Managed Azure Security Services

Simform delivers managed security services on Azure through 24×7 monitoring, structured governance, and Microsoft-native security services, enabling continuous protection at scale, reducing risk, and improving overall security posture.

Overview summary

As Azure environments grow in scale and complexity, security challenges rarely stem from missing tools, but from fragmented ownership, inconsistent governance, and reactive operations. Simform's managed Azure security services help organizations turn Microsoft security capabilities into consistent, day-to-day security operations. The result is continuous protection, clearer accountability, and security operations that scale without compromising compliance, performance, or cost control.

- **24×7 security operations:** Round-the-clock monitoring and incident management across Azure environments, with structured detection, triage, and escalation to ensure consistent and timely response.
- **Threat detection and response:** Continuous threat detection, investigation, and response using Microsoft Sentinel and Microsoft Defender to reduce mean time to detect and contain security incidents.
- **Security posture and compliance management:** Ongoing visibility into security posture and configuration risks using Microsoft Defender for Cloud, with continuous alignment to regulatory and compliance requirements.
- **Identity and access governance:** Centralized identity security using Microsoft Entra ID, including multi-factor authentication, privileged access management, and conditional access to reduce identity-based risk.
- **Centralized governance & operations:** Secure, multi-tenant Azure management using Azure Lighthouse, combined with centralized logging, alert correlation, and integration with ITSM and FinOps workflows.

What you get

- Continuous security coverage across Azure environments, with coordinated monitoring, investigation, and response that reduces blind spots and shortens time to contain incidents.
- A consistent, audit-ready security posture across subscriptions and tenants, with unified controls and visibility that support regulatory, customer, and internal assurance requirements.
- Clear operational ownership of Azure security, with defined escalation paths and repeatable processes that reduce reliance on reactive, ad-hoc response.

Simform and Azure – Empowering digital transformation with cutting-edge AI/ML

Simform specializes in Cloud/MACH architectures, DevOps, data, and AI using Azure technologies. From SaaS development to advanced AI integrations, our Azure services align with Microsoft's well-architected framework to deliver highly performant, efficient, and secure cloud solutions.

Digital Product Engineering

- Cloud native and MACH development
- Serverless API development
- Application modernization
- Advanced DevOps transformation
- API management and integrations
- PaaS integrations
- Low-code development with Power Platform

Data & AI/ML Engineering

- Data engineering and analytics
- Data platform modernization
- GenAI using Azure AI Studio
- Data science and ML
- Azure AI services PaaS

Infrastructure Engineering

- Migration assessment and implementation
- Well architected reviews
- Kubernetes and containerization
- Infrastructure as a Code
- Unified observability
- Cloud governance and FinOps
- Hybrid cloud and VDI migration

Security and Compliance Engineering

- Security posture improvement
- DevSecOps
- Compliance management
- Vulnerability assessment and penetration testing

75+ Azure-certified engineers

250+ Microsoft developers

50+ Projects delivered