fálaina

Converged . Modernized . Intelligent

Product Data Sheet:

Multi-factor Authentication (MFA)

With the rising number of cyber threats, password-based authentication alone is no longer sufficient to protect enterprise applications and sensitive data. Multi-Factor Authentication (MFA) has become a critical security layer to prevent credential-based attacks such as phishing, brute force, and account takeovers.

Fálaina Multi-Factor Authentication (MFA) is a modern authentication solution designed to provide phishing-resistant, password-less authentication and adaptive risk-based security across cloud, on-premise, and hybrid environments. Built on the principles of Zero Trust and identity-first security, Fálaina MFA enables enterprises to eliminate credential-based attacks while ensuring seamless and secure access for users.

Falaina MFA Key Functionalities:

1. **Phishing-Resistant MFA**
   - Supports FIDO2, passkeys, certificate-based authentication (X.509), and biometric authentication to eliminate phishing and MFA bypass attacks.
   - Strengthens authentication security with hardware security keys, smartcards, and mobile-based biometric authentication.

2. **Password-less Authentication**
   - Enables biometric authentication, security keys, mobile push authentication, and device-bound credentials to eliminate passwords.
   - Supports adaptive authentication policies to provide frictionless yet secure access.

Industry Trends & Statistics:

- By 2027, 90% of enterprises will fully meet their MFA needs for remote and cloud access using the native capabilities of AM tools, reducing the total cost of ownership (TCO) by 40%.
- More than 90% of MFA transactions using a token will be based on FIDO authentication protocols (e.g., passkeys) natively supported in AM tools.
- Phishing-resistant MFA adoption is accelerating as attackers exploit vulnerabilities in legacy MFA methods.
- Password-less authentication adoption is growing, with enterprises prioritizing biometric authentication and passkeys.

Source: Gartner

fálaina

3. **Adaptive Risk-Based Authentication**
   - Dynamically adjusts authentication based on user behaviour, device health, location, and security signals.
   - Uses AI-driven analytics to detect anomalies and enforce risk-based authentication policies.
4. **Seamless IAM & SSO Integration**
   - Integrates with Fálaina UAM, Microsoft Entra ID, Okta, Ping Identity, ForgeRock, and other IAM providers for centralised authentication.
   - Supports federated identity management to enable cross-domain authentication and seamless access experiences.
5. **Flexible MFA Methods & Authentication Options**
   - Supports SMS, OTP, push notifications, smartcards, security keys, passkeys, and voice recognition to provide diverse authentication choices.
   - Offers adaptive step-up authentication for high-risk transactions and privileged access.
6. **AI-Powered Fraud Detection & Threat Mitigation**
   - Detects session hijacking, MFA prompt bombing, and anomalous user behaviour in real time.
   - Integrates with SIEM platforms to trigger automated responses to suspicious authentication attempts.
7. **Universal Authenticator App for Any Environment with Integrated IGA**
   - Provides a Fálaina Authenticator to support secure authentication for applications, systems, databases, and network devices.
   - Enables QR code-based authentication, time-based OTPs, and FIDO2-compliant push notifications.
   - Support account unlock and password reset with other IGA functionalities such as workflow approval.
8. **Zero Trust Ready & Continuous Authentication**
   - Ensures continuous user verification throughout active sessions, preventing session hijacking and unauthorised re-authentication.
   - Implements adaptive authentication policies to enforce Zero Trust security principles.
9. **Comprehensive SDK for Developer Integration**
   - Provides a full-featured SDK for integrating Fálaina MFA into third-party applications with multi-platform libraries.
   - Supports flexible authentication methods, robust security protocols, and extensive developer resources for seamless integration.

Business Benefits:

- Eliminates Credential-Based Attacks – Phishing-resistant MFA methods prevent unauthorised access and account takeover attacks (ATO).
- Seamless User Experience – Password-less authentication minimises friction and login fatigue while improving security.
- Meets Regulatory Compliance – Helps organisations comply with GDPR, HIPAA, NIST, ISO 27001, and financial regulations.
- Reduces IT Costs & MFA Fatigue – Reduces password resets, IT support tickets, and authentication-related operational costs.
- Enhances Security for Hybrid & Multi-Cloud Environments – Protects access across On-premise, cloud, and SaaS applications.

fálaina

Case Studies

- **Defence Organisation**
  - Challenge: Needed a phishing-resistant MFA solution for remote employees and privileged users.
  - Outcome: Implemented FIDO2 authentication, reducing phishing attacks by 85% and improving compliance.
- **Healthcare Provider**
  - Challenge: Ensuring secure authentication for doctors, patients, and third-party vendors.
  - Outcome: Adopted adaptive MFA policies, reducing unauthorised access attempts by 70%.

Technical Specifications

- Deployment Models: SaaS, on-premises, and hybrid options with a unified codebase.
- Integrations: Prebuilt protocols support applications, including legacy On-premise, cloud and SaaS applications.
- Scalability: Designed for mid-market and large enterprises with dynamic
- scalability.
- API Support: RESTful APIs for custom integrations.

Pricing and Licensing

- Pricing Model: Subscription
- User Licensing: Flexible plans based on the number of users, customers and machines identities.
- Support Packages: Available in Basic, Standard, and Premium tiers, offering various levels of support and response times.

Why Fálaina?

We get it — Securing authentication across diverse environments can be complex and overwhelming. That's why we've built a solution that simplifies authentication, strengthens security with adaptive MFA, and ensures seamless, password-less access—giving you full control over who verifies their identity, when, and how.

- End-to-End MFA & Password-less Security – Supports biometric authentication, passkeys, and AI-powered risk-based authentication.
- Seamless Integration with Identity Ecosystem – Works with SSO, IGA, PAM, and external identity providers.
- AI-Driven Adaptive Authentication – Reduces MFA fatigue while enforcing real-time, risk-based authentication policies.
- Enterprise-Grade Scalability & Performance – Supports millions of authentication requests per second.
- Zero Trust & Compliance Ready – Aligns with NIST 800-63B, FIDO2, GDPR, and HIPAA security frameworks.

fálaina

Simplify and Strengthen Your Authentication Security

Managing authentication security shouldn't be complicated or overwhelming. With Fálaina Multi-Factor Authentication (MFA), you can eliminate credential-based attacks, enforce phishing-resistant authentication, and enable seamless password-less access—enhancing security, compliance, and user experience with ease.

Ready to Strengthen Your Authentication Security?

- Visit www.falainacloud.com to learn more.
- Email us at sales@falainacloud.com to schedule a demo or talk to our team.

Turn Authentication Security into Your Strongest Defense.

About Falaina

Falaina is at the forefront of cybersecurity innovation, delivering Converged Identity and Access Management (IAM) solutions that empower organisations to protect and optimise their digital ecosystems with unparalleled precision, scalability, and efficiency. Purpose-built to tackle the complexities of modern cybersecurity, Falaina's unified platform integrates powerful capabilities, including Identity Governance and Administration (IGA), Privileged Access Management (PAM), Data Access Governance (DAG), Access Management (AM), and Zero Trust Architecture.

With Falaina, identity security becomes the foundation of progress, helping businesses navigate the future with confidence, resilience, and agility.

fálaina