YASH Technologies

More than what you think.

AI Security Posture Management (AI-SPM) with Defender for Cloud

Secure your AI/ML workloads across Azure, AWS, and GCP with AI BOM discovery, posture governance, and attack-path reduction.

YASH Technologies' ***AI-SPM with Microsoft Defender for Cloud*** helps organizations discover AI assets, evaluate exposure, and reduce AI-related risk across multicloud environments. From AI component visibility to posture and compliance alignment, we enable secure AI adoption without slowing innovation.

Key Highlights

AI BOM Discovery	*Multicloud Coverage (Azure / AWS / GCP)*	*IaC Misconfiguration Detection*	*Attack Path Analysis*	*Compliance Mapping*	*Sentinel + SIEM/ SOAR Integration*

Engagement Structure

Phase 1: Assessment & AI Posture Discovery

Activities:

- AI workload discovery + AI BOM mapping
- Identify posture gaps across AI services and cloud resources
- Review Defender for Cloud coverage for AI workloads
- Initial compliance readiness review for AI governance requirements

Benefits:

- Clear AI asset visibility and ownership mapping
- Faster identification of hidden risks in AI pipelines
- Strong baseline for AI posture governance

Deliverables:

- AI security posture assessment report
- AI BOM visibility snapshot
- Prioritized risk findings & recommendations

Phase 2: AI-SPM Enablement & Configuration

Activities:

- Enable AI-SPM capabilities in Defender for Cloud
- Configure posture policies aligned to AI governance goals
- Detect IaC and service-level misconfigurations impacting AI security
- Enable attack path analysis and risk prioritization workflows
- Integrate outputs with Sentinel / SIEM-SOAR systems

Benefits:

- Structured rollout with faster time-to-value
- Reduced risk exposure across multicloud AI services
- Integrated workflows for security and compliance teams

Deliverables:

- Configured AI-SPM posture policies
- Risk prioritization views + attack path mapping outputs
- Integration reference documentation & KT support

Phase 3: Continuous Optimization (BAU Support)

Activities:	*Benefits:*	*Deliverables:*
• Continuous monitoring of posture changes and AI exposures • Risk tuning and improvement recommendations • Regular compliance posture reviews • Advisory for new Defender for Cloud AI-SPM capabilities	• Improved AI posture maturity over time • Reduced manual governance overhead • Sustained compliance readiness	• Monthly posture insights report • Updated posture baselines • Recommendations roadmap

Our end-to-end Approach

AI BOM Discovery → Posture Insights → Attack Path Reduction

YASH's Unique Strengths in AI-SPM Enablement

- AI governance-first security posture strategy
- Defender for Cloud + multicloud security expertise
- AI risk prioritization using posture + attack path context
- Compliance readiness for regulated industries
- Security integration into existing SecOps operating model

Duration: (in days / weeks):	***Price:***	***Industry:***
4–8 weeks (Assessment + Enablement) | Ongoing BAU support (optional)	Custom pricing based on scope and AI/cloud footprint	Healthcare | BFSI | Manufacturing | Energy | Retail and more

YASH Technologies
More than what you think.

Global Presence: AMERICAS | EUROPE | APAC | MEA

World HQ: 841 Avenue of the Cities East Moline IL-61244 USA

Tel: 309-755-0433 | **Fax:** 309-796-1242 | www.yash.com

For more information contact YASH today at ***info@yash.com*** or scan here