CRITICALSTART® Managed Detection and Response
Service Comparison for Microsoft Products

	Microsoft 365 Defender	Microsoft Defender for Endpoint	Microsoft Sentinel
Automatically resolve false positives at scale with the Critical Start Trusted Behavior Registry™	●	●	●
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts regardless of severity level	●	●	●
ZTAP dashboard provides complete and aggregated visibility into every alert with full details on the investigation and each action taken	●	●	●
Curate the new and updated detections being released daily by Microsoft	●	●	●
Management, curation, and maintenance of out-of-the-box detections and IOCs released by Microsoft	●	●	●
Curation of original and third- party threat intelligence, combined with real-time threat analysis to create a high-fidelity, actionable view of existing and emerging threats	●	●	●
Continuous development and enrichment of new threat detections and Indicators of Compromise (IOCs) based on the latest evolving security landscape	●	●	●
Threat detection content mapped to MITRE ATT&CK® Framework	●	●	●
Disable and logout of all signed in sessions for compromised accounts	●	●	●
ZTAP supports organizations with multiple tenants using parent/child hierarchy	●	●	●
Granular-level audit capabilities	●	●	●
Enhanced and optimized API ingestion	●	●	●

Service Specific Capabilities	Microsoft 365 Defender	Microsoft Defender for Endpoint	Microsoft Sentinel
Investigate, remediate, and resolve alerts for Microsoft Defender for Identity	●	N/A	N/A
Investigate, remediate, and resolve alerts for Azure Active Directory Identity Protection	●		
Investigate, remediate, and resolve alerts for Microsoft Defender for Office 365	●		
Investigate, remediate, and resolve alerts for Microsoft Defender for Cloud Apps	●		
Investigate and respond to suspicious email reported by users	●		
Optional capability to send an email to the user informing them of the outcome of the investigation of their reported emails, positive or negative	●		
Notification templates used to provide investigation results of reported email are customizable	●		
Delete phishing email from all inboxes	●		
Investigate, remediate, and resolve alerts for Microsoft Defender for Endpoint	●	●	
Remediation actions directly from ZTAP and MOBILE**SOC**® app	●	●	
Maintain block and allow lists for file hashes, processes, IP addresses	●	●	
Investigate and monitor multi-source security events (Active Directory, Windows, Linux, Applications, Firewalls)			●

criticalstart.com

© 2022 CRITICAL**START**. All rights reserved.