

Microsoft Security Experts Managed Services

| Category | Capability | Microsoft Management Experts | Microsoft Defender Experts | | Microsoft Security Services |
|---------------|--|---|---|---|--|
| | | Microsoft Managed Desktop | Microsoft Defender Experts for Hunting | Microsoft Defender Experts for XDR | Microsoft Security Services for Enterprise |
| Availability | Is this service generally available? | GA – Available | GA – August 2022 | Public Preview Fall 2022 GA – Fall 2023 | Public Pilot – May 2022 Solution GA – Fall 2022 |
| Security Tech | What environments are covered? | Windows Endpoints (including W365 or Azure Cloud PCs) | Endpoint, Microsoft 365, Cloud Apps, Identity | Endpoint, Microsoft 365, Cloud Apps, Identity | Multi-cloud, Cloud Apps, Azure Sentinel, Endpoint, Identity, Microsoft 365 |
| Discover | Architecture and Operations Review | | | | |
| | Threat Activity Assessment | | | | |
| Onboard | Onboarding | | | | |
| | Baseline Configuration | | | | |
| | Service Delivery Manager | | | | |
| Manage | Managed Detection (Management of Defender Incident queue) | | | | |
| | Managed Extended Detection (Multi-cloud and Azure Sentinel) | | | | |
| | Threat hunting and analysis | | | | |
| | Targeted attack notifications (TAN) from M365 Defender | | | | |
| | Hunter-trained AI | | | | |
| | Microsoft Azure Sentinel Automation | | | | |
| | Cross Cloud Protection (AWS, GCP etc.) | | | | |
| Respond | Incident Response (IR) (Includes O365 IR) | | | (1 week IR) | (2 weeks IR) |
| | Compromise Recovery (Includes Rapid Ransomware Rec) | | | | |
| | Experts on demand (guidance & Insights) | | | | |
| | Managed Response | | | | |
| | Tier 1 Support – Rapid Remediation and Escalation | | | | |
| | Tier 2 Support - Advanced Analysis and Remediation | | | | |
| | Tier 3 Support - Proactive Hunting and Advanced Forensics and Detection Tuning | | | | |
| Evolve | Dedicated Advisory Consultant | | | | |
| | Reports | | | | |