SECUREKI®

Privileged Access Management (PAM)

www.secureki.com

Privileged Access Management (PAM)

What is PAM?

SecureKi Privileged Access Management (PAM) is the next generation automated privileged password management solution with visual recording, fine-grained access control, multifactor authentication, and Infrastructure Single-Sign-On capabilities.

Challenges

As the integration of core infrastructure and business system expand in the age of digital connectedness, safeguarding privileged access is imperative to successfully avert data breach and is a core requirement of multiple compliance regimes.

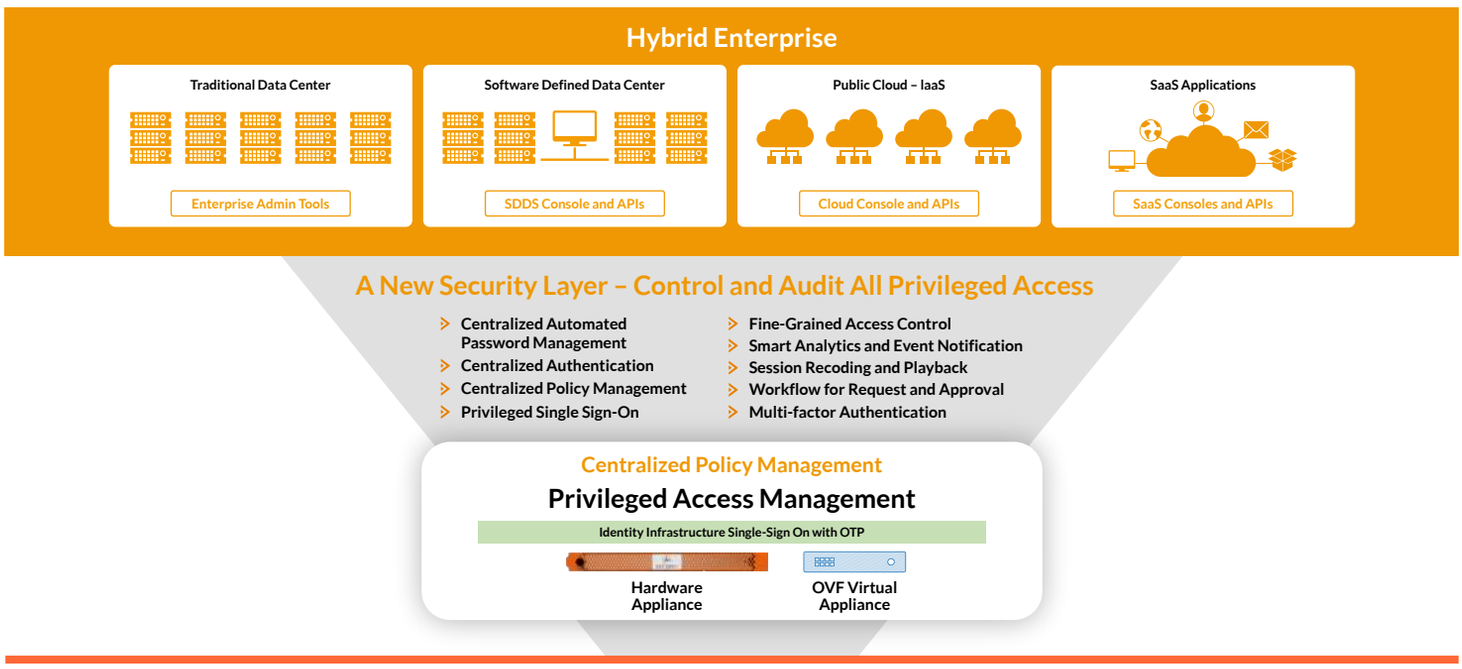
SecureKi Privileged Access Management helps drive IT security and compliance risk reduction and improves operational efficiency by enabling privileged access defense in depth—providing broad and consistent protection of sensitive administrative credentials, management of privileged identity access and control of administrator activities.

PAM Solution

SecureKi Privileged Access Management (PAM) is a simple-to-deploy, automated, proven solution for privileged access management in physical and virtual environments. Available as a rack-mounted, hardened hardware appliance or an Open Virtualization Format (OVF) Virtual Appliance. SecureKi PAM enhances security by protecting sensitive administrative credentials such as root and administrator passwords, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity across all IT resources with multifactor authentication.

