YASH Technologies
More than what you think.

Vulnerability Management with Microsoft Defender

Continuous discovery, risk-based prioritization, and automated remediation powered by Microsoft Defender Vulnerability Management

Modern enterprises operate across hybrid environments where vulnerabilities evolve faster than traditional scanning cycles can handle. YASH delivers a structured Vulnerability Management service using Microsoft Defender Vulnerability Management (MDVM), enabling real-time visibility, intelligent prioritization, and integrated remediation across endpoints, cloud workloads, and containers—ensuring a proactive and unified security posture.

What this engagement solves

Enterprises often struggle with:

- **Limited visibility** across hybrid environments and asset sprawl
- **Overwhelming vulnerability** volumes with no risk-based prioritization
- **Delayed remediation cycles** due to manual processes
- **Fragmented security** tools lacking unified insights
- **Compliance reporting** that is reactive and resource-intensive

This offering bridges the gap between **visibility, prioritization, and action**, ensuring vulnerabilities are addressed based on real-world risk.

Key Highlights

Continuous vulnerability discovery across endpoints and cloud workloads	*Risk-based prioritization using Microsoft Threat Intelligence*	*Unified visibility with Defender for Endpoint and Defender for Cloud*	*Automated remediation workflows and patching guidance*	*Detection of misconfigurations and insecure settings*	*Integration with Microsoft Sentinel and ITSM tools for tracking*

Engagement Approach (Assessment | Implementation | BAU)

Phase 1: Assessment Phase

Activities:

- Discover and map assets across on-premises and multi-cloud environments
- Assess vulnerabilities and configurations across endpoints, servers, and containers
- Map compliance requirements (GDPR, HIPAA, ISO 27001) to current posture

Benefits:

- Complete visibility into vulnerability exposure across hybrid environments
- Risk-based prioritization aligned to business impact
- Clear understanding of compliance gaps and security posture

Deliverables:

- Security posture report with prioritized vulnerabilities
- Misconfiguration and vulnerability analysis with remediation actions
- Compliance gap assessment aligned to regulatory standards

Phase 2: Implementation Phase

Activities:

- Deploy and configure MDVM across endpoints and cloud workloads
- Integrate with Defender for Endpoint, Defender for Cloud, and Microsoft Sentinel
- Configure:
  - Risk-based alerting and prioritization
  - Automated remediation workflows
  - Policy baselines and security controls

Benefits:

- Unified vulnerability visibility across the Microsoft security ecosystem
- Faster remediation through automation and orchestration
- Improved security posture with proactive vulnerability management behaviors affecting AI workloads

Deliverables:

- Fully configured MDVM environment (production-ready)
- Custom alerting rules and automation playbooks
- Integration runbooks and operational documentation
- Knowledge transfer for security and IT teams

Phase 3: BAU Phase (Continuous Monitoring & Optimization)

Activities:

- Continuous vulnerability monitoring and risk assessment
- Policy tuning and baseline optimization
- Monthly posture reviews and remediation tracking
- Optional threat hunting and incident investigation via SIEM

Benefits:

- Continuous reduction in attack surface and exposure risk
- Improved remediation efficiency over time
- Sustained compliance readiness and reporting visibility

Deliverables:

- Weekly/monthly vulnerability reports with trend analysis
- Updated policy baselines and exception tracking
- Incident summaries and remediation insights
- Strategic advisory roadmap for ongoing improvements

Core Framework Components

PHASE	KEY ACTIVITIES
Discover	Identify all assets including endpoints, servers, and cloud workloads using automated scanning tools integrated with MDE.
Assess	Analyze vulnerabilities with real-time exposure scoring and prioritize based on exploitability, severity, and business impact.
Remediate	Analyze vulnerabilities with real-time exposure scoring and prioritize based on exploitability, severity, and business impact.
Validate and Report	Validate remediation success through scans and provide analytics dashboards for compliance, audit, and continuous improvement.

Step-By-Step Implementation Guide

Onboarding Endpoints	Begin by onboarding endpoints and servers into the security platform for centralized vulnerability data collection.
Dashboard Enablement	Enable the vulnerability management dashboard to gain real-time visibility into vulnerabilities and exposures.
Policy Configuration	Configure vulnerability baselines and security policies to meet compliance and industry standards.
Patch Management Integration	Integrate patch management workflows using tools like Intune or SCCM for automated updates and fixes.
Automated Vulnerability Assessment	Use AI-driven threat intelligence to automate vulnerability prioritization and remediation efforts.
Reporting and Compliance	Generate detailed compliance reports and review security posture using built-in dashboards.
Continuous Tuning	Continuously refine policies and workflows using risk insights and analytics to adapt to threats.

Duration | Pricing

Duration: (in days / weeks):	***Price:***	***Industries Served:***
4–8 weeks (Assessment + Implementation); BAU ongoing	$5000	Manufacturing | Healthcare | BFSI | Retail | Automotive | Energy & Utilities

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