Astrix

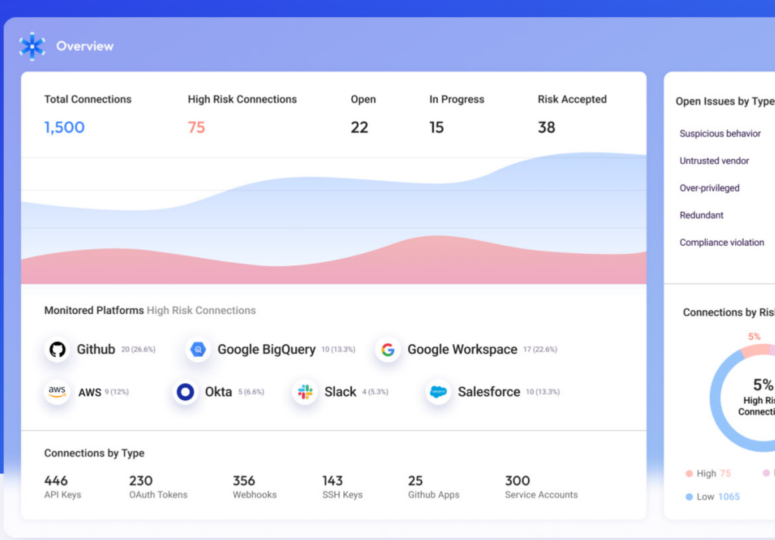
Securing Non-Human Identities

The Astrix security platform enables you to manage and secure service accounts, API keys, OAuth apps and other NHIs, providing a holistic non-human identity security solution across business and engineering environments.

Book a demo →

RSAC Innovation Sandbox 2023 FINALIST

Gartner COOL VENDOR 2023



Overview

Total Connections	High Risk Connections	Open	In Progress	Risk Accepted
1,500	75	22	15	38

Monitored Platforms High Risk Connections

Github 20 (26.6%)
Google BigQuery 10 (13.3%)
Google Workspace 17 (22.6%)
AWS 9 (12%)
Okta 5 (6.6%)
Slack 4 (5.3%)
Salesforce 10 (13.3%)

Connections by Type

446	230	356	143	25	300
API Keys	OAuth Tokens	Webhooks	SSH Keys	Github Apps	Service Accounts

Open Issues by Type

Suspicious behavior
Untrusted vendor
Over-privileged
Redundant
Compliance violation

Connections by Risk

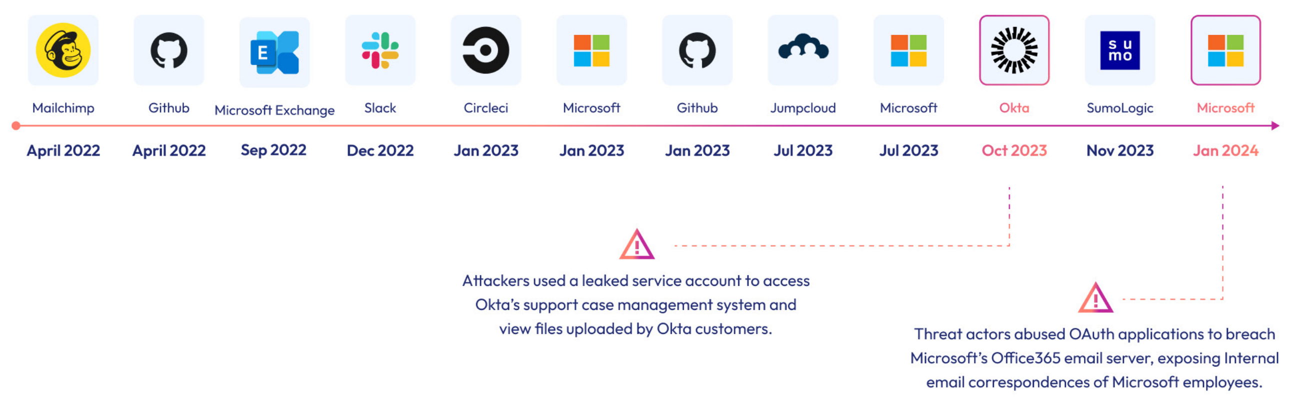
Trusted by industry leaders

Figma · NetApp · priceline · agoda · workato · hopper · Guesty · S&P 500 REIT Company · FINTECH COMPANY

THEC CHALLENGE

The biggest identity blindspot: 10,000 non-human credentials for every 1,000 employees

While 49% of breaches involve stolen credentials, 90% of credentials are not protected by existing IAM solutions. Service accounts, API keys, OAuth apps, SSH keys and other NHIs hold privileged access to enterprise environments and remain under the radar. Recent attacks reveal attackers use access keys, service accounts, and secrets as a backdoor into companies' most sensitive core systems and data.



