SECUREKI

# Privileged Access Management (PAM)

www.secureki.com

# Privileged Access Management (PAM)

## Overview

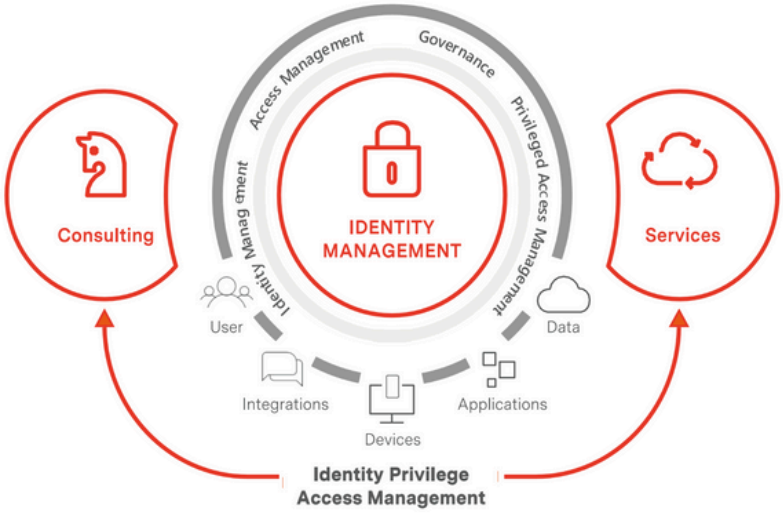
With IT infrastructures now spanning hybrid, multi-cloud, and on-premises environments, privileged accounts have become a prime target for attackers. SecureKi Privileged Access Management (PAM) delivers robust, automated control over privileged identities, helping organizations ensure compliance, reduce risk, and strengthen their security posture.

## Key Challenges Addressed

Modern organizations face growing security and compliance pressures as privileged accounts proliferate across complex infrastructures. SecureKi PAM is designed to counter these critical challenges that can undermine enterprise security and regulatory compliance:

- Expanded Attack Surface: The growth of hybrid, cloud, and on-premises systems has multiplied privileged credentials, making them prime targets for cyberattacks.

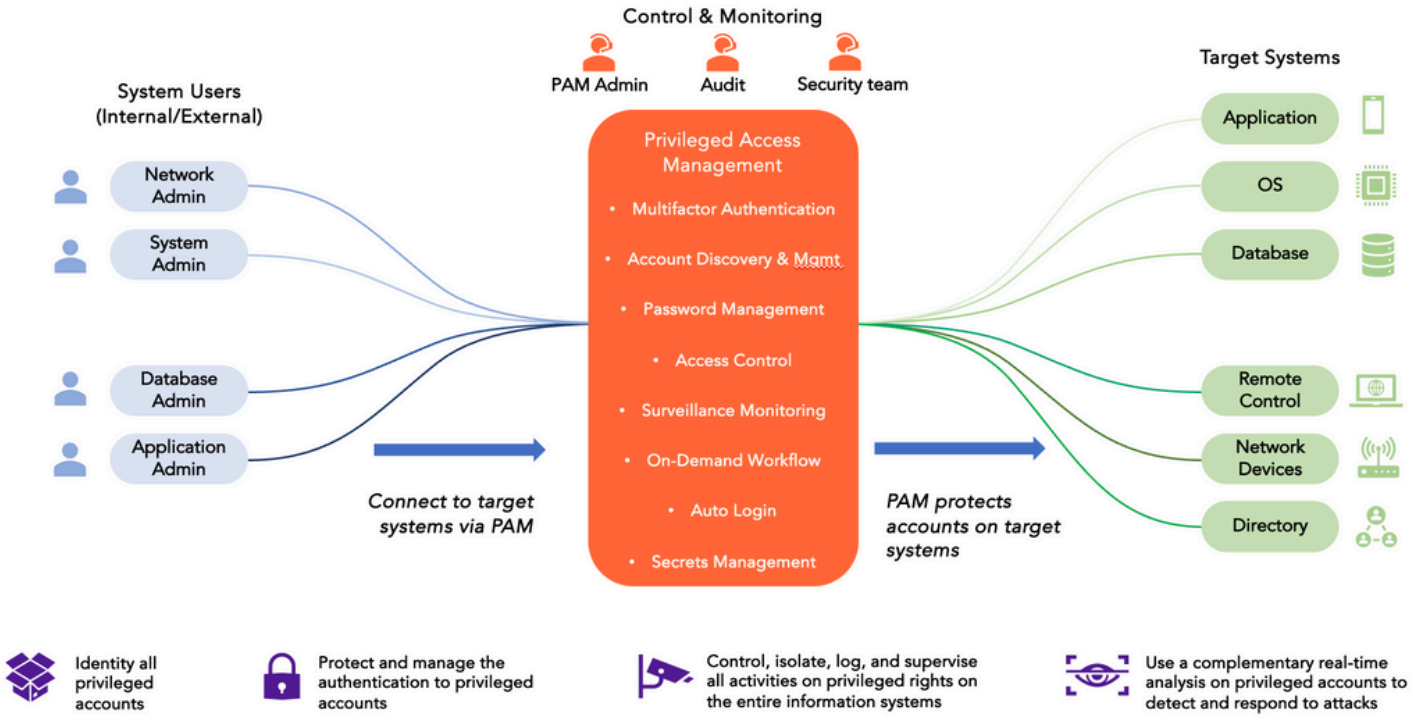
- Stringent Compliance Requirements – Organizations must continuously meet various international and industry-specific regulations, requiring consistent enforcement and auditing of privileged access.
- Insider Threats and Credential Misuse – Whether intentional or accidental, misuse of privileged accounts can result in significant data loss, reputational harm, and regulatory violations.




