Privileged Access Management (PAM) as a Service

THE GROWING NEED FOR EFFECTIVE PAM SOLUTIONS

$4.45

million average total cost of a data breach

19%

stolen or compromised credentials are the most expensive cause for data breaches

277 Days

average time to identify and contain

59%

data breaches due to not having zero trust mechanisms

WHY PAM IS ESSENTIAL IN TODAY'S IT LANDSCAPE

Managing access management in an organization becomes a challenge

Limited or no visibility into users' activities

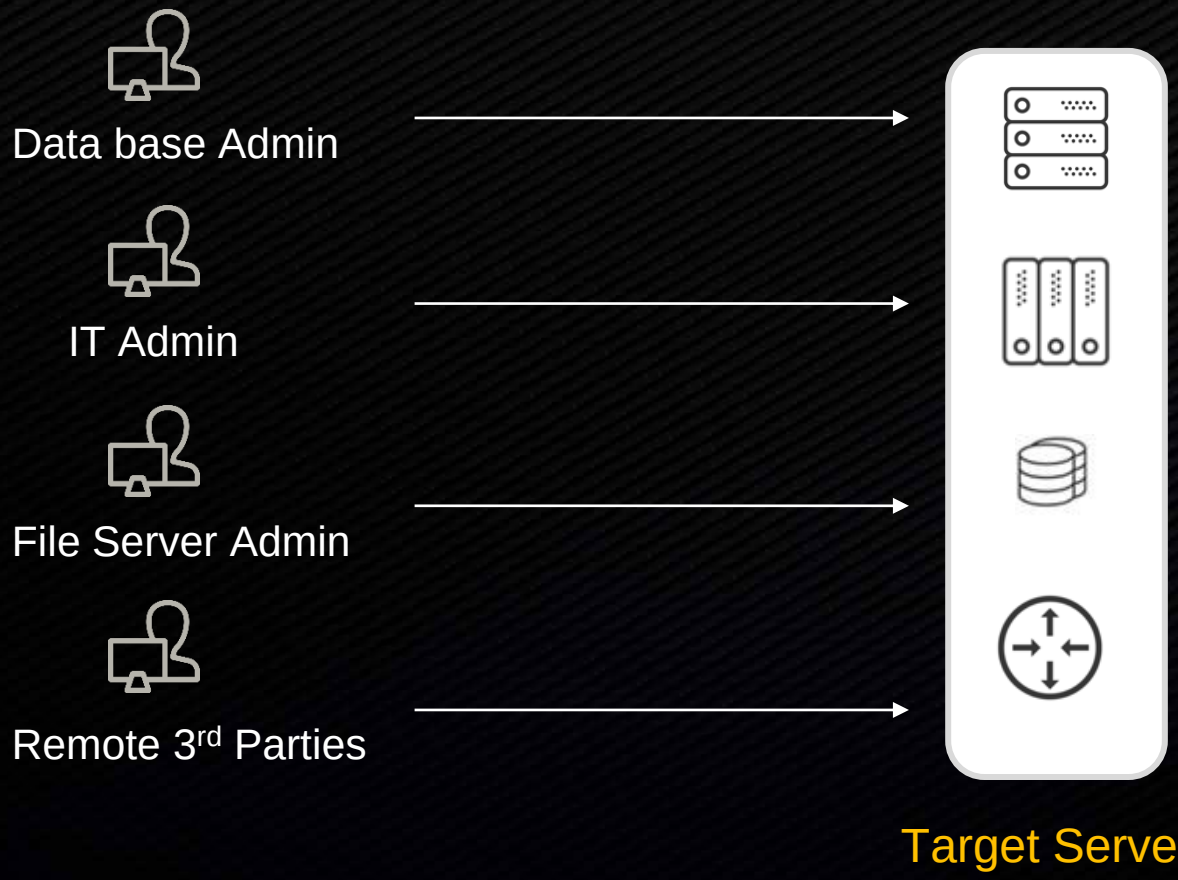
Number of user, devices and Application increase over time

Data breaches may occur more frequently due to password vulnerabilities (such as stale passwords)

The common practice of non-personal super user accounts poses security risks.

