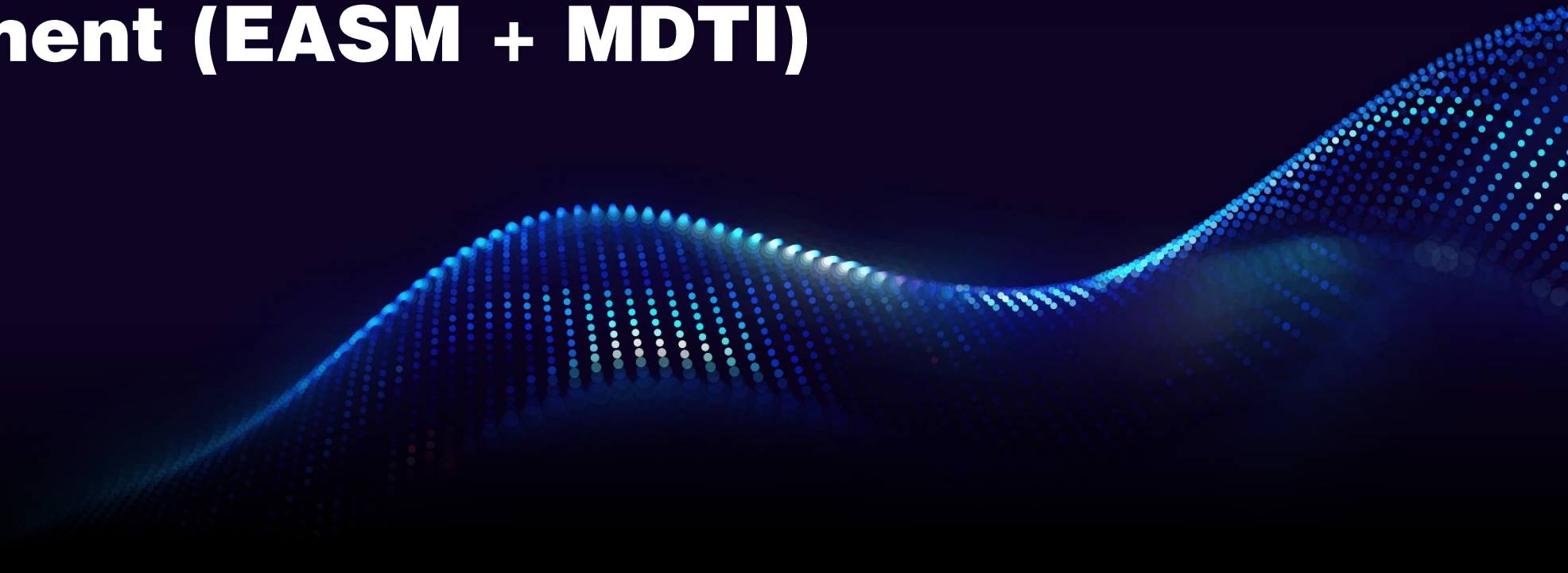


# **Cloud4C External Attack Surface Assessment (EASM + MDTI)**



# Cloud4C External Attack Surface Assessment Offering



Microsoft Defender EASM (Asset  
Discovery & Assessment)

Microsoft Defender Threat Intelligence  
(MDTI)

Shadow IT & Misconfiguration  
Discovery

CVE & Vulnerability Correlation

Risk Dashboards & Prioritized  
Findings

Advisory-Led Remediation Plans

## Proven Business Outcomes with Cloud4C

- 30–40% reduction in external attack surface exposure within one quarter
- 100% inventory coverage of internet-facing assets, including shadow IT
- Faster remediation cycles with prioritized, intelligence-backed actions
- Improved audit readiness with ISO 27001, HIPAA, PCI-DSS, and GDPR mapping
- Executive-ready dashboards for board-level risk visibility
- Enterprise-proven deployments across BFSI, healthcare, telecom, government, and retail

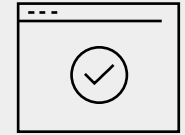


# Cloud4C External Attack Surface Assessment Methodology

- Set up Microsoft Defender EASM + MDTI for asset inventory
- Discover unmanaged, internet-facing, and shadow IT resources
- Establish baseline visibility and risk map



- Provide risk dashboards with CVEs, open ports, and misconfigurations
- Validate findings with threat intelligence and compliance frameworks
- Prepare executive-ready reports with actionable insights



## Onboarding & Asset Discovery



## Risk Assessment & Correlation

- Identify CVEs, misconfigurations, and exposed services
- Correlate vulnerabilities with MDTI intelligence for prioritization
- Deliver detailed exposure mapping for business impact

## Dashboard Delivery & Validation



## Remediation & Continuous Advisory

- Deliver prioritized remediation roadmap with quick wins
- Advisory-led recommendations for compliance and resilience
- Optional continuous monitoring and managed attack surface reduction



# Why Cloud4C for External Attack Surface Assessment?