*SecureKi's PAM solution enables you to build, operate, and manage enterprise-wide Identity Management and Access Management solutions.*

## SecureKi PAM: Your Comprehensive Security Shield

SecureKi PAM is a next-generation solution built for both physical and virtual environments. It integrates centralized policy enforcement, visual session monitoring, automated password management, and advanced analytics to give organizations complete control over privileged access.




*Essential components of Privileged Access Management*

# Core Capabilities

## Centralized Credential Management

SecureKi PAM consolidates the management of privileged credentials into a unified, secure platform, enhancing operational control, reducing risk, and enabling scalable deployment across diverse environments.

- Flexible Architecture – Supports both agent-based and agentless deployments to suit various infrastructure needs.

- Comprehensive Protocol Support – Covers Telnet, SSH (password/key-based), and RDP connections to ensure seamless integration across platforms.

- Versatile Deployment Options – Delivered as a hardened hardware appliance, OVF-based virtual appliance, or secure SaaS offering to support both on-premises and cloud-first strategies.

- Secure Vaulting – Privileged credentials are protected using one-way encryption (digest hash) in a centralized vault for maximum security.

- Hard-Coded Credential Elimination – API integration and push/pull functions remove credentials from source code and automate secure updates.

- Self-Monitoring Capabilities – Includes server self-health checks to ensure high availability and operational resilience.

## Access Governance and Workflow

SecureKi PAM enforces consistent, policy-driven access governance through automated workflows, role-based controls, and real-time auditing to ensure privileged access is tightly monitored, accountable, and compliant.

- Fine-Grained Access Control – Define and enforce granular access rules at the command or session level with real-time controls such as OTP verification, user confirmation, admin alerts, or full session blocking.

- Centralized Workflow Automation – Streamline privileged account provisioning with configurable request and approval workflows to reduce latency and improve governance consistency.

- Role-Based Delegation – Enable secure delegation of administrative roles based on job function, escalation hierarchy, or operational responsibilities.

- Comprehensive Audit Trail – Maintain an immutable, time-stamped log of all privileged access activities, including requests, approvals, denials, and session interactions, to support audit readiness and forensic analysis.

- Mobile Gateway Approval – SecureKi's mobile app enables real-time approval of workflow requests anytime, anywhere.