Attackers used a leaked service account to access Okta's support case management system and view files uploaded by Okta customers.

Threat actors abused OAuth applications to breach Microsoft's Office365 email server, exposing Internal email correspondences of Microsoft employees.

THE ASTRIX PLATFORM

Gain control over the non-human identity layer

Our agentless solution enables you to inventory and manage NHIs across environments, allowing you to prioritize and remediate risks that expose you to supply chain attacks and data breaches.

Inventory & posture

Discover shadow NHIs and their business context. Get a prioritized list of their associated risks: over-privileged & sensitive access, untrusted vendors, etc.

Threat Detection

Detect and respond to abuse of access tokens and suspicious NHI activity in real-time using behavior analysis.

Rapid Remediation

Automatically remediate NHI risks using out-of-the-box policies & workflows integrated to your security stack.

Lifecycle Management

Easily manage the lifecycle of every non-human identity – from creation to expiration and rotation.

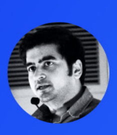
agoda

> "With the rise in automation and new API-based integrations, Astrix's ongoing monitoring and threat detection of what is accessing our environments became a key capability in our arsenal."

Yaron Slutzky
CISO, Agoda

Figma

> "Figma was built on the browser. As a cloud-native company, we work tirelessly to ensure that all of our software is secure and stable for our global users. Astrix bolsters our security promise by effectively monitoring risk from SaaS integrations."



Devdatta Akhawe
Head of Security,
Figma

Safely unleash the power of connectivity, automation and GenAI

To increase productivity and streamline processes, engineering, IT and business units need the freedom to connect third-party apps, internal services and machines to enterprise environments. Astrix allows you to make the most of your interconnected cloud, without compromising security.

Extend IAM programs to non-human identities

Machine credentials outnumber user credentials, and are more privileged. Extend IAM programs to non-human identities from discovery and risk prioritization to threat detection and response.

Discover & secure shadow AI

71% of employees use GenAI at work.* Astrix allows you to discover and secure GenAI services connected to your IaaS and SaaS environments.

Reduce shadow third-party access

Existing TPRM programs assess only a fraction of your digital supply chain. Astrix discovers and secures all third party apps and vendors connected to your environment, including unknown unknowns.

Secure non-human access to engineering environments

A developer creates on avg 10 machine credentials every week. Secure SSH certificates, service accounts, PATs and secrets in AWS, GCP, GitHub, Snowflake, Azure, etc.

aws · GitHub · Azure · Google Cloud · workato · salesforce · slack · Google Workspace · Google BigQuery · okta · snowflake · Office 365 · workday · ATLASSIAN · GitLab · +

We secure NHIs across SaaS, IaaS and PaaS environments

From Salesforce and Office 365 to GitHub, AWS, Azure and BigQuery, we ensure your environments are protected from NHI risks.

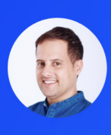
AWARDS & CERTIFICATIONS

Astrix meets the highest industry standards

AICPA SOC 2 · THE WHITE HOUSE WASHINGTON · RSAC Innovation Sandbox 2023 FINALIST · Gartner COOL VENDOR 2023 · GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

Guesty

> "API keys, OAuth tokens, and service accounts are powerful credentials and should be protected as vigorously as user passwords. Astrix has helped us to take control over the app-to-app access layer for the first time."



Gilad Solomon
Head of IT & Information
Security, Guesty

hopper

> "Thanks to Astrix's behavioral analysis, we get alerts about suspicious connections in real-time and can immediately respond to incidents of stolen or abused tokens."

Hannu Visti
Director of Information
Security, Hopper

BACKED BY

KMEHIN VENTURES · F2 · crv · Bessemer Venture Partners · venrock · CYBERFUTURE Global CISO Investment Alliance

Astrix

To learn more and see Astrix in action visit
www.astrix.security