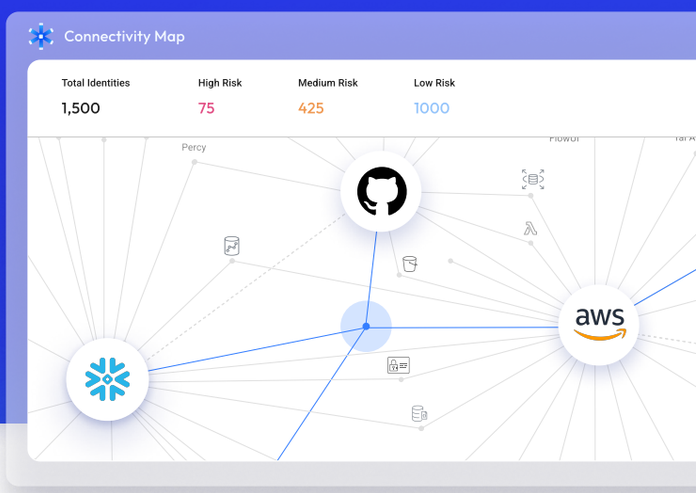
Astrix

Securing non-human identities & access in AWS

Non-human identities like IAM users, roles, service accounts, external keys and secrets provide powerful access to sensitive resources in your AWS.

Only Astrix tells you **what** permissions NHIs have, to **which** resources, and **who** is behind them.



Key Benefits

Discover NHIs in real-time

Manage NHI access with continuous inventory of users, roles, service accounts and keys. Map their interconnectivity within your AWS and with external platforms and suppliers. See the owners of each NHI and its usage.

Manage the lifecycle of NHIs

Enable policy-based attestation, alerts and offboarding of NHIs by managing their lifecycle, from the moment they are created through permission changes, rotation events, revocations and expirations.

Easily respond to third-party breaches

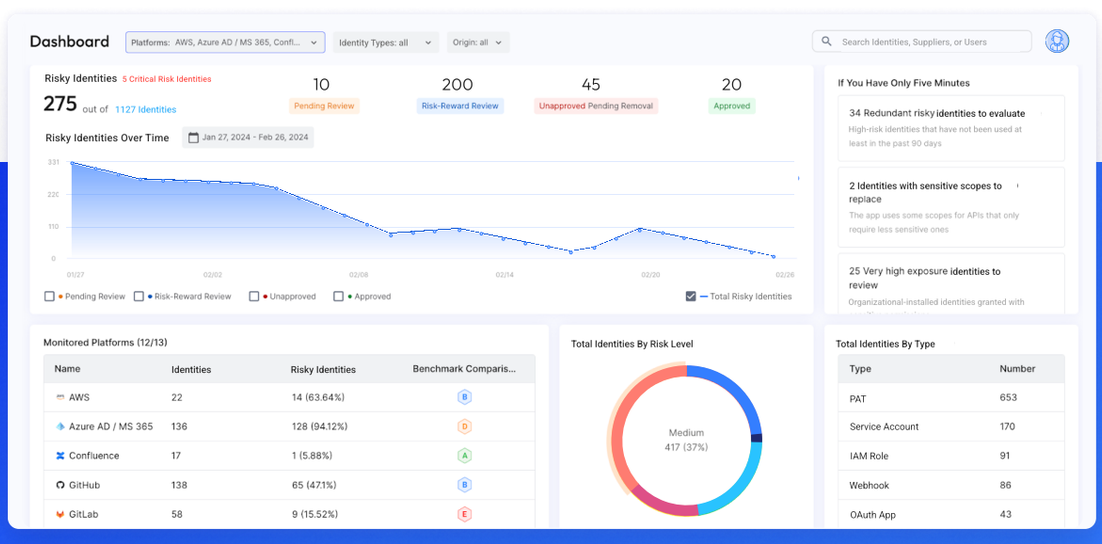
Expedite IR efforts when a supplier is breached. Map every associated NHI, and see everything it's connected to so you can remove or rotate in a jiff.

