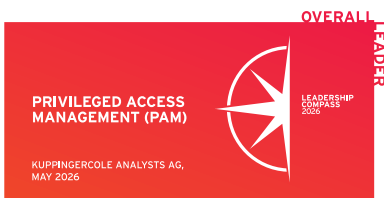


Privileged Access Management

Fastest to Deploy PAM platform converged with Adaptive MFA, Network AAA, and Data Security Capabilities

Your solid PAM foundation for zero trust security architecture against insider and external threats.

Kron is a technology company that provides advanced cybersecurity software solutions in the field of Privileged Access Management. Kron protects enterprises from data breaches and their associated costs. Additionally, it ensures compliance with data security regulations by strictly controlling access to critical IT assets.



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**.

Protect What You Connect™ with Kron PAM

Least Privilege

Only grant users the minimum necessary access to perform their job functions. Any additional access should be temporary and time-bound.

Zero Trust

Always verify before granting access, irrespective of the network source. Don't trust any request by default.

OT Security

Enhance security by limiting access to only the necessary resources with Kron PAM's granular approach, reducing the attack surface, and fortifying your OT environment against unauthorized access.

AI-Based Threat Protection

Detect all user anomalies through AI-based threat analytics. By automating threat detection and response, free up valuable time and resources that can be redirected toward core business activities.

Just-in-Time (JIT) Access

Instead of granting permanent privileged access, use a JIT approach where users request access when needed and it's granted for a limited duration.

Manager Approval

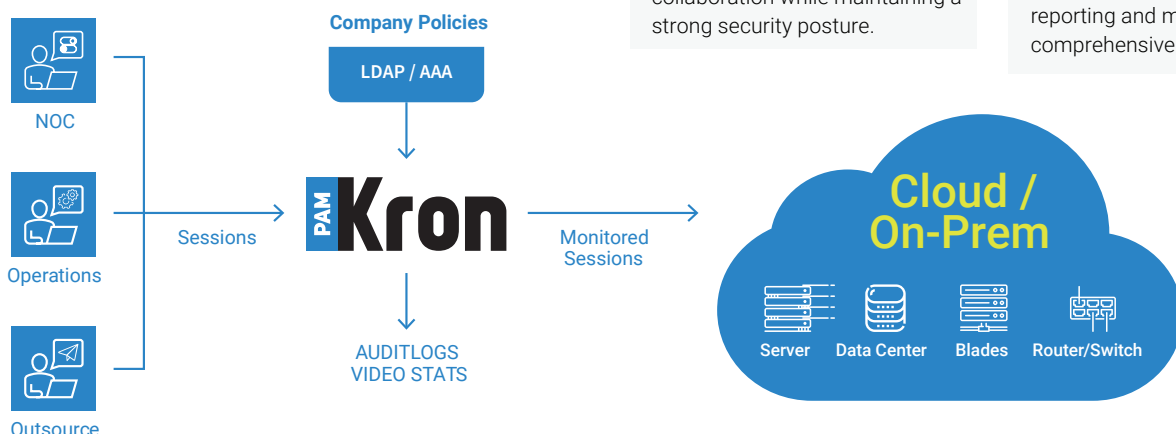
Implement workflows where privileged access requests are approved by a supervisor before they are granted.

Secure Remote Access

Extend the reach of your organization with ease, as Kron PAM's Secure Remote Access solution simplifies third-party access. Trust in seamless collaboration while maintaining a strong security posture.