- Secure Vaulting – Privileged credentials are protected using one-way encryption (digest hash) in a centralized vault for maximum security.

- Hard-Coded Credential Elimination – API integration and push/pull functions remove credentials from source code and automate secure updates.

- Self-Monitoring Capabilities – Includes server self-health checks to ensure high availability and operational resilience.

## Built-in Security & Compliance

SecureKi PAM is architected with security-first principles and certified compliance readiness to protect sensitive systems while simplifying audit and regulatory requirements.

- Common Criteria Certified (EAL2) – Validated against international standards (ISO/IEC 15408) to ensure rigorous and repeatable security evaluation.

- Enterprise-Grade Encryption & Access Controls – Enforces secure communication via HTTPS, applies AES-256/ARIA encryption to stored data, and restricts console access to authorized personnel only.

- Integrated Audit Logging & Integrity Validation – Continuously monitors and logs all system and user activities with built-in self-integrity checks to detect tampering or abnormal behavior.

- Comprehensive Audit Reporting – Includes pre-built and customizable reports tailored for both internal governance and external audits.

## Availability & Reliability

SecureKi PAM is engineered for operational resilience, ensuring business continuity and secure access even under adverse conditions or system failures.

- High Availability Architecture – Built-in HA configuration with real-time synchronization between primary and secondary systems to ensure uninterrupted access to privileged accounts.
- Resilient Backup Support – External USB backup functionality provides an additional layer of data protection in case of system failure.
- Automated System Health Monitoring – Continuous self-health checks and credential verification routines detect system anomalies and maintain operational integrity.

## Password Lifecycle Automation

SecureKi PAM automates the full lifecycle of privileged credentials, reducing manual effort and eliminating password-related vulnerabilities through policy-driven enforcement.

- Post-Session Rotation – Automatically changes passwords immediately after each use to eliminate lingering access risks.
- Scheduled Password Rotation – Enforces regular password changes using randomized patterns and defined time intervals to meet compliance requirements.
- Administrative Force Change – Allows manual batch password changes for critical systems or emergency scenarios.
- Policy-Based Enforcement – Prevents password reuse, enforces complexity standards, and ensures adherence to security policies.

## Secure Single Sign-On (SSO) with Multi-Factor Authentication (MFA)

SecureKi PAM simplifies and secures privileged access by enabling seamless, passwordless login to target systems, reinforced with strong multi-factor authentication mechanisms.

- Frictionless Access – Enables secure and instant login to target systems using mobile OTP or biometric methods such as palm vein or fingerprint scanners.
- Passwordless Authentication – Credentials remain concealed during the authentication process, minimizing exposure risks.
- Broad Device Compatibility – Supports Apple Face ID, FIDO-compliant fingerprint sensors, and offline OTP modes to fit diverse user environments.

## Least Privilege & Just-in-Time Access Control

SecureKi PAM strengthens privileged access security by combining least privilege enforcement with just-in-time (JIT) access, ensuring users have the minimum rights necessary only when needed.

- Granular Command Filtering – Enforce least privilege with detailed command-level control using blacklist or whitelist groupings, tailored per role or access level.
- Context-Aware Enforcement – Apply dynamic actions such as block, OTP verification, user confirmation, or admin notification to specific commands based on policy or context.
- Regex-Based Control Logic – Utilize regular expressions for precise control over command patterns across diverse systems.
- Just-in-Time Privilege Elevation – Grant time-bound elevated access only upon approved request, automatically revoking privileges after use.

- Zero Standing Privileges – Remove persistent administrative rights by providing temporary access on demand to reduce risks.