Granting more privileges than necessary to every user increases the risk of data loss or theft

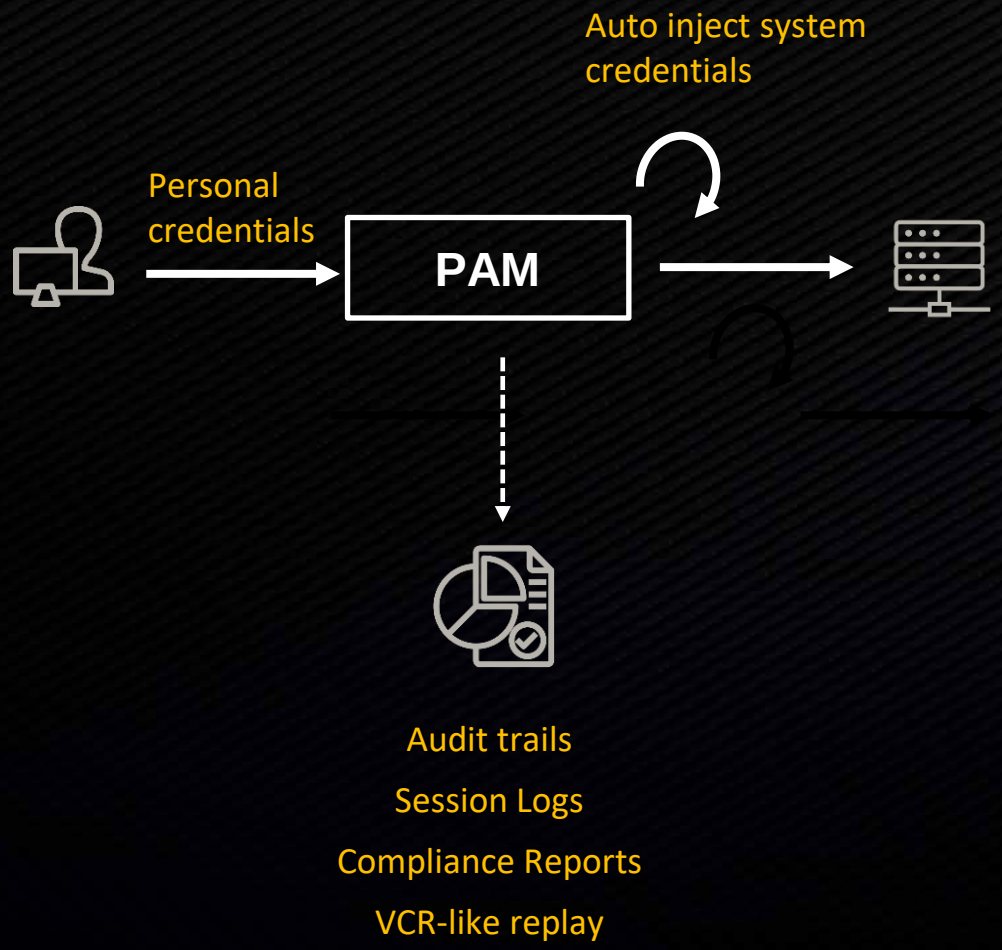
PRIVILEGED ACCESS WITHOUT PAM



Challenges

- Non personal super user account
- Shared Credentials
- Stale Passwords
- Personal administrative rights
- Trust based processes
- More than required level of privileges
- Limited/ Non visibility

