MXDR for SMB – Microsoft Defender XDR

Microsoft Defender XDR: Threat Detection & Investigation	MXDR for SMB
Identify, threat hunt and report suspicious activity across identity, email, cloud apps, and endpoints.	✓
Leverage advanced hunting queries across identity, endpoint, and cloud apps to proactively identify threats before they escalate.	✓
Threat correlation between identity and device-based attacks for faster detection and response.	✓
Microsoft Defender for Office 365: Email and Collaboration Security Monitoring	
Monitor for phishing, malware, and spam threats through Defender for Office 365.	✓
Review alerts related to Safe Links, Safe Attachments, and email anti-phishing mechanisms.	✓
Removal of malicious emails from inboxes and block suspicious links or files.	✓
Microsoft Defender for Endpoint: Security Monitoring	
Monitoring of devices for malware and triage alerts related to suspicious activities on endpoints such as malicious file downloads or execution.	✓
Detect and investigate file-based threats, network anomalies, suspicious user behavior, and lateral movement across endpoints.	✓
Analyze telemetry to identify indicators of compromise (IOCs) & advanced persistent threats (APT).	✓
Antivirus scans, threat removal, and remediation actions such as file quarantining and blocking malicious processes.	✓
Playbooks to respond to common endpoint threats, including isolating devices, running antivirus scans, and quarantining malicious files with full device isolation capabilities to contain threats.	✓
Utilize live response capabilities to remotely execute commands on devices for investigation or threat containment	✓
Microsoft Defender for Identity & Identity Protection	
Continuous monitoring for identity-based threats using Entra Identity Protection and Defender for Identity. Provide an analysis of incidents, with guidance on improving identity protection measures.	✓
Detect and alert on identity-based threats such as brute-force attacks, compromised accounts, lateral movement, and unusual sign-in behavior.	✓
Confirm & Dismiss Risk user sign-in	✓
Response actions, such as user account lockdown, MFA enforcement, or password resets.	✓
Microsoft Defender for Cloud Applications	
Monitor and alert on cloud app usage with Microsoft Defender for Cloud Apps for suspicious behavior and risky app usage.	✓
Detect and remediate risky activities within SaaS apps, such as abnormal download volumes or unusual data-sharing behavior.	✓
Revocation of risky app access tokens in response to detected threats.	✓
Incident Response	
Customer Self-Managed Incident Response. Manual intervention from the customer's IT or SOC teams for response actions (e.g., isolating a device, blocking attachments).	✓
Configuring Auto Investigation, Auto Remediation, and Auto Disruption in Defender XDR	✓
Populating Allow/Block Lists	✓
Playbooks for KMicro SOC Analysts to respond with human oversight to common endpoint threats, including isolating devices, running antivirus scans, account logout, and quarantining malicious files.	✓
Utilize live response capabilities to remotely execute commands on devices for investigation or threat containment.	✓
Professional & Advisory Services	
Microsoft 365 Security Engineer as a Service	Available