

White Paper:
**Fálaina Managed IAM
Security Services**
Driving Identity Security Through
Integrated Managed Solutions

Introduction

In today's complex and rapidly evolving cybersecurity landscape, protecting digital identities is more crucial than ever. Enterprises face unprecedented challenges, from sophisticated cyber threats to strict compliance requirements and an increasing reliance on hybrid and multi-cloud environments.

To address these challenges, organisations must implement comprehensive, scalable, and integrated security solutions. However, managing identity and access infrastructure in-house can be resource-intensive, complex, and costly. This is where Fálaina Managed Security Services (MSS) come in—offering a suite of advanced, AI-driven security solutions designed to simplify operations, enhance security, and ensure regulatory compliance.

Fálaina's MSS solutions include:

- Managed Identity Governance and Administration (IGA) - Powered by IACM and ILM products
- Managed Privileged Access Management (PAM)
- Managed Access Management - Integrating UAM and MFA products

Fálaina MSS is purpose-built to empower Managed Security Service Providers (MSSPs) and enterprises to overcome modern security challenges, automate key processes, and accelerate Zero Trust implementation.

Why Choose Managed Services for IAM Solutions?

Outsourcing IAM to an MSSP like Fálaina delivers significant benefits, ensuring robust security while reducing operational complexity and costs. Key reasons to choose managed services for IAM include:

- Expertise and Specialisation: Gain access to dedicated experts with deep experience in managing identity security, ensuring the latest industry standards and security practices.
- Cost Efficiency: Avoid heavy capital investments and reduce operational costs with scalable, subscription-based models.
- Rapid Deployment: Accelerate time-to-value with pre-configured solutions, ready for quick deployment and immediate impact.
- 24/7 Monitoring and Support: Proactive threat detection and continuous monitoring minimise risks and prevent security incidents.
- Scalability: Easily scale security operations as your business grows, without compromising security posture.
- Compliance Support: Meet regulatory and audit requirements with automated reporting and compliance frameworks.
- Operational Efficiency: Free up internal resources to focus on core business operations while leaving security management to experts.

By partnering with Fálaina MSS, organisations can enhance security resilience, improve operational efficiency, and ensure sustainable compliance.

Managed Identity Governance and Administration (IGA)

Fálaina's Managed IGA service, powered by IACM and ILM products, ensures seamless identity lifecycle management and continuous compliance across digital ecosystems.

Key Features:

- Automated Lifecycle Management: Streamlines onboarding, role changes, and off-boarding processes.
- Identity Visibility: Provides complete oversight of human and machine identities.
- AI-Driven Role Optimisation: Recommends optimal role structures to eliminate privilege creep.
- Automated Access Reviews: Ensures access rights are continuously monitored and verified.
- Policy Enforcement: Enforces organisational access policies and segregation of duties.
- SIEM Integration: Enhances threat detection and response with real-time analytics.

Why It Matters:

- Reduces Identity Risk: Ensures only authorised users have access to critical resources.
- Supports Compliance: Automates audit processes and provides real-time reporting.
- Enhances Security Posture: Continuously monitors identity access for security gaps.

Use Cases:

- Automated Onboarding/ Off-boarding: Simplify user provisioning with automated identity lifecycle processes.
- Continuous Access Reviews: Proactively detect and remediate access risks.
- AI-Powered Role Management: Utilise insights to optimise roles and eliminate unnecessary access rights.

Refer to IACM and ILM product data sheet for more functionalities supported.

Managed Privileged Access Management (PAM)

Fálaina's Managed PAM solution provides comprehensive security for privileged accounts across on-premise, hybrid, and multi-cloud environments.

Key Features:

- Zero Standing Privilege (ZSP): Ensures no permanent access privileges, granting access only when needed.
- Just-in-Time (JIT) Access: Provides temporary, time-limited access to privileged accounts.
- Credential Vaulting: Secure storage and rotation of sensitive credentials to prevent unauthorised access.
- Privileged Session Monitoring: Continuous session tracking with AI-powered risk analysis.
- Automated Risk Scoring: Real-time assessment and alerts for high-risk activities.
- Integration with DevOps: Secure credential management for automated CI/CD pipelines.

Why It Matters:

- Prevents Credential Theft: Safeguards privileged credentials against internal and external threats.
- Enhances Regulatory Compliance: Detailed logs and audit reports simplify compliance reporting.
- Improves Operational Efficiency: Automates credential management and reduces manual effort.

Use Cases:

- DevOps Secrets Management: Secure secrets and credentials used in automated pipelines.
- Third-Party Access Governance: Grant temporary, controlled access to vendors with full session visibility.
- Risk-Based Access Monitoring: Identify and mitigate suspicious activities across privileged accounts.

