Securden

NHI Security Platform

Discover,assign ownership, and secure non-human identities across your cloud, code, and server environments.



- ✓ Discovery
- ✓ Inventory and ownership
- ✓ Risk assessment
- ✓ Remediation
- ✓ Audit and reporting



Find identities and secrets across your environment

Securden NHISecurity Platform connects to your cloud accounts, code repositories, web servers, and Linux machines to build one inventory of the non-human identities and secrets running there. Each identity gets an owner and a risk assessment. Each secret is classified and assessed, then rotated directly or remediated through a guided process.

Discover across cloud, code, & servers.

Securden connects to AWS, Azure, GitHub, Bitbucket, IIS Manager, and Linux devices. Connections are agentless, use each provider's APIs, and run continuously.

Inventory non-human identities.

Discover and classify IAM users and roles, service accounts, service principals, personal access tokens, OAuth applications, and other non-human identities.

Find secrets in the same pass.

Find credential pairs, API keys, OAuth tokens, SSH keys, JWT secrets, access key pairs, database credentials, and other secrets in the same discovery process.

Define your own detection rules.

Detection uses built-in rules for common credential formats. Add your own for formats specific to your environment, and exclude file types from scans.

For security engineering, DevOps, platform, and identity and access management teams.

Securden

Unified PAM

Know what puts an identity at risk, then fix it

Discovering anidentity is only the firststep.Security teams also need to know what it can reach, whether its credentials are a liability, and what to do about it first.



Assess risk in context

Every identity is assessed when it is discovered. The score considers its blast radius, meaning the secrets it can reach, together with its permissions, credential age and strength, last activity, and ownership.

See why an identity is at risk

Each identity and secret carries the specific conditions behind its score, such as an access key that is 180 days old, console access without multi-factor authentication, or rotation left switched off.

Know what to fix first

Every identity carries a recommended first action, followed by the checks needed to resolve the issue safely. Confirm the owner. Review the permissions. Replace or rotate the credential.

Remediate credentials

Rotate credentials that can be changed through the connected provider directly from Securden. Where one API call cannot replace a credential safely, follow a staged path instead. AWS, for example, never returns the value of an access key after it is created.

Audit & reporting:

Securden records the user, source IP address, time, and reason behind security-sensitive actions, including every time a secret value is viewed. Three prebuilt reports cover secrets without rotation, high-risk identities, and identities without an owner, exportable to PDF, CSV, and XLSX.

Built on Securden Unified PAM

Securden NHI Security Platform is delivered as part of Securden Unified PAM. Credential vaulting, privileged session management, endpoint privilege management, and the wider privileged access capabilities are available from the same deployment and are managed in the Unified PAM interface.

See the non-human identities running in your environment, and who owns them.

Book a demo →

Securden

2810 N Church St, PMB 75693, Wilmington, Delaware 19802-4447 | support@securden.com

USA: +1 844 228 0327 | UK: +44 203 868 6147