

IAM · MFA · SSO · PAM · GOVERNANCE

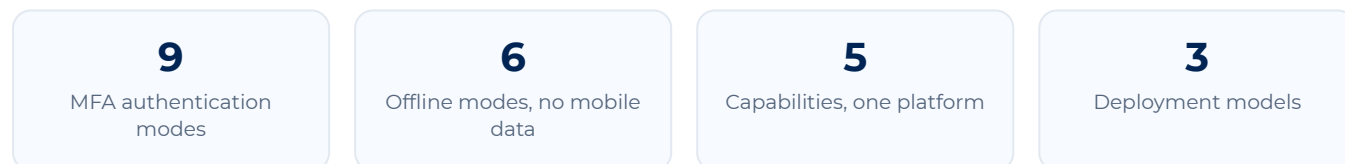
Unified Identity Platform

Secure every identity. Manage every access. Protect every privilege.

Protecting identity and data essential to your business

iSquare TechLabs delivers the Unified Identity Platform, helping organisations improve operational efficiency, reduce cyber risk, simplify access management, strengthen compliance and protect critical business resources.

The Unified Identity Platform brings together Identity Management, Access Management, Multi-Factor Authentication (MFA), Single Sign-On (SSO) and Privileged Access Management (PAM) within a single platform. By consolidating identity services into a unified architecture, organisations can **eliminate identity silos** and adopt a holistic approach to identity security.



The modern identity challenge

Modern enterprises operate across a growing mix of cloud services, SaaS applications, on-premises systems, mobile devices, remote users and privileged accounts. Identity information is frequently distributed across multiple directories, applications and infrastructure platforms.

This fragmented approach increases security risks, administrative complexity, compliance challenges and operational costs. The platform enables organisations to centralise identity management, authentication, governance and privileged access controls through a single platform that provides visibility, control and security across the entire identity lifecycle.



Platform capabilities

01 Identity Lifecycle & Directory Services

Comprehensive identity lifecycle management that automates provisioning, deprovisioning and identity synchronisation across enterprise systems. Integrates with Microsoft Active Directory, LDAP directories, HR systems, enterprise applications and cloud services.

- › Identity synchronisation across directories and applications
- › Directory consolidation to eliminate identity silos
- › Role-based provisioning and access assignment
- › Workflow-driven approvals for access requests

02 Privileged Access Management

Secure, monitor and audit privileged accounts with credential vaulting, Just-In-Time access and session recording, cutting insider and credential-theft risk.

- › Secure privileged credentials in an encrypted enterprise vault
- › Discover and manage privileged, administrative, service and shared accounts
- › Enforce least-privilege and Just-In-Time (JIT) access policies
- › Monitor, record and audit privileged sessions
- › Reduce risks associated with insider threats and credential theft

03 Access Management & Single Sign-On

One secure front door to every application, with federation, identity brokering and adaptive, policy-based access controls.

- › Simplify access across cloud, on-premises and hybrid applications
- › Secure access portal for employees, partners, vendors and customers
- › Identity federation and SSO with SAML, OAuth 2.0 and OpenID Connect
- › Modernise legacy application access while supporting modern authentication standards
- › Implement adaptive and policy-based access controls

04 Multi-Factor Authentication

Out-of-band, risk-based MFA that defeats phishing, man-in-the-middle and SIM-swap attacks across applications, VPNs, desktops and remote environments.

- › Strengthen security using adaptive and risk-based MFA
- › Support Push notifications, QR authentication, GRID, TOTP, Email OTP, SMS OTP, biometrics and FIDO2
- › Protect workforce access across applications, VPNs, desktops and remote environments
- › Reduce account takeover and credential-based attacks
- › Enable passwordless authentication for enhanced security and user experience

05 Identity Governance & Administration

Govern access with automated lifecycle management and centralised audit reporting.

- › Automate user onboarding, offboarding and role management
- › Maintain compliance through centralised audit reporting
- › Ensure users have the right access at the right time
- › Certification reviews and access-governance insight

06 Identity Intelligence & Analytics

A centralised reporting and analytics framework providing visibility into identity activities, access patterns, privileged operations, compliance status and security risks.

- › Identity analytics and reporting
- › Risk visibility and audit trails
- › Compliance dashboards
- › Access governance insights
- › Operational intelligence

Key benefits

● Unified identity security

Consolidate Identity Management, MFA, SSO, governance and PAM into a single platform. Simplify administration while gaining centralised visibility and control across all identities.

● Reduced cyber risk

Protect users and privileged accounts with strong authentication, least-privilege access and intelligent security controls. Reduce the risk of credential theft, account compromise and unauthorised access.

● Improved user experience

Deliver seamless and secure access through Single Sign-On, passwordless authentication and self-service capabilities. Improve productivity while reducing password-related frustrations.

● Enhanced privileged access protection

Secure administrative and high-risk accounts with credential vaulting, session monitoring and Just-In-Time access. Minimise privileged access risks while maintaining operational efficiency.

● Faster compliance & audit readiness

Simplify compliance with centralised auditing, access governance, certification reviews and reporting. Demonstrate compliance and reduce audit preparation efforts.

How the modules deploy

The platform is modular, so you can start with the capability that answers your most pressing risk and add the rest as the programme matures.

DEPLOY ON THEIR OWN

Multi-factor authentication and identity lifecycle each stand alone

ALWAYS PAIRED

Single sign-on and privileged access management both deploy with multi-factor authentication

SHARED THROUGHOUT

Whatever combination you run shares one policy engine and one audit trail

Why the Unified Identity Platform

Lower total cost of ownership	Replace multiple standalone identity and security products with a unified platform. Reduce infrastructure, licensing, integration and operational costs while improving security outcomes.
Centralised identity lifecycle management	Automate user onboarding, access changes and offboarding across enterprise systems. Ensure users receive the right access at the right time throughout their lifecycle.
Zero Trust security foundation	Implement a Zero Trust approach by continuously verifying identities and enforcing least-privilege access. Secure every access request based on context, risk and policy.
Unified visibility & control	Gain a single view of identities, access rights, authentication events and privileged activities. Improve decision-making with centralised monitoring and reporting.
Hybrid & multi-cloud ready	Secure identities consistently across cloud, on-premises and hybrid environments. Support modern IT infrastructures without adding complexity.

Flexible deployment

Deploy **on-premise** for full control inside your own data centre, in a dedicated **private cloud**, or fully managed **as a service**. Six of the nine authentication modes work entirely offline, needing no mobile internet — which matters for plant floors, branches and field staff.

About iSquare TechLabs

iSquare TechLabs is an Information Security company delivering innovative solutions. Our strength lies in building strong products that provide best-in-class identity authentication and data protection. We secure both sides of the enterprise — the Unified Identity Platform controls who gets in, while Data Loss Prevention controls what goes out.



+91 86670 69354

sales@isquaretechlabs.com

www.isquaretechlabs.com



Scan to visit