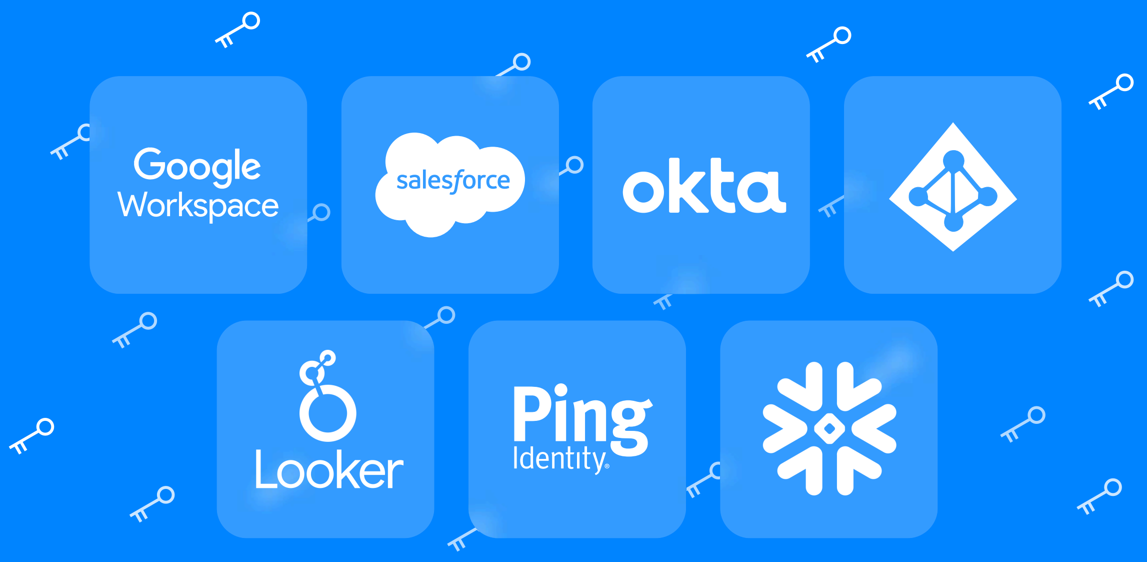
Astrix

Non-Human Identity & Access Management

Astrix helps you extend IAM & IGA programs to non-human identities, from inventory and posture to ITDR, lifecycle management and remediation.



According to Astrix research

salesforce

50%

Of active NHIs are unused

Google Cloud

33%

Of active NHIs are unused

> “Astrix strengthens our identity security program by providing us with continuous visibility and governance over thousands of non-human identities across the entire organization, from the corporate to the production environments.”

PAGAYA

Yaniv Toledano
CISO, Pagaya

The IAM layer is at risk

Attackers exploit ungoverned NHIs

Okta, Microsoft, Snowflake and GitHub all got breached via NHIs in the past 2 years.

NHI sprawl

A company with 1,000 employees has roughly 20,000 NHIs granting sensitive access to core environments.

Existing solutions are not built for NHIs

CASB, MFA, ITDR and IGA tools have very limited (if any) coverage of the NHI attack surface.

Existing solutions are not built for NHIs

Ungoverned machine credentials

Tools like MFA, SSO and password managers protect usernames and password logins. We help you monitor and secure programmable access credentials like API keys, OAuth tokens, service accounts and SSH keys.

Limited threat detection & response

Existing Identity Threat Detection and Response (ITDR) tools specifically monitor user identity systems and user activity logs for attacks. Astrix helps extend ITDR to non-human identities and monitor them for misuse and compromise.