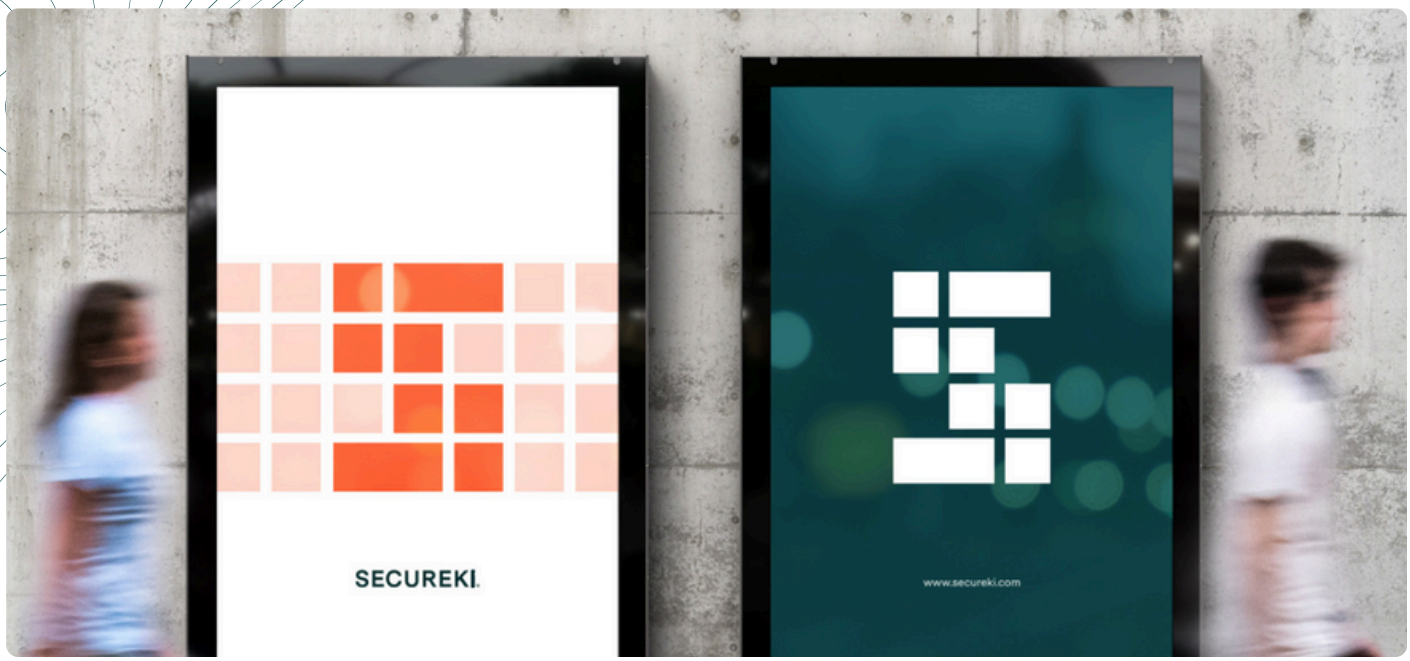
- Audit-Ready Expiry Logs – Log every JIT access request, duration, and activity to support compliance and forensic analysis.

## Visual Session Recording and Audit

SecureKi PAM ensures full visibility and accountability of privileged user activity through continuous monitoring, recording, and playback.

- Comprehensive Session Coverage – Captures and monitors interactive sessions across SSH, Telnet, RDP, web-based consoles, and client-server applications.

- Replay for Forensics & Compliance – Enables full session playback for forensic investigation, behavioral analysis, and regulatory validation.



# Add-On Advanced Modules for PAM

Extend the power of SecureKi PAM with modular enhancements designed to address evolving enterprise needs—from identity governance to DevOps secrets management. Each module integrates seamlessly with the PAM core to deliver greater control, visibility, and automation across your infrastructure.

## Identity Module (Add-On for PAM)

SecureKi PAM simplifies and secures privileged access by enabling seamless, passwordless login to target systems, reinforced with strong multi-factor authentication mechanisms.

- Infrastructure-Centric Identity Lifecycle – Automates provisioning and de-provisioning of privileged accounts for Windows, Linux, databases, and network devices.
- Access Certification & Attestation – Supports periodic reviews and approvals of privileged access rights to improve accountability and compliance.
- Policy-Based Role Assignment – Defines dynamic access policies based on roles, job functions, and system types, enforcing least privilege consistently.
- Unified Access Visibility – Centralizes monitoring of user identities and their privileged access across servers, databases, and network layers.
- Seamless Integration – Works with IT service desks, enterprise IAM systems, IGA tools, and HR platforms to synchronize identities, streamline ticket-based access, and maintain governance.