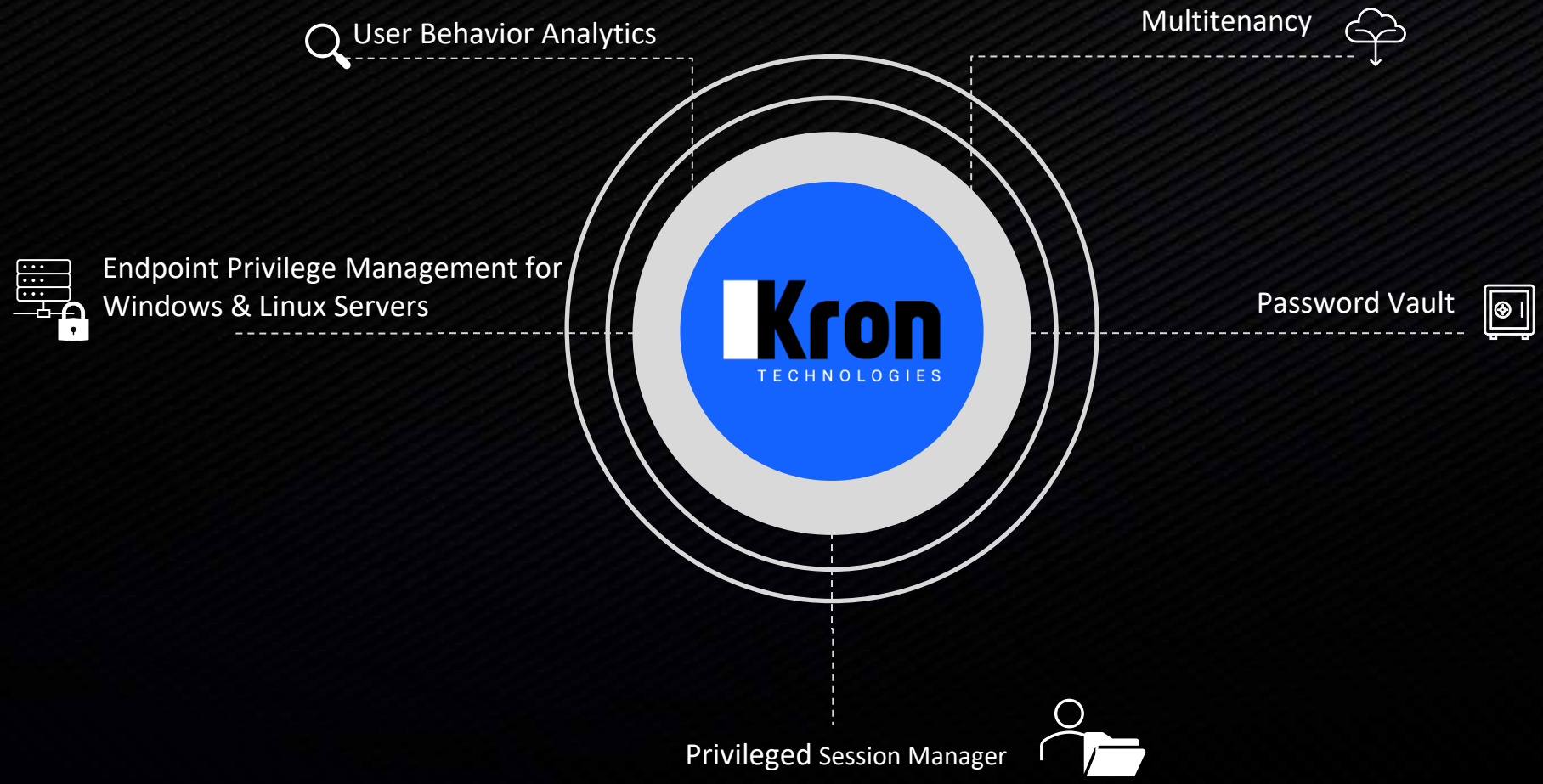
PRIVILEGED ACCESS WITH PAM



Benefits

- No credential exposure
- Preventing stale passwords
- No more personal privileges
- Accountability
- Principle of least privileges
- Segregation of duties
- Regulatory Compliance

