AccessMatrix™ UCM Whitepaper

Modern Privileged Access Management
Built for Zero Trust and Quantum Resilience

Abstract

Privileged credentials remain one of the most exploited attack vectors in modern cyber threats. As organizations expand across hybrid infrastructure, cloud platforms, and automated DevOps pipelines, traditional privileged access management (PAM) solutions struggle to provide the flexibility, scalability, and security required to control sensitive credentials. This whitepaper introduces **AccessMatrix™ Universal Credential Manager (UCM)**, a modular privileged access management platform designed to eliminate credential sprawl, enforce policy-driven access, and provide comprehensive session monitoring across enterprise environments.

Built for **Zero Trust architectures and future cryptographic resilience**, AccessMatrix UCM combines centralized credential vaulting, agentless privileged session management, and secure API-based secret delivery within a unified platform. With post-quantum encryption, workflow-based approvals, and integrated auditing capabilities, UCM enables organizations to strengthen privileged access governance while supporting modern operational needs such as DevOps automation, third-party access, and hybrid infrastructure management.

Trademark Information and Disclaimer

Contents

1. Executive Summary

In the evolving threat landscape, privileged credentials represent a critical attack surface. AccessMatrix™ Universal Credential Manager (UCM) by i-Sprint Innovations addresses this risk by delivering a modular, software-based privileged access management solution that is quantum-safe, agentless, and highly integrable.

Designed for organizations seeking secure, efficient, and scalable credential governance, UCM combines interactive access control, session monitoring, and API-level secret delivery to eliminate credential sprawl and strengthen audit compliance.

2. The Risk of Unmanaged Privileged Access

Uncontrolled privileged credentials, whether shared among teams or embedded in scripts, create significant vulnerabilities. These gaps are often exploited in ransomware attacks, insider threats, and regulatory failures. Traditional PAM tools rely on rigid appliance models or intrusive agents, creating friction and complexity that discourage full adoption.

UCM addresses these limitations by delivering:

- Centralized vaulting with post-quantum encryption
- Workflow-driven access based on organizational policy
- Real-time session recording and filtering for audit traceability
- Agentless architecture compatible with enterprise IT environments

3. Solution Overview – What is AccessMatrix UCM?

AccessMatrix UCM is a modular platform composed of three integrated components:

- PUA (Privileged User Access): For interactive access, approval workflows, and credential checkout/check-in with SSO
- PSM (Privileged Session Manager): For session video recording, live monitoring, and command filtering
- APM (Application Password Manager): For secure API-based password retrieval for applications and scripts

Built to support Zero Trust principles, UCM verifies every access request, applies policy-based controls, and ensures credentials are never exposed unnecessarily.

4. Key Capabilities & Features

It includes:

- Post-Quantum Encryption for credential vault and access channels
- Multi-directory user integration (AD, LDAP, JDBC)
- Agentless connection to Windows, Unix, databases, network devices
- Auto-password reset on check-in; rotation policies per system
- Workflow approvals with business-hour and after-hour enforcement
- Session video recording (RDP, SSH, VNC) with real-time monitoring
- Command-level filtering, keystroke logs, and alert generation
- Password retrieval APIs with offline cache for DevOps pipelines

One of UCM's standout differentiators is its support for off-business hour approval workflows. This is especially critical in industries like finance, healthcare, and manufacturing where after-hour maintenance or emergency access is common. UCM enables organizations to define distinct approval rules and restrictions for access during off-hours — something not typically offered by traditional PAM solutions.

5. Platform Benefits

Security	Strong encryption, workflow enforcement, and granular session control prevent unauthorized access.
Compliance	Complete audit trails, session replays, and approval records streamline audits (PCI, HIPAA, ISO).
Flexibility	Software-based deployment supports hybrid and cloud environments without vendor lock-in.
Efficiency	Users and apps retrieve secrets just-in-time without credential sprawl.
Future-Ready	Post-quantum encryption secures critical assets beyond classical cryptography.

6. Architecture Snapshot

UCM follows a layered architecture:

- Credential Vault with PQC-safe encryption
- Policy and Workflow Engine
- Session Gateway (RDP, SSH, VNC)
- API Consumer Layer for app integration
- Log Collector & Analytics for real-time visibility
- Supports HA, geo-redundancy, and integration with ITSM and SIEM tools.

7. Use Case Scenarios

- Secure third-party access with workflow and recording
- Eliminate hardcoded credentials from deployment pipelines
- Enable just-in-time access for IT ops during incidents
- Meet compliance for shared ID usage with full traceability
- Provide password vaulting without deploying endpoint agents

8. Differentiators vs. Traditional PAM

Traditional PAM	AccessMatrix UCM Advantage
RSA/AES encryption	Post-Quantum ML-KEM Encryption
Hardware appliance deployment	Agentless, software-based deployment
Manual credential entry	SSO with credential masking
Separate session recording tools	Integrated session recording & command control
Limited DevOps support	Secure APIs with offline cache and password consumer
No policy for off-hours access	Workflow approvals supporting business & off-business hours
Patch delays, vendor dependency	Customer-managed lightweight upgrades
RSA/AES encryption	Post-Quantum ML-KEM Encryption
Hardware appliance deployment	Agentless, software-based deployment
Manual credential entry	SSO with credential masking
Separate session recording tools	Integrated session recording & command control
Limited DevOps support	Secure APIs with offline cache and password consumer

No policy for off-hours access	Workflow approvals supporting business & off-business hours
Patch delays, vendor dependency	Customer-managed lightweight upgrades

9. Deployment & Integration

UCM is deployable on-prem, in private cloud, or hybrid setups. It integrates with:

- Microsoft Active Directory
- LDAP v3 and JDBC stores
- UCM REST APIs for automation and orchestration
- SIEM tools (Splunk, QRadar)
- ITSM platforms (ServiceNow, BMC)
- MFA: RADIUS, TOTP, biometric integrations (with UAS)

10. About i-Sprint Innovations

i-Sprint Innovations is a global leader in identity, credential, and access management solutions. With customers across banking, government, healthcare, and manufacturing, i-Sprint enables secure digital transformation with a portfolio that spans authentication, SSO, PAM, API security, and credential governance.

AccessMatrix UCM reflects i-Sprint's commitment to building future-ready security solutions aligned with Zero Trust and post-quantum requirements.

Traditional PAM	AccessMatrix UCM Advantage
RSA/AES encryption	Post-Quantum ML-KEM Encryption
Hardware appliance deployment	Software-Based, Cloud/Hybrid Ready
Manual credential entry	SSO & Credential Masking
Separate monitoring tools	Integrated Session Recording & Command Control
DevOps unfriendly	Native API & Secret Injection
Patch delays due to vendor dependency	Rapid, Self-managed Upgrades