# AccessMatrix™ UCM
secure management of credentials

Privileged Access & Account Management

AccessMatrix™ **Universal Credential Manager (UCM)** provides a virtual password safe deposit box protected by **post-quantum safe encryption** (via advanced **ML-KEM**) and optional **HSM** devices, securely storing privileged account IDs and passwords (aka credentials), safeguarding privileged access against emerging quantum threats. UCM delivers robust security features to address the key audit and operational challenges organizations face in managing credentials and session activities.
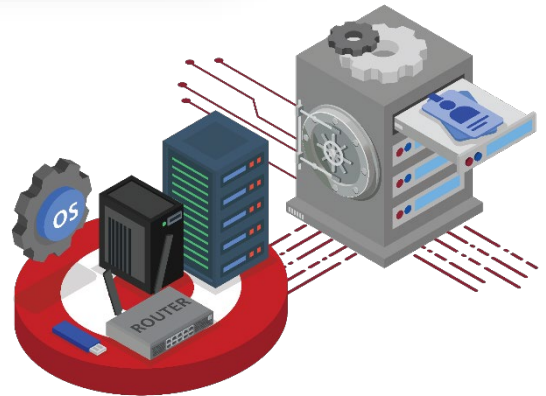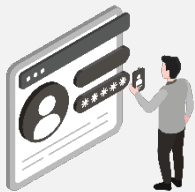
Key Features

Post-Quantum Secure Login
Provides post-quantum secure login with ML-KEM encryption, safeguarding privileged access against emerging quantum threats.

Interactive Session
On-demand password management Privileged User IDs, ensuring immediate retrieval of credentials during emergency or operational requirements for robust security and rapid response.
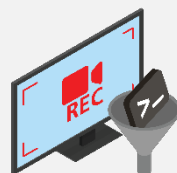
Programmatic Access
Prevent the security exposure of hard coding ID and password (functional ID) in application component for accessing databases and any other resources.
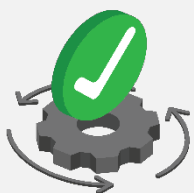
Extendable to Support New Target Systems

