Kron TECHNOLOGIES

DATASHEET

Privileged Session Manager

Gain Full Control Over Your Sessions

In any given IT and **Network Infrastructure,** there are **thousands of servers / devices and thousands of users** (employees, contractors, etc.) who connect to them on a daily basis.

There are tens of thousands of connections established between users and servers / devices every day, which is very complex and probably unmanageable from a security point of view. Not every connection (between user and device / servers) is at the same level of importance.

For instance, there are users (employees) which you trust to connect to servers / devices that do not manage critical enterprise assets. For such connection types it may be enough to just log which user connected to which device / server.

However, some connections are extremely sensitive, like 3rd party technical support workers who access the most critical network / IT resources. In such cases, you want to ensure that you have “full visibility” and “full control” during such connections.

Problems and challenges without a central session management solution

- Complexity of access management for hundreds of users connecting to thousands of systems
- Granting users more privileges than they need
- No or minimal accountability for privileged accounts
- Lateral movement and spread of malware to critical systems
- Lack of data and reports for regulatory compliance and audits
- Unsecure 3rd party remote access

The Kron PAM Privileged Session Manager is the solution…

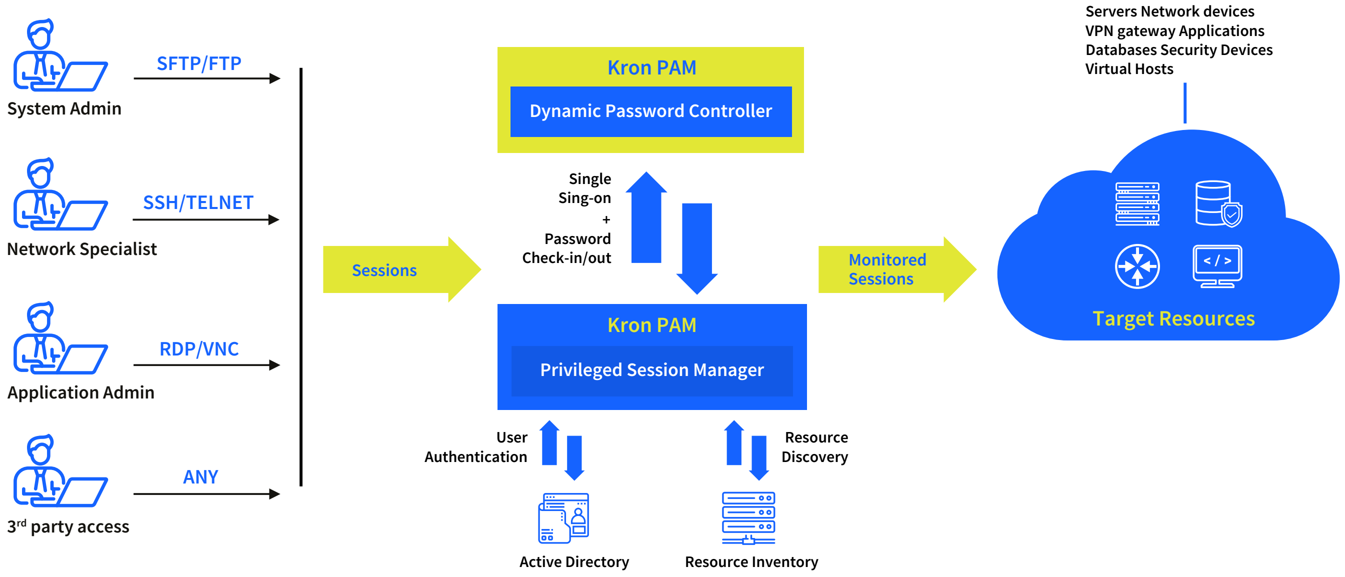
The Kron PAM Privileged Session Manager transparently sits in the middle of sessions and does not require an agent to be installed on Users’ PCs or target servers/ applications. The Session Manager supports Command Line Interfaces (SSH, Telnet), Remote Desktop Connections (RDP/VNC), Web sessions (HTTP/S), File transfer (SFTP), and Database connections (SQL).

Users may choose one the options while connecting to the target hosts:

- Native clients on their PCs (for CLI, SQL and File Transfer Sessions)
- Kron PAM WEB Portal (CLI and RDP/VNC sessions)
- Kron PAM Desktop Client (CLI and RDP/VNC sessions)

How The Session Manager Works?

The Privileged Session Manager (PSM) controls, monitors and audits encrypted administrator sessions, and runs as a gateway between users and the target end points. The Privileged Session Manager's man-in-the-middle approach requires no software agents to be deployed on target end points, and no specific access portal or client application. It is fast to implement and has no impact on end-user experience. Users are authenticated from the enterprise's existing directory service, and the entire session goes through the Privileged Session Manager so that indexed logs, audit trails, videos and statistics are logged indisputably. Any custom policy can be easily created and assigned to user groups on the Privileged Session Manager to implement least privilege practices within the enterprise. The Kron PAM Privileged Session Manager supports a wide range of interfaces, including SSH/TELNET for command line interface sessions, RDP/VNC for remote desktop connections and SFTP for file transfer.



