Service Comparison

Service Category	Service Component	Activity	Managed SIEM	Managed EDR	MDR
Azure Sentinel	SIEM Platform	Deployment and Configuration	•	•	•
		Operational Monitoring	•	•	•
		Management, Optimization, and Troubleshooting	•	•	•
	SIEM Agent	Deployment and Patching Support	•	•	•
Detection Engineering	General Use Cases	Development and Maintenance	•		•
	EDR Use Cases	Development and Maintenance		•	•
	Custom Use Cases	Development and Maintenance	Available	Available	Available
Defender for Endpoint	EDR Platform	Deployment and Configuration		•	•
		Operational Monitoring		•	•
		Management, Optimization, and Troubleshooting		•	•
	EDR Agent	Deployment and Patching Support		•	•
SOC Services	Threat Hunting	Proactive Threat Hunting	•	•	•
	Threat Management	Triage and Investigation	•	•	•
		Case Management	•	•	•
		File Retrieval and Analysis		•	•
	Threat Response	Endpoint Isolation		•	•
		AD User Disable			•
		Other Response Action(s)			•