can lead to downtime and even production disruption.

Tracking the owner of each secret and determining which secrets need rotation, and ensuring all instances are updated correctly is challenging without the right tools.

Also, legacy or older systems may not support modern secret rotation practices, making the process more complex and risky. Updating or replacing these systems to facilitate secret rotation can be costly and disruptive.

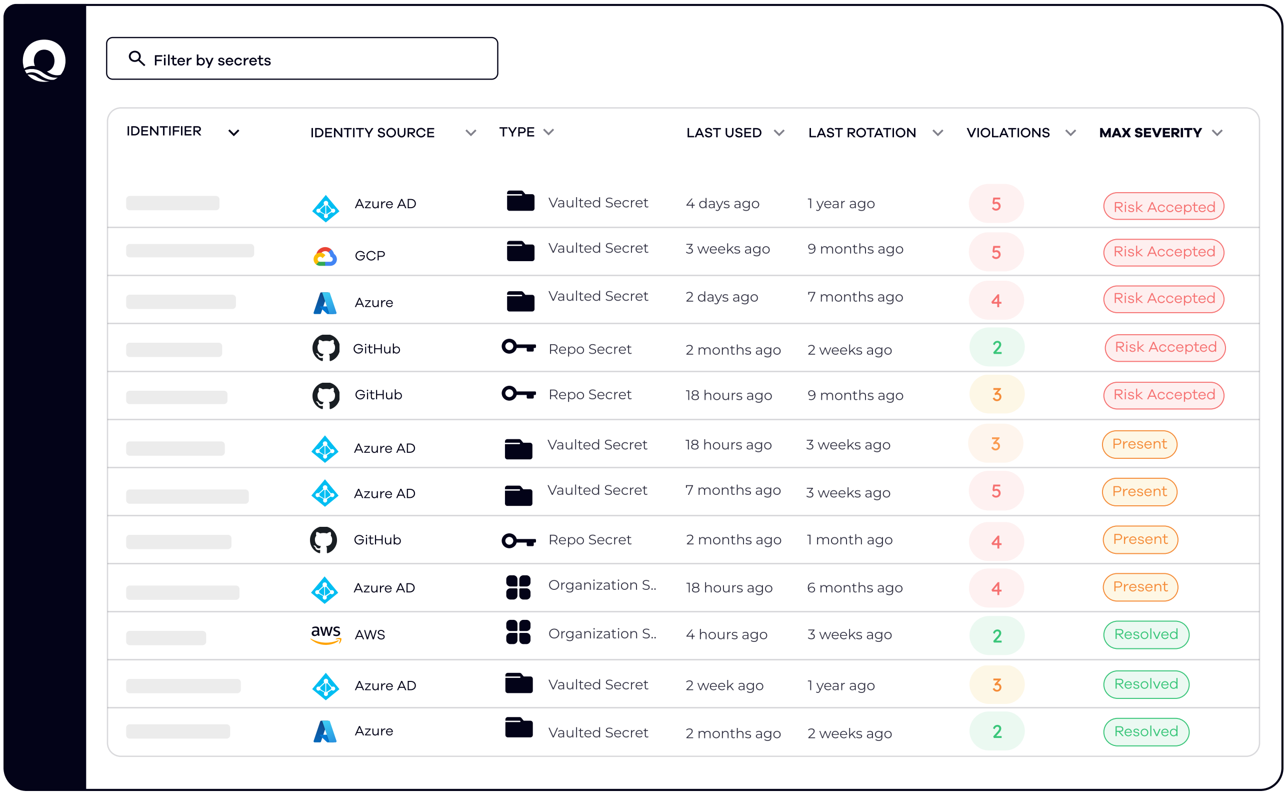
Top challenges

- ⚠ Potential for downtime & disruption
- ⚠ Labor-intensive process
- ⚠ Multi-cloud and vaults
- ⚠ Cloud scale

Solving Rotation with Oasis

We are not a vault or a traditional PAM, which can only manage what they know. Our platform automatically discovers all secrets across your environment, no matter where they are stored—whether in third-party vaults, within your cloud infrastructure, or elsewhere. Furthermore, unlike secret managers, Oasis is an identity-centric solution, which means that, by default, we not only discover a secret, but also the identity that uses it. This is critical to provide you with the insights needed to make rotation safe.

What sets us apart is our integration of powerful posture management with automated remediation and orchestration. We don't just identify risks; we enable you to take action and resolve issues quickly through powerful orchestration that plugs on your infrastructure of choice.



