

# 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:

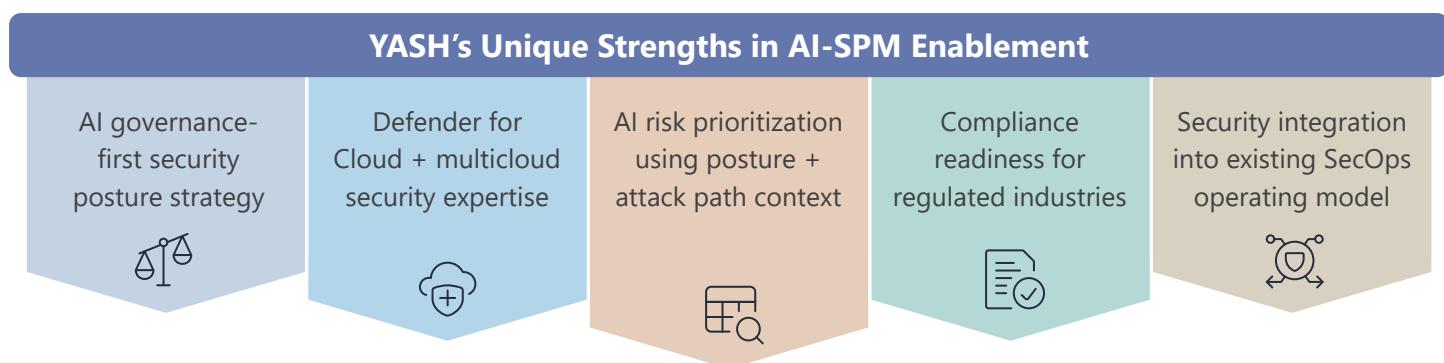
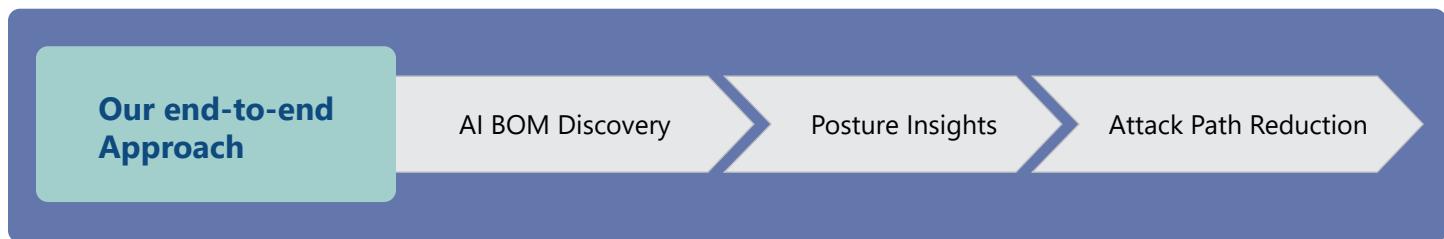
- Structured rollout with faster time-to-value
- Reduced risk exposure across multicloud AI services
- Integrated workflows for security and compliance teams

#### 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:
<ul style="list-style-type: none"> <li>Continuous monitoring of posture changes and AI exposures</li> <li>Risk tuning and improvement recommendations</li> <li>Regular compliance posture reviews</li> <li>Advisory for new Defender for Cloud AI-SPM capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Improved AI posture maturity over time</li> <li>Reduced manual governance overhead</li> <li>Sustained compliance readiness</li> </ul>	<ul style="list-style-type: none"> <li>Monthly posture insights report</li> <li>Updated posture baselines</li> <li>Recommendations roadmap</li> </ul>



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

