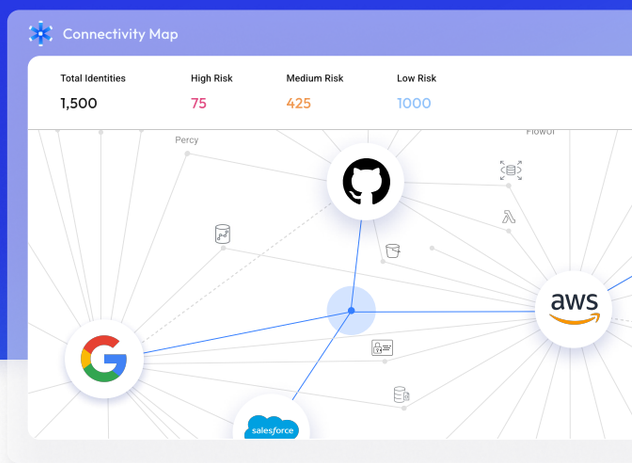
Astrix

# Securing non-human identities with Astrix

Astrix helps identity and security teams secure, manage, and govern non-human identities across IaaS, SaaS, PaaS, and on-prem environments.




## Key Benefits

### Discover NHIs in real-time

Secure NHI access with continuous inventory of service accounts, OAuth apps, IAM roles, and API keys. Map their interconnectivity within your environments, external apps, and suppliers.

### Prioritize NHI risks

Attend to the top 5% risks using threat algorithms based on parameters such as services and resources an NHI can access, permissions, behavioral analysis, and internal or external use.

### Manage the lifecycle of NHIs

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

### Quickly respond to third-party supplier breaches

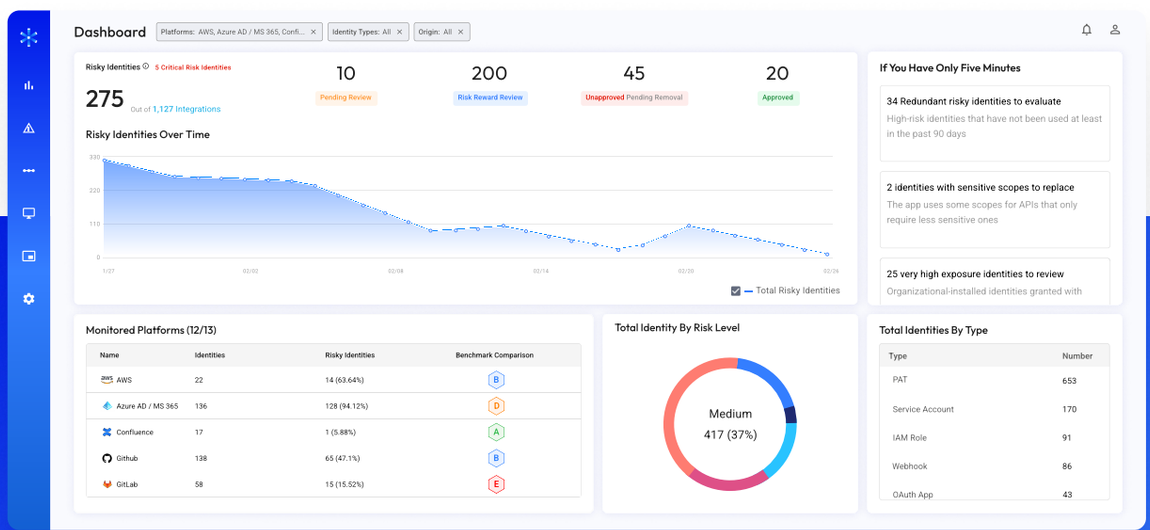
Expedite IR efforts when a supplier is breached. Map every associated NHI, and see everything it's connected to so you can remove or rotate in a jiff.

### Detect suspicious NHI behavior

Easily respond to potential attacks with real-time alerts, workflows, and investigation guides on anomalous NHI activity such as unusual user agent, geo, and API activity.

### Remediate & automate

Use out-of-the-box policies, custom workflows and context to remediate NHI risks across your environments. Reduce overhead with native SIEM, SOAR and ITSM integrations.

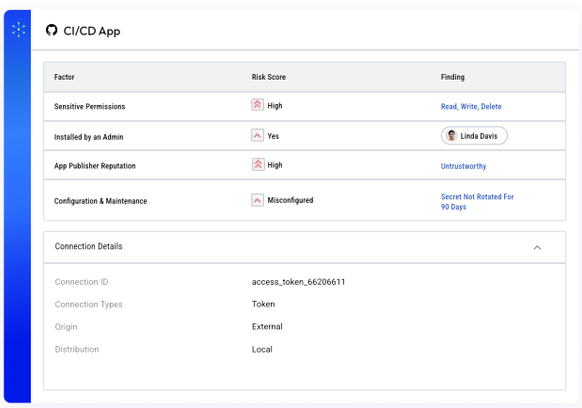


# Key Capabilities

## VISIBILITY & POSTURE

### Discover NHIs in real-time
Get a continuous inventory of provisioned or in-use service accounts, secrets, OAuth apps, IAM roles, API keys and other NHIs. Complete the picture with the owners, third-party vendors behind them and usage.

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




### NHI usage & redundancy
Usage analysis and holistic visibility across environments help you easily understand if an NHI is used, 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).

### 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 be breached.

### Next-gen secret scanning
Map all your exposed secrets across secret managers and cloud environments. Prioritize their risk and easily rotate or revoke with context into which service the secret is used for, its permissions, owner, and rotation policy.

## ITDR & REMEDIATION

### Behavioral threat detection
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.

### End-user communication & remediation
Remediate faster with end-user feedback and self-remediation. Automatically gather business justification from users behind NHIs and allow them to remove risky access themselves, without interfering with business processes.

### Enterprise integrations
Integrate Astrix with your existing security stack to reduce overhead. Use Slack notifications, automatically open Jira tickets, use API automations, or work with your ITSM, SIEM and SOAR systems.

### 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.

### 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.