SELECTING KRON: OUR PREFERRED PAM SOLUTION



CHOOSING KRON: EXCELLENCE IN PAM SOLUTIONS

Garaj
Cloud Platform by Jazz

Kron
TECHNOLOGIES

Leading provider of advanced technology solutions for Access and Data Security

250+ customers globally in 25 countries

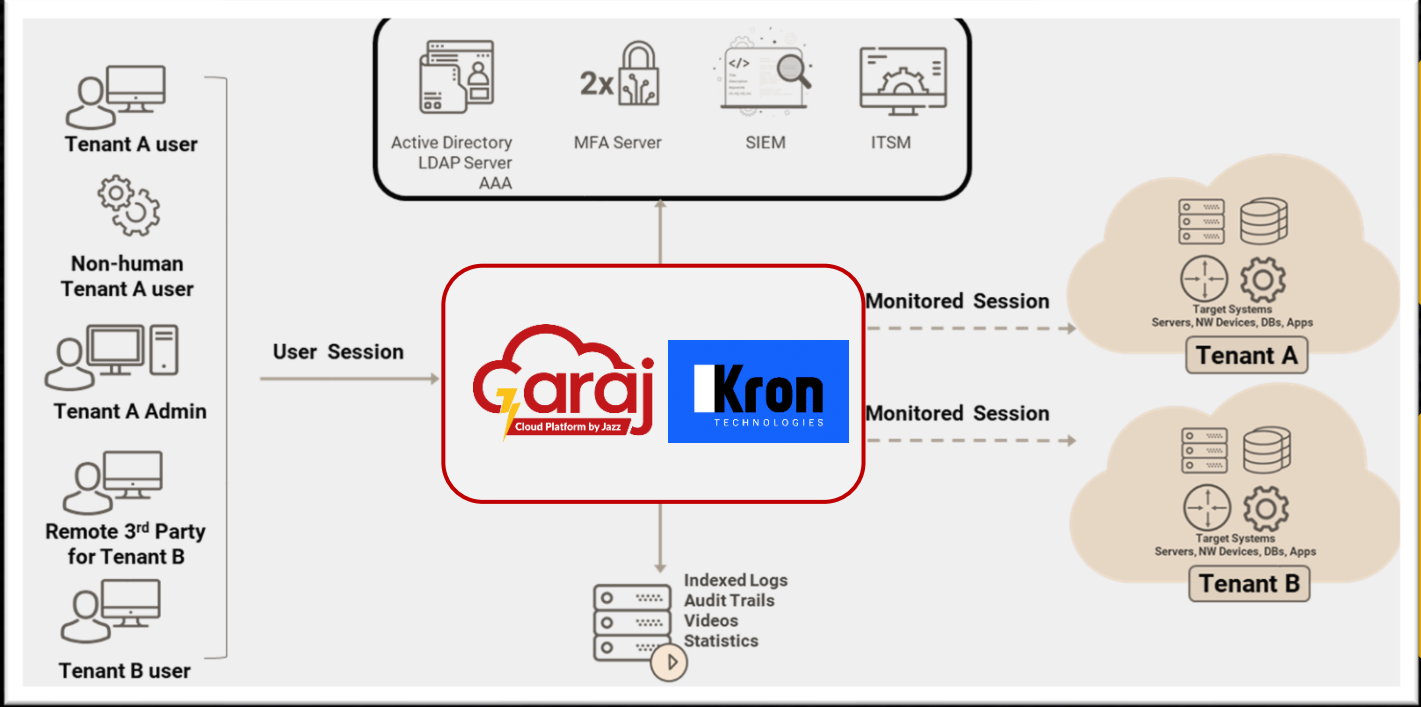
Establish in **2007** and listed on Istanbul Stock Exchange since **2011** globally in 25 countries

All R&D and Product Development done in **Turkey**

Highly recognized by Analyst Firms like Kuppinger Cole, Gartner, Omdia in PAM domain

KRON PAM CUSTOMERS

PAM AS A SERVICE: SECURE AND ISOLATED MULTI-TENANCY



Single Instance

Isolated and virtually separated multiple SingleConnect services running to serve multiple tenants.

Tenant Management

- Tenants manage their own users, devices and policies.
- Tenants can access their audit logs and reports.
- Host Admin cannot access tenant's assets and logs