## Secret Management Module (Add-On for PAM)

The Secret Management Module enables centralized storage, delivery, and lifecycle management of application secrets for both modern cloud-native and legacy systems, reducing exposure and eliminating hard-coded credentials.

- Universal Secrets Vault – Stores and manages secrets such as API keys, certificates, passwords, and tokens for modern and legacy systems.
- Dynamic Secret Injection – Injects secrets securely into applications and scripts at runtime without embedding them in code or configuration files.
- Automated Secret Rotation & Expiry – Updates and revokes secrets automatically based on defined lifecycle policies to meet compliance requirements.
- Audit Logging & Traceability – Records all secret access and usage activities for complete audit readiness and forensic analysis.
- DevOps & Legacy Integration – Integrates with CI/CD pipelines and DevOps tools such as Jenkins, Terraform, and Kubernetes, as well as legacy systems, to ensure secure and seamless secret delivery across modern and traditional environments.
- Role-Based Secret Access Control – Ensures only authorized users or services can access specific secrets based on policy.
- High Availability & Resilience – Maintains continuous availability and fault tolerance for secrets in distributed or hybrid environments.

# Business Value Delivered

SecureKi PAM empowers organizations to take control of privileged access with a unified, automated platform by delivering measurable improvements in security posture, operational efficiency, and regulatory compliance. By minimizing risk, accelerating access workflows, and enhancing visibility, SecureKi enables secure and confident IT governance.

## Mitigate Security Risks

SecureKi PAM reduces the risk of breaches and unauthorized activity by enforcing strict access boundaries and role-based controls.

- Restrict Lateral Movement – Limits attackers' ability to move within the network by controlling privileged access scope.
- Granular Access Enforcement – Applies detailed role-based and command-level restrictions to prevent misuse.

## Improve Operational Efficiency

SecureKi PAM streamlines access workflows and reduces administrative burdens while maintaining strong security controls.

- Accelerated Provisioning – Automates access requests, approvals, and provisioning to reduce delays.
- Seamless Administrator Access – Provides fast, secure access to critical systems without compromising control.

## Enhance Accountability and Visibility

SecureKi PAM improves transparency and traceability across privileged activities, even for shared or third-party accounts.

- Comprehensive Session Monitoring – Captures every action for review and compliance purposes.
- Real-Time Alerts – Flags unusual or risky activities before they escalate.

## Support Regulatory Compliance

SecureKi PAM simplifies alignment with global and industry-specific security standards.

- Multi-Standard Compliance – Supports regulations such as RMIT, ISO/IEC 27001, GDPR, HIPAA, and PCI-DSS.
- Audit-Ready Reporting – Offers comprehensive reports, policy traceability, and session playback for faster audits.

# Why SecureKi PAM?

SecureKi PAM redefines privileged identity security with an agile, scalable, and certified platform trusted across industries. Whether deployed on-premises or in virtual environments, SecureKi helps organizations protect critical systems, reduce insider threats, and maintain compliance without sacrificing operational agility.

# Final Take

Privileged accounts are the keys to your most critical systems. Without strong controls, they open the door to costly breaches, insider misuse, and compliance failures. SecureKi PAM provides a unified, automated, and scalable solution to safeguard those accounts, enforce least privilege, and deliver full visibility into privileged activity.

Whether you are modernizing IT operations, meeting regulatory demands, or strengthening your overall security posture, SecureKi PAM equips your organization with the control and confidence needed to protect what matters most.

**Your privileged accounts deserve stronger protection. Let's talk about securing them today.**

**SecureKi Sdn Bhd (1143453-U)**

C-13-09, Sunway Nexis, No 1, Jalan
PJU 5/1, Kota Damansara, 47810
Petaling Jaya, Selangor.

**Contact: info@secureki.com**
**www.secureki.com**

## Common Criteria Certified (EAL2)

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that is commensurate with the target environment for use.