

Non-Human Identity Management

Modern Enterprises Have More Machine Identities Than Human Identities

100+ Billion

Estimated machine identities across enterprise environments

100 : 1

Machine identities to human identities

Yet only a small percentage of organizations have fully automated machine identity lifecycle management.

Where the Risk Begins

Hard-Coded Credentials



Passwords hidden in source code, scripts and configuration files.

Standing Credentials



Privileged accounts permanently configured on target systems.

Long-Lived Secrets



Credentials that remain valid long after they are needed

Excessive Privileges



Applications and services with more access than required.

Unmanaged Access



Limited visibility into which application accessed which resource.

Turn Static Credentials into Dynamic Access

Create. Use. Remove.

Kron PAM replaces persistent, privileged credentials with Dynamic Credential Creation.

When access is requested, Kron PAM creates a credential specifically for that access. The credential is provisioned to the target system, used during the authorized session and removed from the target device when access is completed.

No standing credentials

No persistent exposure

No unnecessary access

Just-in-Time Credentials

REQUEST

Access is requested and authorized

CREATE

Kron PAM dynamically creates a credential

USE

The credential is used for the authorized access

REMOVE

The credential is automatically removed from the target system

Take Secrets Out of Your Applications

Kron PAM Secrets Manager securely delivers application credentials without requiring applications to store them.

Vault

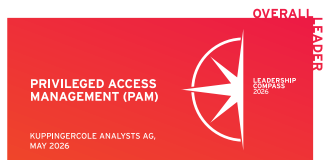
Authorize

Deliver

Rotate

Audit

Applications can retrieve secrets through APIs, SDKs, agents, plugins and JDBC Driver instead of embedding credentials in code or configuration files.



Kron has been recognized by KuppingerCole Analysts as a Leader in 3 Categories and a Challenger in 1 Category Also featured in Forrester, the OmdiaUniverse for PAM, the SPARK Matrix for PAM 2026, the Frost&Sullivan FrostRadar for PAM 2026 and the GigaOm Radar for PAM 2025. Named a Strong Performer in the Gartner Peer Insights™ Voice of the Customer for PAM.

ONE PAM. EVERY IDENTITY.

Kron PAM extends privileged access security from human users to applications, services and workloads — without creating another security silo.

CENTRALIZED CONTROL One Vault



Secure privileged credentials, application secrets, API keys and service credentials centrally.

LEAST PRIVILEGE Right Access. Right Time



Give machine identities only the access they need, when they need it.

AUTOMATED LIFECYCLE Create. Rotate. Remove.



Automate credential provisioning, rotation and removal

COMPLETE VISIBILITY Know Every Access.



Bring human and machine access into a centralized audit framework.

Kron PAM's Secrets Manager is natively integrated into the PAM platform, allowing human and machine identities to share policies, access controls and audit trails.

Secure Every Application. Every Workload.

Secrets Management Agent



Local caching for performance and resilience.

Kubernetes Agent



Authorize secret access from pods.

API & SDK



Secure programmatic secret access.

Enterprise Integrations



Jenkins, Tomcat, UiPath, Tenable Nessus, Ansible and more.

Why Kron PAM?

NHI Security Without Another Security Silo

Native PAM Architecture
One platform for human and machine identities.

Deep Application Integration
APIs, SDKs, agents, plugins, JDBC.

Zero Hard-Coded Secrets
Passwords out of source code.

Resilience by Design
Secret delivery with local caching.

Dynamic Credentials
Credentials exist only when needed.

Kubernetes Ready
Secure dynamic workloads and pods.

Automated Rotation
Reduces long-lived credential exposure.

Unified Audit
One audit framework, every identity.

The Next Generation of Privileged Access

Traditional PAM protects who can access privileged resources. Kron PAM goes further — securing what can access them. Users. Applications. Services. APIs. Workloads. Automation. Secure Every Identity. Human or Machine. Kron PAM goes further — securing what can access them. Users. Applications. Services. APIs. Workloads. Automation. Secure Every Identity. Human or Machine.