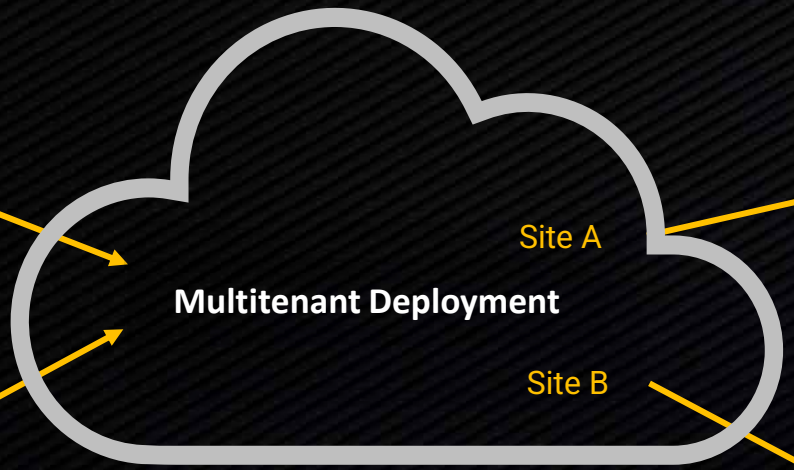
PAM AS A SERVICE: SECURE AND ISOLATED MULTI-TENANCY

Enterprise – A Users

System Admins
Network Admins
Database Admins
3rd Party Users

Enterprise – B Users

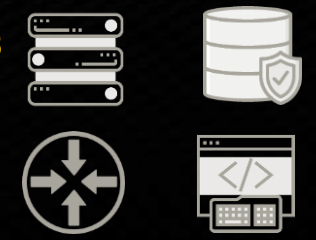
System Admins
Network Admins
Database Admins
3rd Party Users



Enterprise – A Network

Connector A

Connector B



KRON: SINGLE CONNECT MODULES

- Multifactor Authentications
- Password Vault
- Privileged Session Manager

MULTI FACTOR AUTHENTICATION

- Secures your PAM, assets and applications with MFA
- Policy based MFA for preventing unauthorized access
- Apply heuristics to determine risk score
- Integration to external systems

Online Token

SMS, Email, Mobile App

Offline Token

Mobile App, Hard Token,FIDO2 key

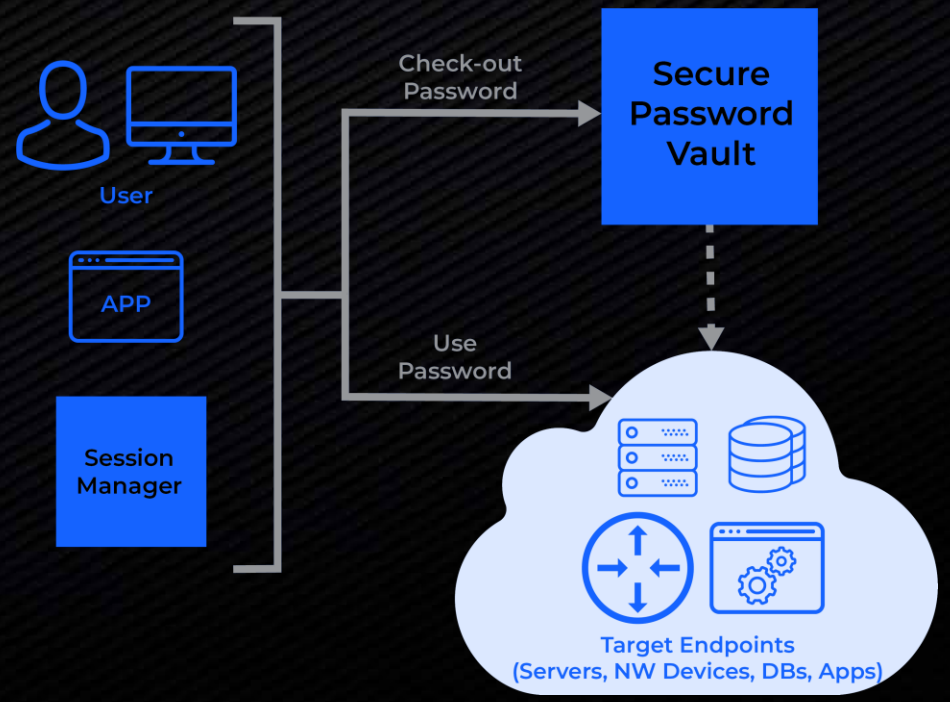
PASSWORD VAULT OVERVIEW

Preserve the system passwords in secure vault

- Operating Systems: Windows/Linux/Unix
- Databases: Oracle, PostgreSQL, MsSQL, etc.
- Devices and Appliances with CLI interface
- Application to Application Password Management

