Securden

Unified PAM

Privileged Access Management for Modern Enterprise Environments

A unified platform to discover, protect, govern, monitor, and audit privileged identities, credentials, sessions, endpoints, third-party access, DevOps secrets, and machine or AI identities across hybrid infrastructure.

Credential Governance

Centralized vaulting, rotation, sharing controls, and audit trails.

Session Security

Secure RDP, SSH, and SQL just-in-time access with monitoring and recording.

Least Privilege

Endpoint privilege control, just-in-time elevation, and policy enforcement.

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

For enterprise security, IT operations, compliance, and infrastructure leadership teams.

Product Datasheet

Platform Goal	Deployment Model	Primary Security Outcome
Discover, protect, manage, control, and monitor privileged identities, credentials, sessions, endpoints, third-party access, DevOps secrets, and machine or AI identities.	SaaS, On-premises, and private cloud options.	Reduce standing privilege, eliminate hard-coded credentials, audit privileged access, and enforce least privilege across hybrid IT environments.

Product Overview

Securden Unified PAM is an end-to-end privileged access management platform for discovering, vaulting, governing, monitoring, and auditing privileged access across human users, workloads, applications, endpoints, cloud resources, DevOps pipelines, third-party users, service accounts, machine identities, and AI identities.

Core Technical Capabilities

Capability Area	Technical Functionality
Enterprise Password Management	Centralized credential vault; controlled sharing; automated rotation of administrator passwords, service account passwords, SSH keys, and shared administrative accounts. Supports credential import from a standard CSV, XLSX, KeePass, CyberArk, Keeper, and Delinea.
Privileged Account and Session Management	Discovery of privileged accounts across Windows, Linux, macOS, databases, SSH devices, network devices, virtual machines, services, scheduled tasks, and IIS application pools. Supports secure RDP, SSH, and SQL sessions with monitoring, recording, and playback.
Endpoint Privilege Management	Removal of local administrator rights, granular application control, temporary administrator rights, just-in-time elevation, and least-privilege enforcement.
Vendor Privileged Access Management	Zero trust third-party remote access without VPN, endpoint agents, or firewall port openings, with complete auditing and session recording.
Self-Service Password Reset	User-initiated password reset and account unlock for Active Directory and Microsoft Entra ID environments.
Machine, AI, and DevOps Secrets	Management of API keys, tokens, service accounts, application credentials, CI/CD secrets, SDK and CLI integrations, REST API access, and secrets used across DevOps pipelines.

Capability Area	Technical Functionality
Cloud Infrastructure Entitlement Management	AWS, Azure entitlement visibility, discovery of privileged policies, and reduction of excessive cloud permissions.

Architecture and Deployment

Deployment Models	SAAS, On-premises, private cloud
Server Operating System (for on-prem)	Windows Server 2019 or later.
Installation Package (for on-prem)	Single binary installer with bundled components and database.
Backend Database (for on-prem)	PostgreSQL bundled by default; Microsoft SQL Server supported as an optional backend.
Database Selection (for on-prem)	Database choice is selected during installation; migration between databases can be handled with Securden support.
System Sizing	Up to 1,000 accounts: 4 cores, 16 GB RAM, 50 GB disk. 1,000–10,000 accounts: 8 cores, 32 GB RAM, 100 GB disk. Above 10,000 accounts: contact Securden support.
Remote Gateway	Securden server acts as gateway by default; dedicated gateway recommended for distributed networks.
AgentLESS	Agentless for discovery, rotation, and session brokering.

Security Architecture: On-Premises vs SaaS

Security Area	On-Premises Edition	SaaS Edition
Vault Model	Dedicated central server connected to a backend database; server handles business logic and users connect through a standard web browser.	Access-controlled, highly available vault instance hosted on AWS cloud with browser-based user access.
Data Encryption	Sensitive vault data is encrypted at the application level using AES-256 before being stored in the database.	Customer data is encrypted using AES-256 and stored in segmented encrypted database storage.
Encryption Key Management	Each installation uses an automatically generated unique random installation key that must be kept separate from encrypted data and made available only during vault startup.	Each customer segment uses a unique encryption key stored through Amazon KMS with cryptographic operations handled in an AWS CloudHSM cluster.
Database Protection	Database accepts secure connections; localhost-only access by default and specific IP allow-listing for high-availability configurations.	Each customer's data is segregated and encrypted with a unique key so unauthorized access exposes only encrypted data.

Security Area	On-Premises Edition	SaaS Edition
Data Integrity	Encrypted data cannot be deciphered without the installation key even if the database is compromised.	Encrypted customer data cannot be deciphered without the corresponding organization-specific key.

Security Controls

Security Control	Details
Credential Encryption	AES-256 encryption.
Encryption Key Management	Per-installation encryption key stored separately from encrypted database; HSM support available.
FIPS Mode	FIPS-compliant mode available.
Certificate Handling	Self-signed certificate by default; CA-signed certificate installable.
Breached Credential Monitoring	Stored credentials checked against known breach data; requires internet connectivity.
Certifications and Testing	ISO/IEC 27001, SOC 2 Type II, GDPR alignment, and periodic third-party penetration testing.
Access Governance	Granular RBAC, credential access policies, request-release workflows, emergency access controls, and just-in-time access.
Passwordless Privileged Use	Access to privileged systems without revealing passwords to users.
Session Auditability	Audit trails for privileged credential use, remote sessions, and administrative activity.

