

Cloud4C's MDR for Microsoft Defender for Endpoint Offering

Cloud4C Competencies on Azure





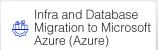
Renewed

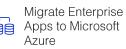


14 Advanced Specializations











Identity & Access Mgmt.





Microsoft Azure VMware Solution (Azure)





SAP on Microsoft Azure (Azure)



Cloud Security (Security)

Microsoft Azure Virtual Desktop (Azure)



Threat Protection (Security)





Build Al Apps on Microsoft Azure

Advanced Specializations Future roadmap - 2025

- · Hybrid Cloud Infrastructure with Microsoft Azure Stack HCI
- Data Warehouse Migration to Microsoft Azure

Solution Partner

- Solutions Partner for Infrastructure (Azure)
- Solutions Partner for Data & AI (Azure
- Solutions Partner for Modern Work
- Solutions Partner for Digital & App Innovation
- Solutions Partner for Security





Partner of the Year, UAE 2022, Qatar 2020



Rising Star of the Year, APAC 2021



Security Partner of the Year (Malaysia 2023)



Finalist - Endpoint Management Trailblazer (MISA 2025)

Cloud4C MDR for Microsoft Defender for Endpoint Offering



24x7 Endpoint Monitoring & Response

Al-Powered Threat Detection & Automated Recovery

Proactive Threat Hunting & Advanced Analytics

Unified Device Protection

Compliance-Ready with Dashboards & Audit Logs

Global + Local SOC Expertise with Regional Threat Intel

Proven Business Outcomes with Cloud4C

- Up to 55% faster response to endpoint incidents
- False positives reduced to ≤10% with Al-driven detection
- 100% compliance alignment to NIST, ISO 27001, HIPAA, PCI-DSS, GDPR
- Minimized endpoint downtime through automated recovery
- 3-week rapid deployment ensuring faster endpoint protection
- 24x7 SOC-backed protection with localized expertise
- Quarterly reviews for continuous endpoint resilience
- Proven wins across BFSI, healthcare, manufacturing, government



Cloud4C's MDR for Microsoft Defender for Endpoint Managed Detection & Response Methodology

- Review endpoint security posture and compliance
- Industry-specific device playbooks and workflows
- Data residency and sovereign cloud compliance
- Regulatory gap analysis and threat intelligence baseline

Endpoint Posture Assessment & Baseline





- Rapid Deployment & Integration
- 3-week rollout with seamless Azure & Microsoft 365 onboarding
- Integration with Microsoft Defender for Endpoint
- Al-driven automated detection and remediation playbooks
- Setup of global and regional SOC monitoring

- 24x7 Al-enabled endpoint risk detection and alerts
- Automated incident summaries and guided SOC analyst actions
- Real-time threat hunting and behavior analytics
- Continuous integration of global and regional threat intelligence



AI-Powered Endpoint Detection & Response



- Reporting, Optimization & Resilience
- Quarterly endpoint health checks and detailed reporting
- Executive insights and remediation validation
- Detection tuning to reduce false positives/negatives
- Compliance audit readiness and resilience metrics





Why Cloud4C for Microsoft Defender?

End-to-End Endpoint Protection



Comprehensive coverage across desktops, laptops, and mobile devices in hybrid environments

Automation-First Recovery



Proprietary playbooks ensure rapid remediation, minimizing downtime and disruption

24x7 Global + Local SOCs



Continuous monitoring and response with regional intelligence for compliance-critical markets





Compliance-Ready by Design

Built-in mapping to NIST, ISO 27001, HIPAA, PCI-DSS, GDPR



Industry-Specific Accelerators

Prebuilt baselines and controls tailored for BFSI, healthcare, manufacturing, and more



Sovereign & Data Residency Expertise

Endpoint deployments aligned with incountry regulations and Microsoft Sovereign Cloud requirements