G-03-1, Plaza Kelana Jaya, Jalan SS7/13A, 47301 Petaling Jaya, Selangor Malaysia

info@secureki.com +603 7652 1099 +603 7652 1189



Key Features & Benefits

Ease of Management

- Operated by agent and agentless system
- Supported protocols inclusive Telnet, SSH Password, SSH Key Login, RDP
- Provided as an appliance or virtual appliance
  - Easy to install and manage
  - Server Self-Health Check
- Remove hard-coded passwords in source code
  - Push / Pull feature available

Reliable Operation

- External USB Backup
- Redundancy of the appliance for High Availability with data in real time sync
- Password verification function provided

Compliance

- Prevent the reuse of passwords
- Mass password change feature
- Integrated Mobile OTP for ACM Web Access Authentication

Workflow

- Account Request Application / Approval Function
- Request and approval for One-time Password
- Report of the request / Approval / User History
- Delegate administrative rights

Integrated Password Management

- Support a variety of operating systems and platforms (Unix / Windows / Database / Network Devices / Applications / Security Equipment)
- Regular password changes and audit management
- Built-in authorization procedures for the account password access permissions (password issued by approval workflow)

Password Policy

- Change Request: Password automatically changes after use
- Periodic Changes: Change password based on random rules and schedule
- Force Change: The administrator can perform manual batch change

Password Security

- Password protection for shared accounts and third parties access
- Prevent reuse of the password and maximize the password complexity
- Support one-way encryption that only stores the message digest hash value of each password in the password vault

Hard-coded Password Management

- Prevent hard-coded passwords in scripts via the provided API
- Automatic request and update passwords within a script

G-03-1, Plaza Kelana Jaya, Jalan SS7/13A, 47301 Petaling Jaya, Selangor Malaysia
info@secureki.com
+603 7652 1099
+603 7652 1189

Compliance Response

- Account /password usage history report
- Built-in reporting system for internal/external audit

Stability and High-Availability

- Password verification function (perform password change and operation verification)
- Support appliance redundancy (built-in HA configuration supports real-time synchronization)
- External USB backup function (ensuring continuity of service due to logical/physical failure)

Session Recording and Playback

- Real-time session monitoring, recording, and playback capabilities for audit trails
- Audit on web-based application, client-server applications, SSH, Telnet & RDP

Built-in Security

- **Physical Security**: Disk encryption, disk Bay lock, the console login restrictions, Multi-Factor Authentication
- **Logical Security**: HTTPS communication, AES / 256, ARIA encryption application, self-integrity check on service process and adapters, audit logging

Multi-Factor Authentication (MFA)

- Built-in with native Mobile Software MFA for IOS and Android
- Support mobile fingerprint-sensor for FIDO authentication
- Support offline login authentication with OTP
- Support Biometric authentication with Palm or Finger Vein scanner
- Support third party authentication integration
- Support Apple devices using Face ID authentication

Secure Single-Sign On with MFA

- Support palm-vein scanner or Mobile OTP authentication auto-login to the target systems
- Auto-login without exposing credentials

Fine-Grained Access Control

- Granular command filtering with blacklist or whitelist grouping
- Support fine-grained command control action with Block, OTP, Confirm & Notify option
- Support regular expression in command control

Business Value Proposition

SecureKi Privileged Access Management (PAM) provides a host of capabilities and controls that actively prevent attackers from carrying out critical components of their attacks, as well as delivering additional support for reducing risks and improving operational efficiency. More specifically, SecureKi Privileged Access Management provides the following benefits:

Mitigate Data Security Reduce risk.

Prevent unauthorized access and limit access to resources once entry is granted to the network. Protect passwords and other credentials from unauthorized use and compromise. Limit the actions users can perform on systems and prevent the execution of unauthorized commands and prevent lateral movement within the network.

Increase accountability.

Observe full attribution of user activity, even when using shared accounts. Comprehensive logging, session recording and user warnings capture activity and provide a deterrent to unauthorized behavior.

Improve auditing and facilitate compliance.

Simplify compliance by providing support for emerging authentication and access control requirements and limit the scope of compliance requirements through logical segmentation of the network.

Reduce operations complexity with automation.

Privileged single sign-on with MFA limits the risk of password-gathering malware attacks and optimizes the productivity of administrators with quick and secured access to their remote systems. Centralized policy definition and enforcement simplify the creation and enforcement of security controls.

COMMON CRITERIA

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.

G-03-1, Plaza Kelana Jaya, Jalan SS7/13A, 47301 Petaling Jaya, Selangor Malaysia
info@secureki.com +603 7652 1099 +603 7652 1189