Privileged Access Control Design

Control Layer	Technical Detail
Primary Authentication	Vault access can be controlled through LDAP-compliant directory services such as Active Directory and Microsoft Entra ID, SAML-based SSO, RADIUS authentication, smartcard authentication, or native local authentication.
Directory-Based Authentication	When directory authentication is used, the vault authenticates through the configured directory and does not need to store directory user passwords.
User Lifecycle	Directory integrations support user onboarding, offboarding, authentication, and access provisioning workflows.
Second Factor	Cloud and on-premises designs support MFA through any TOTP authenticator, Securden Authenticator, OTP through email, any RADIUS-based MFA, Duo, Yubikey, and others.
Access Policies	Granular role-based access controls, request-release workflows, just-in-time access, and passwordless privileged sessions reduce credential exposure.

Identity, MFA, and Integration Support

Integration Area	Supported Options
Primary Authentication	Local accounts, Active Directory, Microsoft Entra ID, LDAP, and RADIUS.
SSO	SAML 2.0 support for Okta, Microsoft Entra ID, ADFS, OneLogin, PingIdentity, Google Workspace, and other SAML identity providers.
MFA	TOTP apps such as Google Authenticator and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP, and RADIUS-based MFA.
Smart Card Authentication	Supported for on-premises deployments.
RBAC	Predefined and custom roles.
Supported Browsers	Chrome, Edge, Firefox, and Safari.
Client Applications	Browser, Desktop application (Windows, Mac, Linux), iOS and Android applications, and browser extensions for Chrome, Firefox, Edge, and Safari.
API Access	API-based credential retrieval and REST API access with token-based authentication.

Product Specifications Snapshot

Specification	Details
Supported Access Types	Privileged account passwords, shared administrator accounts, service accounts, SSH keys, machine identities, API keys, tokens, application credentials, CI/CD secrets, remote sessions, endpoint privileges, vendor access, and cloud entitlements.
Remote Session Protocols	RDP, SSH, and SQL sessions (both browser-launched and native tools) with access without password disclosure, session monitoring, recording, and playback.
Enterprise Integrations	Active Directory, Microsoft Entra ID, LDAP, Google Workspace, SAML SSO, SIEM, ticketing systems, MFA providers, SDKs, CLI access, and APIs.
Endpoint Controls	Removal of local administrator rights, application control, on-demand elevation for standard users, temporary administrator rights, and least-privilege enforcement.
MSP Support	Multi-tenant architecture for managed service providers, with data segregation and client-specific administration.
Audit and Reporting	Visibility into who has access to what, privileged activity tracking, password hygiene monitoring, access reports, and compliance support.

Discovery and Operations

Operational Area	Details
Account Discovery	Windows, Linux, macOS, databases, network devices, cloud applications, SSH-enabled devices, virtual machines, services, scheduled tasks, and IIS application pools.
Credential Import	Standard CSV, XLSX, KeePass, Keeper, CyberArk, Delinea.
Automated Rotation	Scheduled at folder level; dependent services updated in the same operation.
Remote Connection Types	RDP, SSH, and SQL through web-based and native client access.
Session Recording	RDP, SSH, and SQL recording; requires remote gateway; enabled globally and then per account or folder.
Emergency Access	Designated users, maximum duration, and mandatory waiting period configurable.

Scale and Resilience

Resilience Area	Details
High Availability	Secondary application server with automatic failover; read-only replica on a separate subnet. Encrypted HTML backup.
Database Clustering	SQL clusters supported with Microsoft SQL Server backend.

Resilience Area	Details
Disaster Recovery	Scheduled full database backup to remote destination; minimum hourly interval.
Offline Access	Encrypted HTML export of stored credentials protected by passphrase. Desktop applications.
Distributed Architecture	Application servers and remote gateways deployable per network.

Commercial Notes

Commercial Area	Details
Licensing Model	Per user accessing the Unified PAM interface.
Endpoint Privilege Management	Included; Endpoint agent licenses purchased separately.
Vendor PAM	Included; Vendor user licenses purchased separately.
SSPR	SSPR user licenses purchased separately.
Non-Production Environments	No separate license required for test, staging, or DR instances.
Support	24x5 standard support; 24x7 premium support.
Upgrade Cadence	Minor monthly releases; major quarterly releases.
Free Trial	30 days; no credit card required.

Common Use Cases

Use Case	Description
Credential Governance	Consolidating and rotating privileged credentials across Windows, Linux, macOS, databases, network devices, applications, and cloud infrastructure.
Privileged Remote Access	Providing secure privileged remote access while recording and auditing all sessions.
Endpoint Least Privilege	Removing local administrator rights and enabling just-in-time privilege elevation for standard users.
Third-Party Access	Granting secure, time-bound vendor access without VPN dependency.
DevOps Secrets	Reducing risks from hard-coded secrets in DevOps pipelines and application environments.
Machine and AI Identities	Securing machine identities, service accounts, API keys, tokens, AI agents, and MCP servers.