Session Recording & Command Filtering for Auditing

Secure & Scalable with High Availability Options

Ease of Deployment & Flexibility

AccessMatrix™ Universal Credential Manager

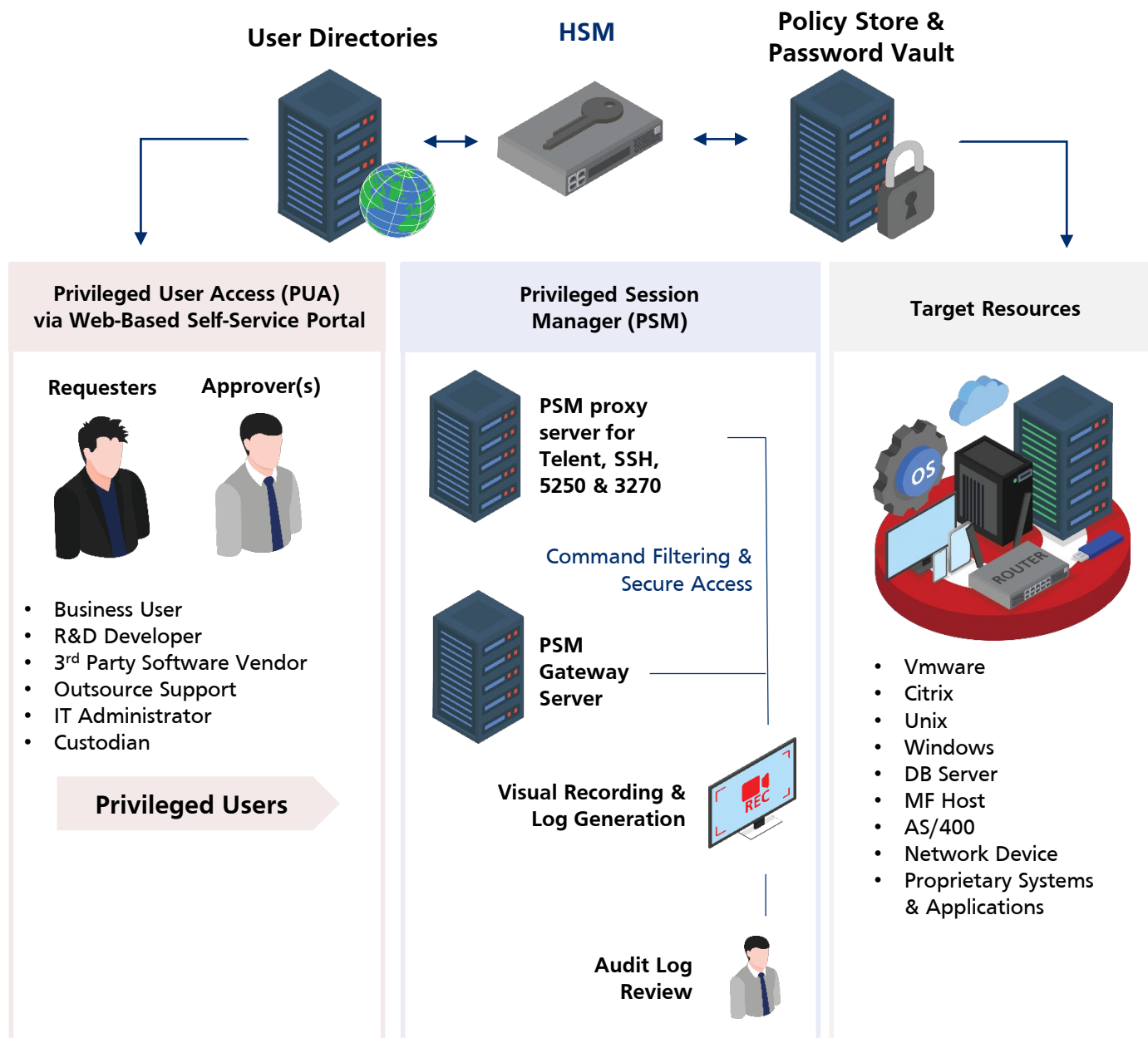## Privileged User Access (PUA) Module

UCM provides a secure approach with multi-level approval flow and empowers organizations to manage security administrators to retrieve and deposit privileged credentials. This enables authorized users to check-in and check-out privileged credentials to perform their duties or during emergency situations.

Privileged Session Manager (PSM) Module

Add-on Windows RDP Gateway Recorder to monitor and record privileged sessions. It supports video recording playback for forensic analysis. It also supports commands access control for selected protocols
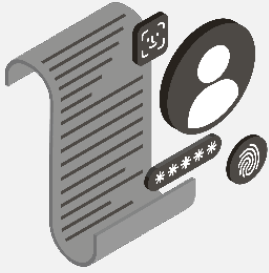
Application Password Manager (APM) Module

Enables organizations to retrieve user IDs and passwords for specific applications during run time so that the user credential information does not need to be hard-coded in applications or command files.

User Directories   **HSM**   **Policy Store & Password Vault**

Privileged User Access (PUA) via Web-Based Self-Service Portal

Requesters   **Approver(s)**

- Business User
- R&D Developer
- 3rd Party Software Vendor
- Outsource Support
- IT Administrator
- Custodian

Privileged Users

Privileged Session Manager (PSM)

PSM proxy server for Telent, SSH, 5250 & 3270

Command Filtering & Secure Access

PSM Gateway Server

Visual Recording & Log Generation

REC

Audit Log Review

Target Resources

OS

ROUTER

- Vmware
- Citrix
- Unix
- Windows
- DB Server
- MF Host
- AS/400
- Network Device
- Proprietary Systems & Applications

End-to-End Privileged Account Activity Management

Core Functions

Policy Driven Approach
Automatically enforces enterprise-wide security policies for passwords, authentication, and access restrictions, ensuring consistent policy application across the organization base on the defined security policy.
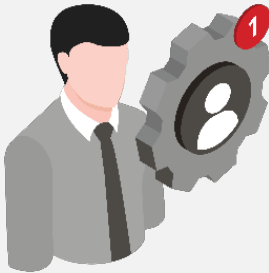
Auto Account Discovery
Provide automatic account discovery report and notify administrators of new accounts not managed by UCM

Workflow Approval
Provides a built-in workflow for secure credential retrieval, and tracking credential usage in performing password reset. Supports multiple workflow types, including multi-level approval, after-hours access, and manager-subordinate workflows, to suit various organizational needs.

Dynamic Tag by Target Resource Type and Credentials
Support tagging of credentials for ease of management and retrieval of credentials and target resources.

Password Consumers & Flexible APIs
Enables organizations to have quick deployment to address the password challenges with APIs and password consumers for dynamic replacement of IDs / password parameters

Web-Based Self-Service Portal
Web portal that enables request submission, check in, check out and approval functionalities with role-based access control

Comprehensive PAAM Features

Build-in workflows for office hours / non-office hours or integrate with external ticketing system

Workflow-driven credentials Check-in / Check-out with auto password update on check-in

Tagging credential (privileged passwords) e.g by project, UAT, production, OS

Bulk Import (CSV import) and Break Glass (backup PDF versioning)

Use encryption key, security policies from Safe with optional HSM protection

Support various authentication options

SSO to target resource with session video recording

Agent & Agentless integration with databases, Unix, Windows, routers, firewalls

Native Integration to existing Enterprise user store or target resource data store

Secure access and seamless connection from any location on any device (desktop, laptop, mobile)

System Requirements

UCM Server / UCM Gateway:
MS Windows 2019 and 2022, RedHat Enterprise Linux 9.x

Java Runtime:
JRE 17 LTS

Database for Policy Store:
MS SQL Server, Oracle RDBMS, and Oracle MySQL

External User Store:
Active Directory, LDAP v3 compliant directories and JDBC compatible databases

Support Target Resources:
JDBC database servers, UNIX Servers, Window Servers, Active Directory, AS400, IBM RACF Mainframe, Cisco / Array, Cisco ACS, Scriptable SSH / Telnet-based network devices e.g TopSec, Juniper, Huawei, H3C and RuiJie, http, https, Z/OS, Weblogic, Websphere and Webportal

Supported clients for UCM Gateway:
Database clients, VNC, rdp, web-based consoles, PuTTY, Tera Term, secureCRT and CuteFTP, WinSCP, SSH Secure File Transfer, IBM Data Studio, Pcomm, Exceed, vSphere Client

Scan for more information

🌐 www.i-sprint.com f iSprintInnov X iSprintInnov in company/i-sprint-innovations

i-Sprint
Trust without Boundaries