IDENTIFIER	IDENTITY SOURCE	TYPE	LAST USED	LAST ROTATION	VIOLATIONS	MAX SEVERITY
	Azure AD	Vaulted Secret	4 days ago	1 year ago	5	Risk Accepted
	GCP	Vaulted Secret	3 weeks ago	9 months ago	5	Risk Accepted
	Azure	Vaulted Secret	2 days ago	7 months ago	4	Risk Accepted
	GitHub	Repo Secret	2 months ago	2 weeks ago	2	Risk Accepted
	GitHub	Repo Secret	18 hours ago	9 months ago	3	Risk Accepted
	Azure AD	Vaulted Secret	18 hours ago	3 weeks ago	3	Present
	Azure AD	Vaulted Secret	7 months ago	3 weeks ago	5	Present
	GitHub	Repo Secret	2 months ago	1 month ago	4	Present
	Azure AD	Organization S..	18 hours ago	6 months ago	4	Present
	AWS	Organization S..	4 hours ago	3 weeks ago	2	Resolved
	Azure AD	Vaulted Secret	2 week ago	1 year ago	3	Resolved
	Azure	Vaulted Secret	2 months ago	2 weeks ago	2	Resolved

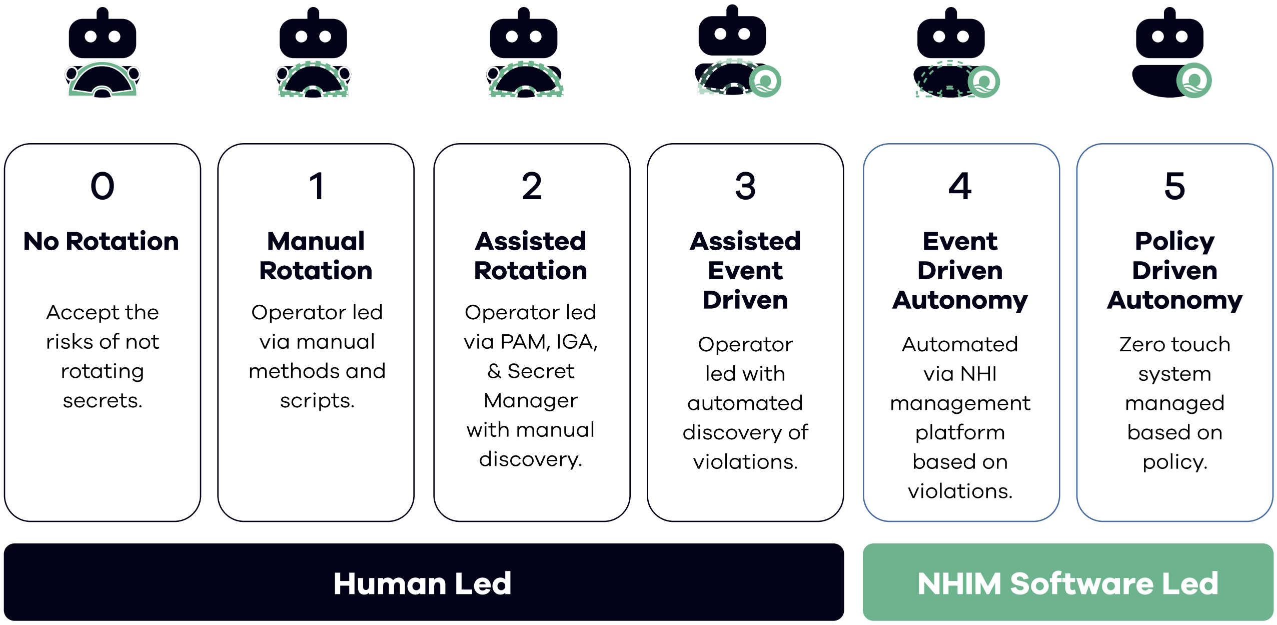
Oasis tailored solution for every Secret Rotation scenario

Oasis offers a comprehensive solution to address the complexities of secret rotation, providing organizations with a range of capabilities to make secret rotation safe and efficient. We recognize the complexities involved in secret rotation and offer solutions tailored to different levels of control and automation.

For those who prefer complete control, our **Manual Rotation** option alerts users when a secret needs rotation and provides a step-by-step guide for manual intervention on the third-party vendor side.

For a more streamlined approach, **On-demand Rotation** simplifies the process with a one-click integration; Oasis Posture Engine identifies policy violations, and after user initiation, handles the secret rotation automatically with the third-party vendor.

For those looking to maximize automation, our **Policy-based Automatic Rotation** allows users to set policies for fully automated, scheduled secret rotations for a single cycle or on a scheduled, permanent basis, ensuring real lifecycle management. These options empower companies to efficiently manage secret rotation based on their specific needs.



0
No Rotation
Accept the risks of not rotating secrets.

1
Manual Rotation
Operator led via manual methods and scripts.

2
Assisted Rotation
Operator led via PAM, IGA, & Secret Manager with manual discovery.

3
Assisted Event Driven
Operator led with automated discovery of violations.

4
Event Driven Autonomy
Automated via NHI management platform based on violations.

5
Policy Driven Autonomy
Zero touch system managed based on policy.

Human Led

NHIM Software Led

Oasis's automation capabilities are unique in several ways

Identity-centric

Oasis rotates secrets with a complete understanding of the NHI that uses them. This approach ensures that rotations are performed safely and do not disrupt operations.

