DATASHEET

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

KEY BENEFITS

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

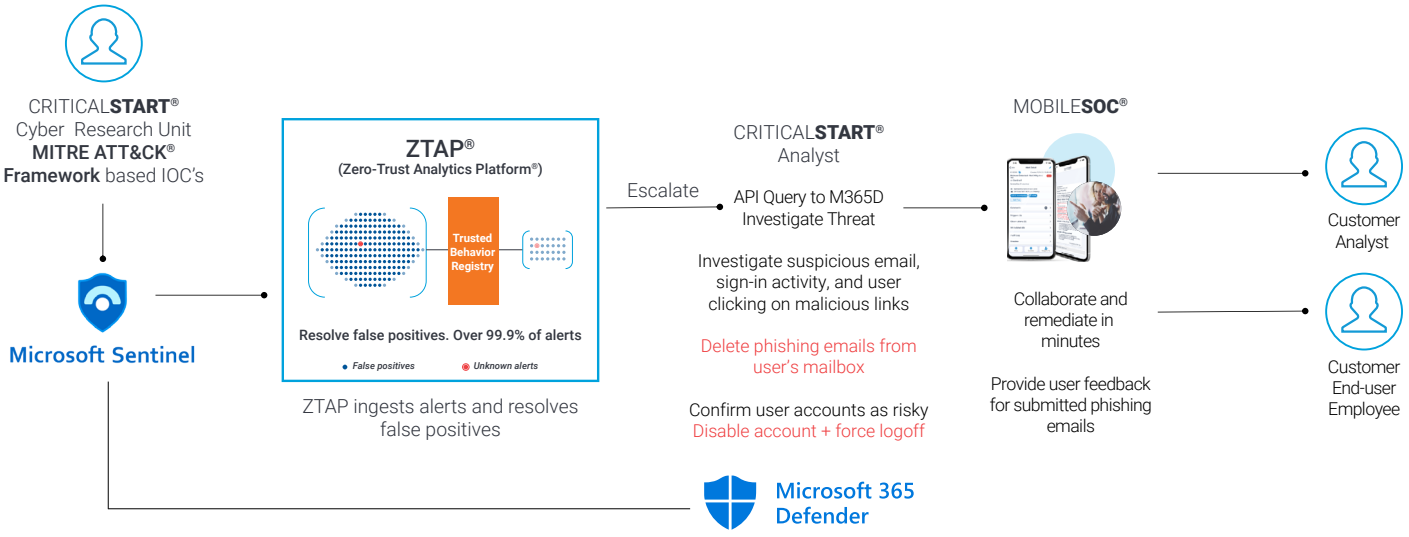
Detect and disrupt attacks beyond the endpoint.

Make no mistake, the volume and severity of cyberattacks is increasing through multiple cyber-attack vectors such as compromised credentials, email phishing and cloud misconfiguration. 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

Critical Start Managed Detection and Response (**MDR**) services for Microsoft 365 Defender (**M365D**) extend your security defenses to provide cross-domain threat protection and simplify breach prevention. Our team of Microsoft security experts leverage our integration with M365D to detect, investigate and respond with the right actions to non-endpoint alerts from identity, to email and cloud – before they disrupt business operations.

MDR for M365D



CRITICALSTART®

How We Do It

Prioritizing data ingested into SIEM

Critical Start MDR for Microsoft 365 Defender combines our exclusive technology – the Zero-Trust Analytics Platform® (**ZTAP®**), our Security Operations Center (**SOC**) and the elite experts in the Critical Start Cyber Research Unit - to maximize cross-domain detection, investigation, and remediation.

M365D Optimization

We configure M365D to your environment, define detection and prevention policies and continuously fine-tune your deployment as new risks are identified.

Automated Investigation & Triage

ZTAP automates the investigation and triage of alerts from M365D, removing false positives and escalating true positives to the Critical Start SOC for further enrichment and investigation.

24x7x365 Coverage

Highly skilled Microsoft certified analysts quickly investigate escalated alerts and help you make more accurate decisions on which response action to take through 24x7x365 monitoring, rapid investigation and continuous threat hunting.

Disrupt Attacks

We go beyond response recommendations with our multiple response actions designed to disrupt attacks across the kill chain like disabling a user's Azure Active Directory Account, blocking new sign-ins and deleting phishing emails from a user's inbox.

Timely & Actionable Threat Intel

The Cyber Threat Intelligence team that sits within in the Critical Start Cyber Research Unit, 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

Leveraging the CRITICALSTART® Threat Navigator, we manage, maintain and curate M365D out-of-box detections and Indicators of Compromise (IOCs).

MITRE ATT&CK Mapping

Threat detection content is mapped to the MITRE ATT&CK® Framework to ensure you are protected from the latest attacker TTPs.

Mobile Application

Our MOBILESOC® application (iOS and Android) puts the power of the ZTAP platform in your hands, giving you the ability to triage, escalate and isolate cross-domain attacks from your phone.

Member of
Microsoft Intelligent Security Association

Microsoft

Contact Us **Request a Free Assessment**

CRITICALSTART®