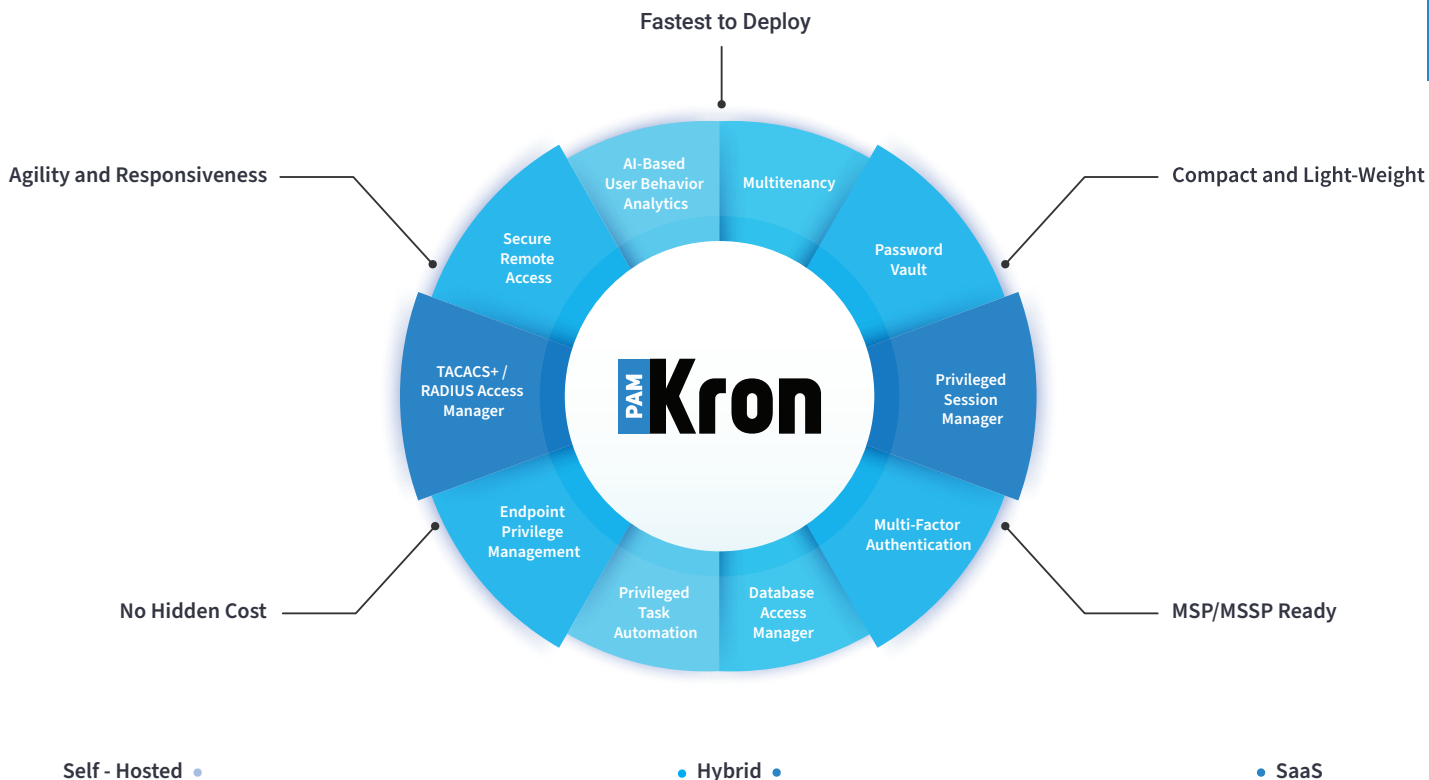
Audit and Regulatory Compliance

Simplify compliance with various regulations and standards, including GDPR, HIPAA, SOX, and SOC 2, by employing automated reporting and maintaining a comprehensive audit trail.



UNLOCK THE POWER OF SECURITY

ELEVATE YOUR DEFENSE WITH KRON PAM



Unified Access Management and Data Security

In today's digital landscape, where cyber threats are ever-evolving and the need for remote access is increasing, a unified approach to access management and data security is essential for businesses of all sizes.

Kron PAM supports a wide range of features in one box and helps enterprises to establish a flexible, centrally managed and layered defence security architecture against insider threats.

Password Vault

Manages and keeps all passwords in an encrypted secure vault and ensures privileged passwords are used only for legitimate business purposes.



Database Access Manager

Isolates database sessions, tracks and controls all user activities and prevents exposure of sensitive data with on the fly data masking.



AI Based User Behavior Analytics

Detects and responds to insider threats proactively. Stays one step ahead with automated risk-based actions to mitigate potential threats efficiently, ensuring the safety of organizations.



Session Manager

Eliminates the inadequacy of central access control point for critical systems and makes you gain full control over privileged sessions along with indisputable track records of user activities.



Privileged Task Automation

Simplifies and automates routine tasks that require privileged credentials and eliminates exposure of system credentials.



Privileged Elevation and Delegation Management

Provides more granular access control and authorization on endpoints. Promotes accountability by maintaining detailed logs of elevated privileges and delegation activities, enabling organizations to track and audit user actions.



Adaptive MFA

Enables an AI-based user behavior factor in authentication on top of login credentials before accessing target systems and privileged credentials.



Unified Access Manager

Extends Active Directory policies to network infrastructure and controls direct access to network elements through built-in TACACS and RADIUS support.

