Securden

NHI Security Platform

Discover, secure, and govern every non-human identity across your cloud, on-premises, hybrid, and DevOps environments

A single control plane to discover the service accounts, keys, tokens, and workload identities running in your environment, assign an owner to each one, assess its risk, remediate what it finds, and manage certificates end to end.

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

Product Datasheet | **SaaS, On-Premises, and Private Cloud Deployment**

Product Overview

Securden NHI Security Platform discovers non-human identities and the secrets they use across cloud accounts, code repositories, web servers, and Linux devices. It establishes ownership, assesses identity and credential risk, guides remediation, and manages certificates through their lifecycle.

Platform Goal	Deployment Model	Primary Security Outcome
Discover, own, assess, secure, and remediate non-human identities, secrets, and certificates across cloud, code, and server environments.	SaaS, on-premises, and private cloud. Delivered within Securden Unified PAM.	Eliminate unowned machine identities, retire credentials left exposed in code or running years past rotation, and prevent outages caused by untracked certificate expiry.

Core Capabilities

Capability Area	Technical Functionality
Data Source Connectivity	Connects to cloud platforms, git repositories, web servers, and Linux devices. Agentless, through source-provider APIs.
Non-Human Identity Discovery	Discovers and classifies non-human identities across connected sources. Each identity carries its type, source, environment, status, severity, creator, ownership, and multi-factor authentication state where available.
Secret Discovery and Classification	Discovers secrets across connected sources and classifies them into categories. Detection uses built-in and customer-defined PCRE rules, with file-extension exclusions to cut scan time and false positives. Each finding carries source location, environment, entropy score, severity, and last access information where available.
Ownership Management	Assigns a separate business owner and technical owner to every identity and secret.

Capability Area	Technical Functionality
Risk Assessment	Assesses identities and secrets automatically at discovery and on demand. Produces a risk score with named findings, including blast radius across the identity's reachable secrets and resources.
Credential Rotation	Rotates supported credentials directly at the source provider.
Remediation	Surfaces the best next action per identity, with provider-specific hardening guidance and staged remediation where a credential cannot be rotated without updating the workloads that use it.
Certificate Lifecycle Management	Creates certificate signing requests, issues certificates through private and public authorities, automates ACME issuance and renewal, deploys certificates, maintains inventory, and tracks expiry.
Audit and Reporting	Audit trails across data sources, identities, secrets, and certificate management. Six prebuilt reports with PDF, CSV, and XLSX export.
Relationship Visualization	Shows relationships between identities, secrets, and their access paths.

Extended Platform Capabilities

UPAM marks a capability of the Securden Unified PAM platform, available to every NHI Security deployment because NHI Security ships within Unified PAM. These are managed through the Unified PAM interface and operate independently of NHI discovery.

Capability	Detail
Secrets Vaulting [UPAM]	Stores passwords, API keys, tokens, SSH keys, and certificates in an AES-256 encrypted vault with policy-based access control.
Cloud Entitlement Management [UPAM]	AWS and Azure entitlement visibility, identification of excessive or unused privileged policies, and reduction of standing cloud permissions.
Just-in-Time Privileged Access [UPAM]	Time-bound, approval-controlled access replacing standing privileged credentials.

Capability	Detail
Privileged Session Recording [UPAM]	Recording and playback of interactive RDP, SSH, and SQL sessions for administrators who manage the systems behind your non-human identities.
Endpoint Privilege Management [UPAM]	Removal of local administrator rights and just-in-time elevation on the endpoints and build servers where automation identities originate.
Vendor Privileged Access [UPAM]	Time-bound remote access for third parties and managed service providers, without VPNs or standing credentials.

Supported Data Sources

Category	Sources
Cloud Platforms	AWS, Microsoft Azure
Git Repositories	GitHub, Bitbucket
Web Servers	Internet Information Services (IIS) Manager
Operating Systems	Linux devices
Authentication	Access key, service principal, OAuth, platform app, or other source-specific method

Identities, Secrets, and Risk

Identity types discovered

Group	Types
Cloud and directory	IAM User, IAM Role, Service Account, Service Principal
Automation and CI/CD	VCS Bot, CI/CD Identity, Actions Runner, Repository Webhook, Deployment Environment

Group	Types
Keys and tokens	Deploy Key, SSH Signing Key, SSH Authentication Key, Personal Access Token
Applications and integrations	GitHub App, OAuth Application, Workspace Integration, Ruleset Bypass Integration
Scopes and resources	Repository, Organization or Workspace, Project or Team, Codespace

Category	Types
Secret categories	Credential Pair, API Key, OAuth Token, SSH Key, JWT Secret, Certificate, Access Key Pair, Encryption Key, Generic Secret, Database Credential.

Risk assessment

Area	Detail
Identity risk factors	Permission, credentials, activity, ownership, and blast radius, meaning the number of secrets and resources the identity can reach.
Secret risk factors	Credential strength, rotation status, severity, and expiry.
Security findings	Names the specific security condition behind the score rather than presenting a number alone. Examples returned by the product: access key older than 180 days, console access without multi-factor authentication, automated rotation not enabled.
Secret value handling	Discovered secret values are stored encrypted in the Securden database. Every retrieval is logged with the user, originating IP address, timestamp, and stated reason.

