DATASHEET

CRITICALSTART® Managed Detection and Response Services for Microsoft Defender for Endpoint

KEY BENEFITS

- ✓ Team expansion with Microsoft Security expertise
- ✓ Every endpoint alert investigated
- ✓ Guaranteed 1-hour SLA for TTD and MTTR
- ✓ Personalized playbooks and SOC operations
- ✓ 100% visibility consolidated in one portal
- ✓ Containment of infected devices
- ✓ Tool configuration and tuning
- ✓ Triage and contain alerts anytime, from anywhere with MOBILESOC®

At CRITICALSTART®, our managed detection and response (MDR) service is all about simplifying your security. We built our MDR service for Microsoft Defender for Endpoint to go beyond monitoring alerts to helping customers see attacks across hybrid device types and operating systems to reduce risk exposure, eliminate alert fatigue, and optimize security operations center (SOC) efficiency.

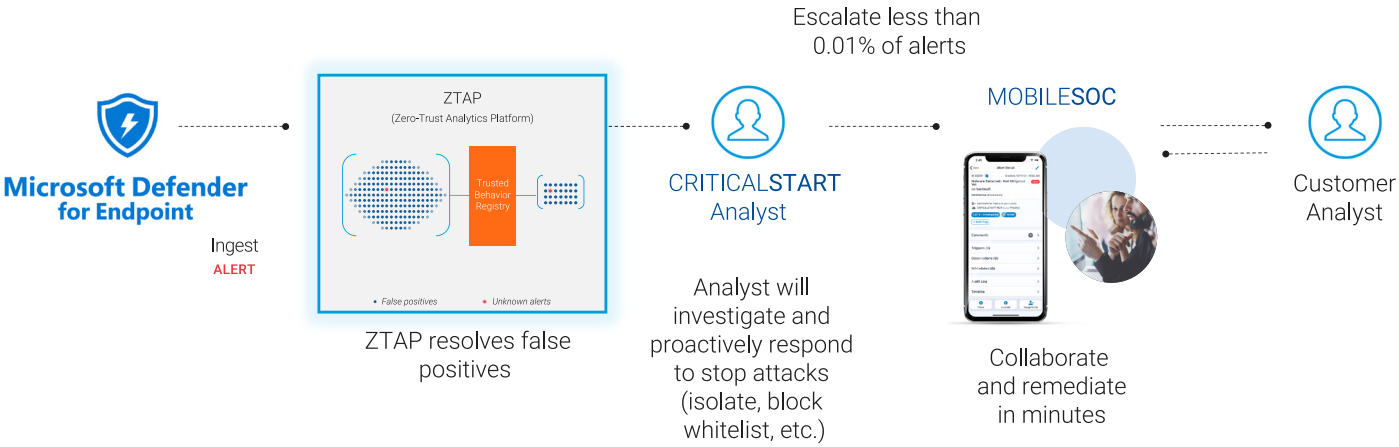
We detect the right threats and respond with the right actions

CRITICALSTART does this by ingesting every alert from Microsoft Defender for Endpoint (MDE) into the Zero Trust Analytics Platform™ (ZTAP™), the backbone of our MDR service. We compare alerts against known good behaviors in the Trusted Behavior Registry™ (TBR) where playbooks auto-resolve known good alerts. Alerts not identified by the TBR are escalated for investigation to the CRITICALSTART Security Operations Center (SOC) where our human-led services help you make more accurate decisions on which response action to take.

How we do it

Resolving alerts is good. Resolving all alerts is better.

- ✓ Trust oriented approach leverages the power of ZTAP and TBR to address all alerts
- ✓ We resolve more than 99.9% of alerts across Microsoft Security resources
- ✓ We escalate less than 0.01% of alerts – the alerts that really require the attention of your security team



CRITICALSTART®

CRITICAL**START MDR services for Microsoft Defender for Endpoint leverage:**

- ✓ Cross-operating system (Windows, Mac, Linux) Indicators of Compromise (IOCs)
- ✓ Azure Active Directory as an identity provider, single sign-on, and user provisioning management
- ✓ Microsoft automated alerts and actionable incidents
- ✓ Cross-signal context in device timeline investigations
- ✓ Ability to pivot directly to the device timeline from any generated IOC

Elite SOC capabilities, at your side, at your service.

Whether you are looking to expand the capacity of your SOC, optimize the efficiency of your tools or both, our highly proficient team of Microsoft security experts stand ready to extend the detection and response capabilities of your cyber security operations 24x7x365 through real-time monitoring, rapid investigation, and proactive response to endpoint alerts, with full-scale, complete alert resolution.

Our security experts:

- ✓ Have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Security Technologies certifications
- ✓ Use Microsoft Security Best Practices to deploy Microsoft Defender for Endpoint

So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service for MDE is IOC management. Microsoft is the fastest-moving security company today. IOCs are published and updated hourly across various locations. Leveraging the CRITICAL**START**® Threat Navigator, we manage, maintain, and curate MDE out-of-box detections and IOCs. Threat detection content is also mapped to the industry leading, MITRE ATT&CK® framework.

Never miss a threat. Or your desk with MOBILE**SOC**.

Take threat detection and response on-the-go with our MOBILE**SOC** application, an iOS and Android app that puts the power of the ZTAP platform in your hands, giving you the ability to triage, escalate and isolate attacks from your phone. With MOBILE**SOC**, you're able to see the full alert data, can communicate directly with senior SOC security analysts and can take immediate action with information gathered by tools and in coordination with your MDR team.

Contact Us **Request a Free Assessment**

CRITICALSTART®