Secure user access only

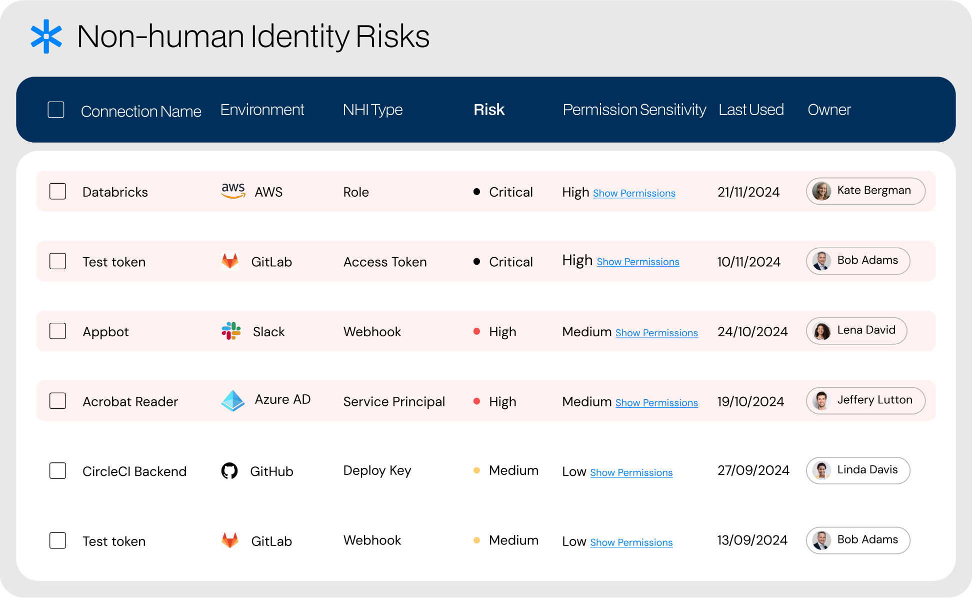
Identity Governance and administration (IGA) solutions manage only user identities and secure user access. Astrix provides the visibility and context required to secure non-human identity, access, and activity.

Context-less secrets protection

Vaults and scanners lack risk prioritization. Astrix finds exposed secrets, checks their validity, usage, and permissions – enabling you to prioritize risks and prevent threats.

Secure the biggest identity blindspot with Astrix

NHI visibility & posture



Non-human Identity Risks

☐	Connection Name	Environment	NHI Type	Risk	Permission Sensitivity	Last Used	Owner
☐	Databricks	AWS	Role	● Critical	High Show Permissions	21/11/2024	Kate Bergman
☐	Test token	GitLab	Access Token	● Critical	High Show Permissions	10/11/2024	Bob Adams
☐	Appbot	Slack	Webhook	● High	Medium Show Permissions	24/10/2024	Lena David
☐	Acrobat Reader	Azure AD	Service Principal	● High	Medium Show Permissions	19/10/2024	Jeffery Lutton
☐	CircleCI Backend	GitHub	Deploy Key	● Medium	Low Show Permissions	27/09/2024	Linda Davis
☐	Test token	GitLab	Webhook	● Medium	Low Show Permissions	13/09/2024	Bob Adams

Real-time discovery

Continuously inventory provisioned or in-use service accounts, secrets, OAuth apps, IAM roles, API keys and other NHIs. Complete the picture with the third-party vendors behind them, owners, and usage.

Dynamic access analysis

Usage analysis and holistic visibility help you easily understand if an NHI is redundant (not in use), stale or over-privileged, what it's connected to, and how to rotate or remove it without breaking anything.