Step 1

The user initiates a session towards the Session Manager with his/her own username and password.

Step 2

A session between the User and the Session Manager is established. The Session Manager displays the list of devices that the user has permission to access.

Step 3

The User selects the Target Device he/she wants to connect to from the list.

Step 4

The Session Manager initiates a session towards the Target Device with a username / password.

Step 5

A session is established between the Session Manager and the Target Device.

Step 6

Two separate sessions (User<->Session Manager and Session Manager<->Target Device) are connected back-to-back by the Session Manager. The Kron PAM Session Manager is the man-in-the-middle for the entire duration of the session and has "full control" and "full visibility" of the session. In case of a CLI session, when the User enters a command to forward the command to the Target Device or reject it.

Product Family

Password Vault

Takes control of deivce and database passwords, providing security while sustaining efficiency.

Privileged Session Manager

Logging and recording of all sessions for network and servers, including command and context-aware filtering.

Adaptive MFA

Additional layers of authentication integrating mobile device, geo-location and time.

Database Access Manager

Single point of access control management for database layer, secures data access with logging, policy enforcement, and masking.

Privileged Task Automation

Provides a single interface to configure the capabilities of network business flows with dynamic and extendable command sets.

Unified Access Manager

Provides AAA services for network infrastructure and extends AD authentication and policy configurations to the network.

AI Based User Behavior Analytics

Employs advanced alghoritms to identify anomalies and potential security thretas within privileged access environment.

Privileged Elevation and Delegation Management

Granular control over privilege users using fine-grained access policies and comprehensive auditing.

Password Vault

The Kron PAM Password Vault is a central secure password vault and helps to prevent stealing or unauthorized sharing of passwords.Users check-out the credentials of a privileged account from the Kron PAM Password Vault and use them to connect to a target endpoint in order to fulfil their tasks. Indexed logging and audit trails are generated to meet security and compliance requirements. The Password Vault supports integration with the enterprise's existing directory service so that users continue to use their existing personal accounts to log in to Kron PAM's Password Vault and check-out the credentials of the target privileged accounts they are authorized to use.

The Password Vault secures user credentials of operating systems (Windows, Linux, Unix), databases (Oracle, MySQL, MsSQL, PostgreSQL, etc.), virtually any network device or appliance that has an SSH/TELNET interface, and any application that provides user credential management API's.

With its agentless architecture, this solution supports Application-to-Application Password Management (AAPM) to eliminate static passwords in configuration files and application source codes. The Password Vault enables secure storing, tracking, and sharing of confidential data/file or unmanaged credentials among employees.

Feature & Benefits

Full visibility. Detailed audit logs. All **commands,** either failed or successful, are logged. Indisputable logging of which user attempted to run which command on which device and when.

Fully complies with regulations, provides logs and reports required for **audits** and compliance.

"Separation of duties" and "least privilege" practices are achieved, regardless of the **role / profile** capabilities of the Target Device. Any custom policies (allowed command sets, blocked command sets) can be defined and applied to any user group, ensuring thatonly the "required set of commands" can be executed by a user in order to fulfill his tasks, restricting standard user accounts from having over-privileged access.

Eliminates weak passwords and/or **non-expiry** passwords.

Enables the definition of time-based access limitations, based on time of day, day of the week, maintenance window hours, etc.

Disables inactive **privileged** accounts and sessions.

Session recording and video playback for forensic **analysis.**

Object Character Recognition for RDP session **recording** - OCR

Helps to **eliminate password** sharing and shared accounts usage. Users always log in with their own username/password, even if a shared account is used to connect to the device. For example, I connect to Kron PAM with username=Frank and then select a device to connect. The Kron PAM Session Manager establishes a session towards the target device, but may be using username=admin. As a user, I never see/know the real username/ password used to connect to the target device - all I know is my own username/password.

Makes sure it is the **real user** connecting to the target device, indisputably.

Context-aware policy. For example, do not allow "delete" command to run at the **device level** (higher/outer level of the command tree), but allow it to run at the port level (lower/inner level of the command tree).

Multi-factor authorization. It is possible to define that certain commands (e.g. shutdown command) require an approval from a second person to run, i.e., when a user enters a "shutdown" command, his supervisor receives an email, and if he/she clicks the "approve" link then the command is executed, otherwise it is rejected.

Dual control (referred to as "four eyes" or "second eye"). When a user is connected to a device, a supervisor can monitor the session in real-time and can also **take/release** the control of the session. This is particularly useful when real time monitoring is required for emergency accounts or to monitor someone who is in training.

Single sign-on. The user connects to the **Kron PAM** Session Manager with his/her username/ password and selects any allowed device to connect. The user does not need to use/know separate username/passwords to connect to different devices/servers.

Auto lock user account when an employee **terminates** employment (integration with enterprise Active Directory or LDAP is required).

Auto enable new user accounts with correct privileges when new employees start work (integration with enterprise Active Directory or LDAP is required).

Auto-login. The Kron PAM Session Manager enables the user to connect to enterprise applications without **knowing the application** username/ password.