Respond to suspicious NHI behavior

Detect attacks and respond to real-time alerts on anomalous activity and lifecycle events such as permission changes, owners and suppliers.

Easily remediate NHI risks

Use out-of-the-box policies, workflows and rich context to remediate risks across your IaaS and SaaS environments. Reduce friction and maintain productivity by integrating Astrix with your existing security stack.



Key Capabilities

VISIBILITY & POSTURE

Real-time discovery
Get a continuous inventory of provisioned or in-use service accounts, roles, entitlements and keys. Complete the picture with the owners, usage or third-party suppliers behind them.

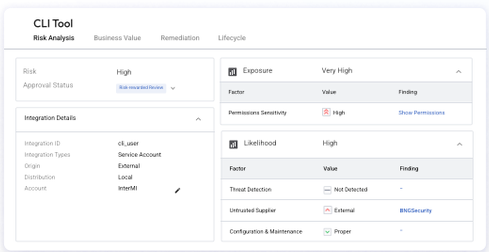
Actionable risk modeling
Prioritize risk with context into the services & resources an NHI can access (API Gateway, S3, secret managers), the permissions it has (full access, read, add), and internal or external use.

Supply chain breach likelihood
Astrix's likelihood engine rates suppliers according to their reputation, configuration, maintenance and anomaly detection - highlighting the ones most likely to get breached.

Secret security
See and manage all your secrets across secret managers and cloud environments. Understand the secret permissions, owner and the obtaining service.

NHI ownership
Streamline remediation and verification by easily assigning ownership for each NHI to their human owners and, if external, the third-party supplier.

NHI usage & redundancy
Usage analysis and holistic visibility across environments helps you easily understand if an NHI is used, what it's connected to, and how to rotate or remove it without breaking anything.



The drill down of an identity's risk and business context, as well as remediation guidance and lifecycle info.

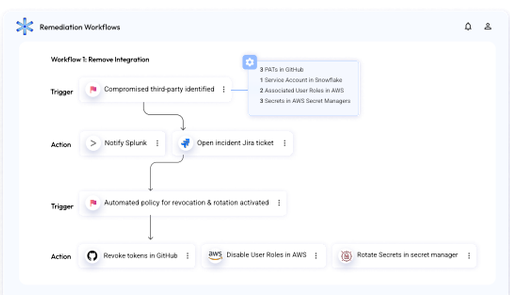
THREAT DETECTION & RESPONSE

Behavioral threat detection
Get alerted on potential breaches in real time. AI-based threat engines detect abuse of NHIs based on parameters such as unusual IP, user agent and API activity.

Threat mitigation
Quickly respond to potential breaches using anomaly investigation guides and activity logs, outlining the anomaly and the baseline along with suggested response steps.

Automatic end-user communication
Remediate faster with end-user feedback. Automatically gather business justification from users behind NHIs so you can remove risky access without interfering with business processes.

Integrations with existing tech stack
Maintain productivity by integrating Astrix with your existing security stack. Get a Slack notification, automatically open Jira tickets, use API automations or work with your SIEM.



Purposely built for the NHI attack surface

Existing cloud security solutions are not built for the NHI challenge. Here's why:

	ASTRIX	CSPM	CIEM
Identity context	**Deep visibility and context of non-human identity lifecycle, ownership and behavior.**	Focused only on cloud configurations. Lack identity capabilities such as secret inventorying across secret managers.	Focused on entitlements for internal cloud identity configs. Lack visibility into crucial identity aspects like ownership and third-party suppliers.
Behavioral analysis	**Real-time anomaly detection, identifying NHI abuse and providing response guidance.**	Focused only on posture elements. Lack behavioral analysis capabilities.	Focused only on static data like permissions. Lack behavioral analysis capabilities.
Holistic context	**Holistic visibility across IaaS SaaS and on-prem, correlating your entire NHI connectivity to provide deeper context and better prioritization.**	Monitor only cloud environments.	Monitor only cloud environments.