DATASHEET

CRITICAL**START**® Managed Detection & Response Services for Microsoft 365 Defender

KEY BENEFITS

- ✓ Maximize the value of M365D
- ✓ Consolidate & improve visibility across M365D in one portal
- ✓ Prevent breaches through the disruption of attacks across the kill chain
- ✓ Improve overall SOC efficiency and productivity

Detect and disrupt attacks beyond the endpoint.

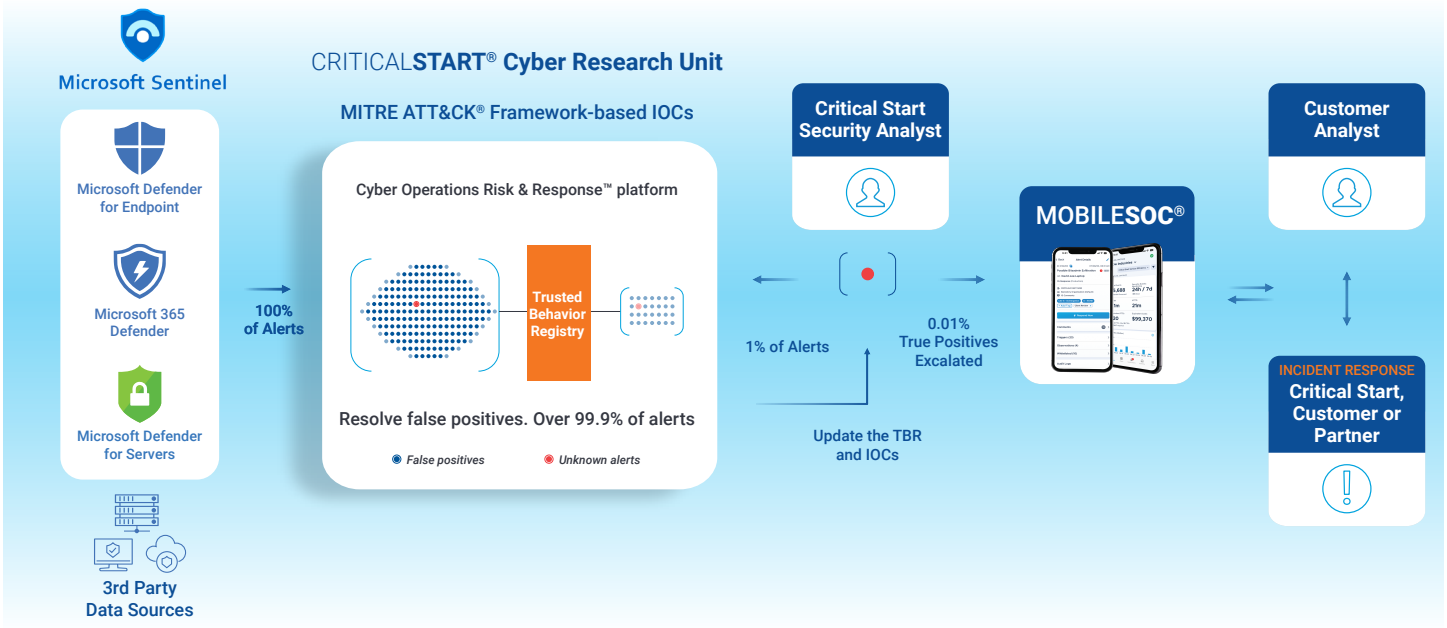
Make no mistake, the volume and severity of cyberattacks are increasing through multiple cyber-attack vectors such as compromised credentials, email phishing, and Cloud application-based risks. And security teams are missing the attacks sliding through these openings. Unfortunately, most organizations experience these types of attacks, regardless of size and level of security maturity.

The Solution

Get the most out of your Microsoft 365 Defender (**M365D**) solution with Critical Start's risk-based approach to Managed Detection and Response (**MDR**). Our team of Microsoft security experts leverages our integration with M365D to extend your security defenses for cross-domain threat detection and protection. Our 24x7x365 Risk & Security Operations Center (**RSOC**) analysts detect, investigate, and offer guided response to non-endpoint alerts from identity to email and cloud—before they disrupt business operations.

How It Works

Our **Cyber Operations Risk and Response™ platform** automates the investigation and triage of alerts, while our purpose-built Trusted Behavior Registry® removes false positives and escalates true positives to our RSOC for further enrichment and investigation. Throughout the service, we make continuous recommendations on additional data sources and update detection content to uncover more attacks.



CRITICALSTART®

How We Do It

Critical Start MDR for Microsoft 365 Defender combines our exclusive technology—the **Cyber Operations Risk & Response™ platform**, our Risk and Security Operations Center (**RSOC**) and the elite experts in the Critical Start Cyber Research Unit—to maximize cross-domain detection, investigation, and remediation.

M365D Optimization
Through continuous improvement and policy recommendation, we can improve detections and refine as new threats and identified.

Automated Investigation & Triage
Our platform automates the investigation and triage of alerts from M365D, removing false positives and escalating true positives to the Critical Start RSOC for further enrichment and investigation.

24x7x365 Coverage
Highly skilled threat analysts, researchers, and responders investigate threats occurring within your organization and across the rapidly expanding threat landscape. Microsoft Certified Analysts utilize proven methodologies leveraging threat intelligence and key sources to gather context to ensure the efficacy of detection. Advanced playbooks and response actions provide necessary mitigation, remediation, or containment actions to protect your organization 24x7x365.

Disrupt Attacks
We go beyond response recommendations to provide proactive response actions across the kill chain to disrupt attacks, such as disabling a user's Microsoft Entra ID (formerly AAD) Account, blocking new sign-ins and deleting phishing emails from a user's inbox.

Timely & Actionable Threat Intel
Within the Critical Start Cyber Research Unit is a dedicated Cyber Threat Intelligence team that conducts research and reports on new threats and suspicious Tactics, Techniques and Procedures (**TTPs**) requiring action by Critical Start and you. This information is fed into our Threat Detection Engineering team to develop new detections for M365D.

IOC Management & Expert Threat Detection Content
Critical Start monitors for new threats and curates new Indicators of Compromise (**IOCs**) to continuously improve Microsoft 365 Defender detections.

MITRE ATT&CK Mapping
Threat detection content is mapped to the **MITRE ATT&CK® Framework** to to ensure your visibility to coverage against the latest attacker TTPs.

Mobile Application
Our MOBILE**SOC®** application (iOS and Android) puts the power of the our platform in your hands, giving you the ability to triage, escalate, and isolate cross-domain attacks from your phone.