Remediation

Path	Detail
Secret Insights	Shows how exposed each secret is, judged on how strong it is, whether it rotates, how serious it is, and when it expires.
Provider-aligned remediation	Gives the steps for replacing that credential on that provider, in the order that keeps everything working. A four-point security checklist to clear before you start, and links to the provider's own documentation.

Certificate Lifecycle Management

Area	Detail
Certificate signing requests	Created from reusable templates, with configurable key algorithm, key size, signature algorithm, key store type, and validity period.
Private certificate authority	Create and manage a private root certificate authority for internally signed certificates.
Public certificate authorities	GoDaddy, The SSL Store, DigiCert, GlobalSign, Sectigo, Entrust, emSign.
ACME providers	Let's Encrypt, Buypass Go SSL, ZeroSSL, Telia, and any custom ACME-compatible provider. Certificates issued through ACME are renewed automatically.
Certificate inventory	Certificates created in Securden, discovered from connected sources, or added manually.
Certificate deployment	Push to Windows systems and the Microsoft Certificate Store.
Expiry tracking	Upcoming expirations ordered by remaining validity, with expired and soon-to-expire certificates surfaced.

Audit and Reporting

Area	Detail
Audit coverage	Data sources, identities, secrets, and certificate management.
Logged actions	Discovery synchronization, connection and authorization activity, identity creation, owner assignment, security assessment, secret retrieval, certificate addition, and certificate signing request creation.
Recorded per entry	Entity and source, action, user, originating IP address, timestamp, and stated reason.
Prebuilt reports	Secret Rotation, High Risk NHI, Identity Ownership, Expiring Certificates, Expired Certificates, and Self-Signed Certificates.
Export formats	PDF, CSV, and XLSX.

Architecture and Deployment

NHI Security runs within Securden Unified PAM and inherits its application, database, gateway, availability, and disaster recovery architecture.

Area	Detail
Deployment models	SaaS, on-premises, and private cloud.
Discovery cadence	Continuous synchronization with on-demand re-sync per source.

Server requirements, installation, backend database, sizing, high availability, disaster recovery, and gateway architecture follow the Securden Unified PAM technical specifications.

Security and Encryption

Security Area	On-Premises	SaaS
Data encryption	Sensitive data encrypted at the application level using AES-256 before storage.	Customer data encrypted using AES-256 and stored in segregated encrypted database storage.
Encryption key management	Unique random installation key kept separately from encrypted data and available only during startup.	Unique key per customer segment managed through Amazon KMS, with cryptographic operations in an AWS CloudHSM cluster.
Database protection	Localhost-only access by default, with IP allow-listing for supported high availability configurations.	Per-customer data segregation with separate encryption keys.
FIPS mode	FIPS-compliant mode available.	FIPS-compliant mode available.
Certificate handling	Self-signed certificate by default; CA-signed certificate can be installed.	Managed by Securden.
Access governance	Granular role-based access control, request and release workflows, and audit trails.	Granular role-based access control, request and release workflows, and audit trails.
Certifications and testing	ISO/IEC 27001, SOC 2 Type II, GDPR alignment, and periodic third-party penetration testing.	ISO/IEC 27001, SOC 2 Type II, GDPR alignment, and periodic third-party penetration testing.

Identity, Access, and Integrations

Integration Area	Supported Options
Platform authentication	Local accounts, Active Directory, Microsoft Entra ID, LDAP, and RADIUS.
Single sign-on	SAML 2.0 for Okta, Microsoft Entra ID, ADFS, OneLogin, PingIdentity, Google Workspace, and other SAML identity providers.

Integration Area	Supported Options
Directory-based authentication	Authentication through the configured directory without storing directory user passwords.
Multi-factor authentication	TOTP applications including Google and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP, and RADIUS-based providers.
Role-based access control	Predefined and custom roles, request and release workflows, and time-bound sharing.
API access	REST API with token-based authentication
SIEM integration	Audit event forwarding to SIEM platforms.
ITSM integration	ServiceNow and Jira for approval workflows.
Client access	Browser, desktop applications for Windows, Mac, and Linux, iOS and Android applications, and browser extensions.
Supported browsers	Chrome, Edge, Firefox, and Safari.

Scale and Resilience

Area	Detail
High availability	Secondary application server with automatic failover and read-only replica support.
Database clustering	Microsoft SQL Server clusters supported.
Disaster recovery	Scheduled full database backup to a remote destination, with a minimum hourly interval.
Distributed architecture	Application servers and remote gateways deployable across networks.
Sizing	Follows the Securden Unified PAM technical specifications.

Common Use Cases

Use Case	Description
Ownership and accountability	Identify identities and secrets without accountable owners, and assign separate business and technical ownership for review and remediation.
Stale credential retirement	Identify credentials that are old, unrotated, or unused, and replace or retire them without breaking the workloads that depend on them.
Inherited cloud estate	Establish what exists and who owns it in an environment built by people who have since moved on, where nobody knows which service accounts and keys are still in use.
Certificate outage prevention	Maintain certificate inventory, track upcoming expirations, and automate supported issuance and renewal through ACME.
Audit evidence	Produce a record of credential access and administrative activity showing who did what, against which asset, from where, when, and why.

Frost Radar™ Leader, Privileged Access Management, 2026 | Top 150 Fastest-Growing Cybersecurity Companies

See how Securden can help your organization **Book a Demo**

Securden

+1 844 228 0327 +44 203 868 6147

support@securden.com www.securden.com

2810 N Church St, PMB 75693, Wilmington, Delaware 19802-4447, United States.