✓ Context-aware. Operates safely without downtime risk

Vault and Cloud Agnostic

Oasis integrates with various secret management systems and automates rotation across multiple cloud providers. This dual flexibility simplifies tracking ownership, determining rotation needs, and ensuring updates are seamless.

✓ Seamlessly plugs on your infrastructure of choice

Policy-based

Predefined policies governing secret rotation ensure consistency, compliance, & security across the org while eliminating human errors, especially at scale. With Oasis, set your internal policies, and the system automatically applies them.

✓ Operates efficiently and effortlessly at cloud scale

Targeted

Oasis streamlines operations by allowing you to focus on the most relevant secrets out of hundreds or thousands, such as rotating those exposed to an offboarded employee, ensuring efficiency and security.

✓ Gets the job done fast

Use Case: Secret Rotation for Leaver and Mover

When an employee leaves a company or changes their role, the impact extends beyond just clearing their desk. Offboarding involves transferring ownership of assets, revoking access to applications, and ensuring all IT assets are recovered. However, NHIs and secrets the employee was exposed to are often left behind and not decommissioned, posing significant security risks.

For instance, if an employee who had **access to sensitive information** leaves, their access must be revoked immediately. Simply decommissioning their identity in your Identity Governance and Administration (IGA) system or source of truth is not enough. It is crucial to review users and roles within specific applications, considering any privileged information and secrets the employee had access to. Oasis ensures that any exposed sensitive information is promptly flagged and managed, providing a comprehensive view of dependencies linked to the offboarded identity.

When employees move to **different roles within the company**, their permissions need to be reassessed and adjusted to prevent excessive access. This process ensures that employees have the appropriate level of access for their new role while minimizing the risk of unauthorized access to sensitive information. Oasis's solution simplifies this process by automating the reassessment and adjustment of permissions, ensuring that only authorized individuals have access to company assets, including non-human accounts and secrets.

Oasis also helps **maintain business continuity** during these transitions. By automating the rotation of secrets associated with offboarded or reassigned employees, Oasis ensures that expired or compromised secrets do not cause disruptions. This proactive approach supports uninterrupted operations and reduces the risk of security breaches.

Key Takeaways

Make regular rotation a default
Regular secret rotation is critical to reduce the window of opportunity to attackers, respond quickly to threats, meet regulatory compliance and ensure workforce access and business continuity.

Vaults and scanners are not enough
Relying solely on vault storage, secret scanners, decommissioning accounts, or monitoring tools is insufficient—regular secret rotation remains crucial to closing security gaps.

Identity context is a pre-requisite to successful rotation
Oasis offers a comprehensive solution to address the complexities of secret rotation, providing organizations with a range of capabilities: manual rotation, on-demand rotation and policy-based automatic rotation

Policy-based automated rotation is key at scale
Oasis provides an automated, identity-centric secret rotation solution that integrates across various vault systems and cloud providers, enhancing security, compliance, and operational efficiency.

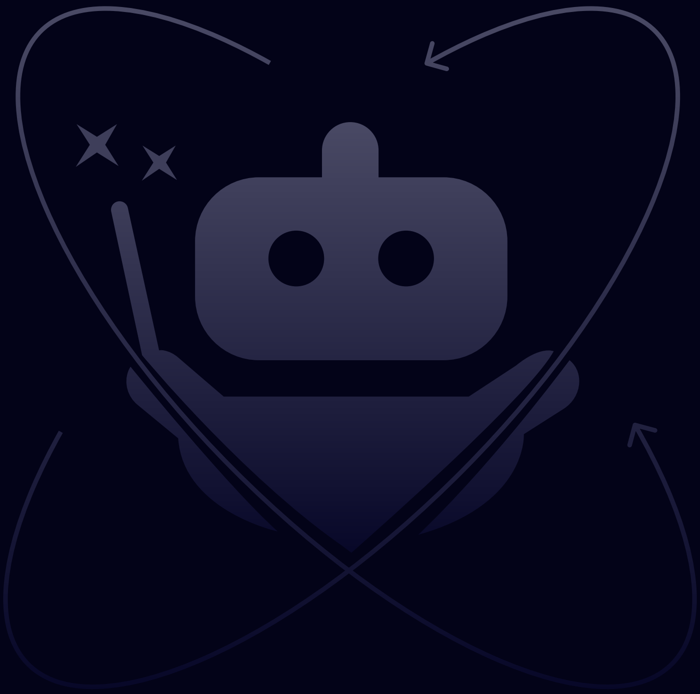
OASIS

Stop worrying.
Start rotating.

Simple, smart, and effective Non-Human Identity management.

Get a Demo

Get a Free Assessment



Start now

Read our blog series
Read our Safe Secret Rotation page

Contact us at sales@oasis.security or visit
our website at oasis.security