Refer to PAM product data sheet for more functionalities supported.

Managed Access Management

Fálaina's Managed Access Management, powered by UAM and MFA products, ensures adaptive and frictionless access across applications and systems.

Key Features:

- Unified SSO and Federated Authentication: Simplifies access to multiple systems through a single sign-on experience.
- Adaptive MFA: Risk-based multi-factor authentication, supporting biometrics, OTPs, and device-based authentication.
- API Security and Governance: Ensures secure access for third-party integrations and applications.
- Context-Aware Access Control: Adjusts access levels based on device, location, or user behaviour.
- Session Validation: Continuously validates active sessions to mitigate session hijacking risks.

Why It Matters:

- Enhances User Experience: Delivers seamless, secure access across systems.
- Strengthens Security: Adaptive MFA and contextual access policies mitigate identity threats.
- Enables Compliance: Ensures regulatory adherence through automated access control and reporting.

Use Cases:

- Secure Remote Access: Use adaptive MFA to provide secure access for remote employees.
- Password-less Authentication: Implement biometrics for frictionless and secure authentication.
- Granular API Access Control: Secure third-party integrations with robust API governance.

Refer to UAM and MFA product data sheet for more functionalities supported.

Implementation Approach

1. Assessment & Planning

- Conduct comprehensive security assessments to understand current security posture, identify vulnerabilities, and determine regulatory obligations.
- Engage with key stakeholders to define business objectives, operational requirements, and desired security outcomes.
- Develop a detailed implementation roadmap, outlining key phases, timelines, resource allocations, and milestones to ensure alignment with organisational goals.

2. Solution Design

- Customise MSS solutions by aligning them with specific organisational needs, risk tolerance levels, and compliance standards.
- Design architecture that integrates seamlessly with existing infrastructure while ensuring scalability for future requirements.
- Develop security policies, workflows, and operational guidelines to streamline processes and ensure consistency.

3. Deployment & Integration

- Execute a phased deployment to minimise disruptions to ongoing business operations.
- Conduct pilot implementations to validate solution effectiveness and fine-tune configurations.
- Integrate MSS solutions with existing IT systems, identity frameworks, and security platforms to ensure a cohesive security ecosystem.
- Provide hands-on training and knowledge transfer to internal teams to ensure smooth adoption.

4. Optimisation & Automation

- Leverage AI and machine learning to identify security gaps, automate repetitive tasks, and enhance threat detection.
- Continuously refine workflows and security protocols to maximise efficiency and reduce manual intervention.
- Implement automated remediation processes to respond swiftly to security incidents and minimise potential impact.

5. Monitoring & Reporting

- Establish 24/7 monitoring to detect and respond to potential threats in real-time.
- Generate detailed compliance and performance reports, offering insights into security posture, incident trends, and risk mitigation strategies.
- Regularly review security metrics and adjust strategies to align with evolving cyber threats and business objectives.

Why Partner with Fálaina for MSS?

- **Cost-Effective:** Leverage a subscription-based model that minimises upfront capital expenditure and allows for predictable, scalable financial planning. This approach helps businesses avoid high infrastructure and operational costs while gaining access to top-tier security services.
- **Rapid Deployment:** Utilise pre-configured templates and standardised processes for fast and efficient solution deployment. This approach accelerates time-to-value, allowing organisations to enhance their security posture without lengthy implementation cycles.
- **Enhanced Security Posture:** Gain from AI-powered insights that provide proactive threat detection, continuous risk assessment, and automated response mechanisms. This strengthens the overall security framework, ensuring organisations are protected against both current and emerging threats.
- **Automated Compliance:** Simplify the audit process with comprehensive, automated reporting frameworks that deliver real-time insights into compliance status. This not only reduces the manual burden of audit preparation but also ensures continuous adherence to regulatory standards.
- **Expert Support:** Access to industry-leading security experts for strategic consultation, threat response, and best-practice recommendations. Enjoy 24/7 monitoring and support services to ensure immediate assistance and continuous system protection.

Conclusion

Managing identity security doesn't have to be complex or costly. Fálaina's Managed Security Services (MSS) deliver scalable, AI-driven, and integrated solutions designed to simplify security operations, ensure compliance, and elevate organisational resilience. Whether you're an enterprise strengthening security or an MSSP expanding service portfolios, Fálaina MSS provides the expertise, automation, and adaptability to meet evolving cybersecurity challenges.

Ready to Strengthen Your Security Operations?

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

Let's transform managed security into your organisation's strongest advantage.



About Fálaina

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