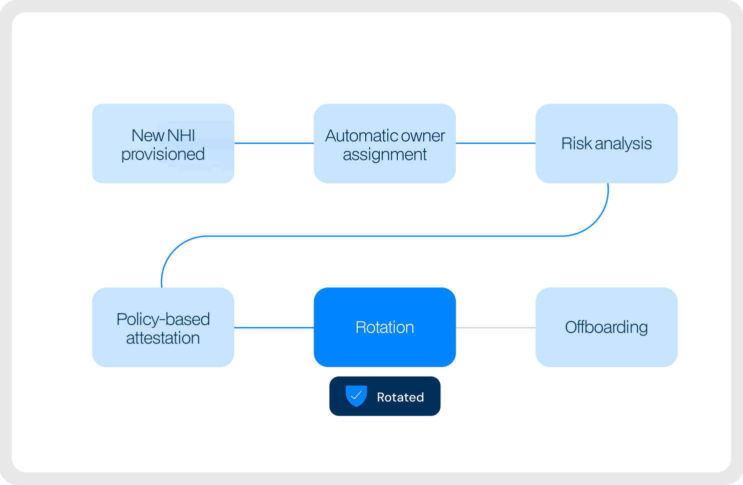
Actionable risk scoring

Prioritize remediation efforts through rich context about services and resources an NHI can access (Google Drive, S3, Git repos, Slack channels), its permissions (full access, read, add), usage, and its consumers (internal users and third-party vendors).

Out-of-the-box remediation

Remediate with a click of a button using out-of-the-box policies for posture and incidents. Easily build custom workflows to fit your security needs.

NHI lifecycle management



NHI ownership

Streamline remediation and verification by easily assigning ownership for each NHI to their human owners and users.

Policy-based attestation

Ensure NHIs comply with your organizational policies using attestation workflows based on the NHI's access permissions, risk, usage, and expiration or rotation.

NHI decommissioning

Automate NHI offboarding when an employee leaves, when a supplier is untrustworthy or when the NHI is no longer in use.

Non-human ITDR

Behavioral analysis

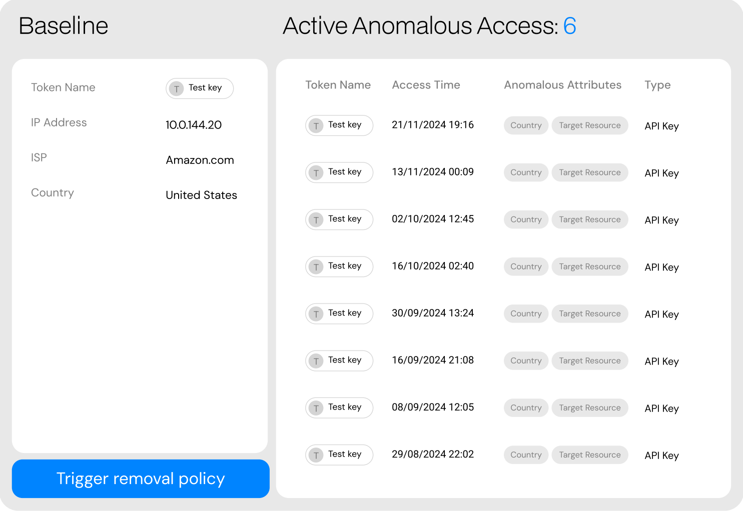
AI-based threat engines detect abuse of NHIs based on anomaly indicators such as unusual IP, user agent, and API activity. Detailed investigation guides and activity logs help you respond swiftly.

Vendor supply chain attacks

Drastically expedite incident response when one of your vendors is compromised. Map every associated NHI, see everything it's connected to and what it's used for to quickly rotate or remove without breaking business processes.

Policy deviations

Prevent NHI abuse by enforcing organizational policies on NHIs. Use your existing tools to mitigate policy deviations such as access from forbidden geos, number of API calls and more.



Baseline

Token Name	T Test key
IP Address	10.0.144.20
ISP	Amazon.com
Country	United States

Active Anomalous Access: 6

Token Name	Access Time	Anomalous Attributes	Type
T Test key	21/11/2024 19:16	Country Target Resource	API Key
T Test key	13/11/2024 00:09	Country Target Resource	API Key
T Test key	02/10/2024 12:45	Country Target Resource	API Key
T Test key	16/10/2024 02:40	Country Target Resource	API Key
T Test key	30/09/2024 13:24	Country Target Resource	API Key
T Test key	16/09/2024 21:08	Country Target Resource	API Key
T Test key	08/09/2024 12:05	Country Target Resource	API Key
T Test key	29/08/2024 22:02	Country Target Resource	API Key