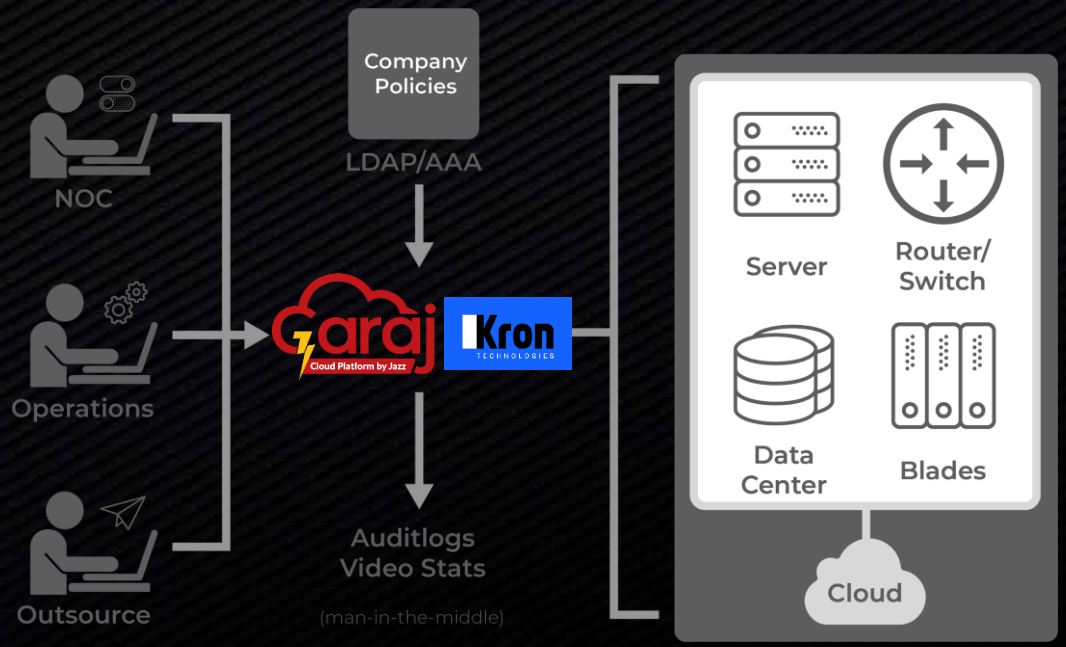
Provides REST APIs to automate provisioning tasks on Ironsphere

- Comprehensive API access for custom workflows and integration
- Create, list, modify and delete entities on PAM
- When integrated, IGA tools can (de)provision privileged user entitlements as life cycle events occur
- When integrated, changes on asset inventory are auto synced



SESSION MANAGER OVERVIEW

Protocols	SSH/Telnet, RDP/VNC, HTTP, SFTP, SQL
Logging and Recording	Logging entire session activities RDP, CLI session video recording
Replay	RDP, CLI session replay Optical Character Recognition for RDP Keylogging
Dual Control	For third party access control Expert guidance or training tool
Command and Context Aware Filtering	Context level policy Limit / filter command sets Black Lists – White Lists
Ensuring Trust and Accountability	No Credential exposure Apply least privilege principle Multi – level approval workflow Geofence MFA



ENABLE ZERO TRUST

Garaj
Cloud Platform by Jazz

Enforce adaptive and Just in Time Access

Allows the privileges of an individual or account to be elevated for specific tasks and then return to their existing privileges

Always verify

- ✓ Mult level Managerial Workflow
- ✓ Multi-factor authentication
- ✓ ITSM integration
- ✓ Geo-fence.

Apply Least Privileges

Ensures that a user account is provisioned with minimum entitlements to complete a specific task.

Monitor & Audit

Monitor every activity related to privileged accounts

YOUR MAIN BENEFIT WITH GARAJ

Scalability

Easily scale up or down based on your organization’s needs

24/7 Support

Access our dedicated support team around the clock.

OPEX Based Billing

Enjoy the advantages of OPEX-based billing for flexible, predictable expenses

Seamless Integration

Fast and efficient deployment process to get you up and running quickly

Top-Tier Security

Benefit from KRON’s robust security features to protect your critical assets

Compliance Assurance

Stay compliant with industry standards and regulations effortlessly.

Garaj

Cloud Platform by Jazz

Technical Support

cloud.support@jazz.com.pk

0304 1110365 (24/7 helpline)

Billing & Invoicing

bizcloudbilling@jazz.com.pk

To Learn More

garaj-cloud@jazz.com.pk

garajcloud.com