SOLUTION BRIEF

CRITICAL**START** Managed Detection and Response Services for Microsoft Defender for Endpoint

Visible threat detection and response for the modern enterprise that's more than good, *it's better.*

KEY BENEFITS

- Extend your team with threat detection and response expertise
- Leverage complete visibility and just-in-time information
- Consolidate automation containment and recovery playbooks
- Accelerate value from Microsoft Defender for Endpoint
- Triage and contain alerts from anywhere with MOBILE**SOC**

We do what others don't. CRITICAL**START** built an MDR service with Microsoft Defender for Endpoint that goes beyond monitoring alerts to helping customers see attacks across hybrid device types and operating systems, investigate the context, and remediate the true positives. **No one has time to waste.**

Why CRITICAL**START**

Resolving alerts is good. Resolving all alerts is better.

- ✓ Trust oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We resolve more than 99% of alerts
- ✓ We escalate less than 0.01% of alerts – the alerts that really require the attention of your security team

Integration, the better way.

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

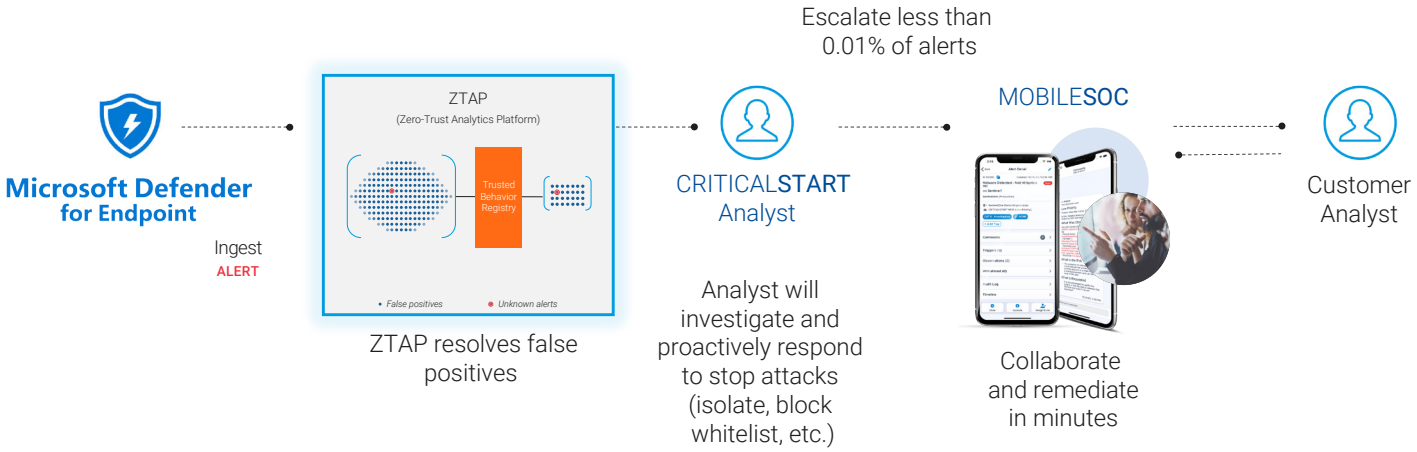
- ✓ Cross-operating system (Windows, Mac, Linux) Indicators of Compromise (IOCs)
- ✓ Azure Active Directory as an identity provider, single-sign on and user provisioning management
- ✓ Microsoft automated alerts and actionable incidents
- ✓ Cross-signal context in device timeline investigations
- ✓ Ability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

Not more resources. Better ones.

- ✓ Security analysts have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications
- ✓ Microsoft Security Best Practices are used to deploy Microsoft Defender for Endpoint to optimize Microsoft content for both Scheduled Query Rules and Indicators of Compromise (IOCs)
- ✓ 24x7x365 end-to-end monitoring, investigation, and response by highly skilled analysts

How we do it

We take every alert from Microsoft Defender for Endpoint into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates and proactively responds to stop the attack on your behalf. Our analysts then collaborate with you to remediate in minutes.



Automated security + control. *Now, that's better.*

Microsoft Defender for Endpoint is built on deep insights into operating system threats and shared signals across devices, identities, and information. Leveraging Microsoft automated alerts and actionable incidents, focus time on what really needs security expertise—deciding what to prioritize next on your Microsoft Roadmap. Leave the research, false positives, and containment of infected devices to Microsoft and CRITICAL**START**.

Wave goodbye to portal fatigue.

A comprehensive integration means you can speed up investigation and response with access to Microsoft Azure Sentinel or Microsoft 365 Defender, get Entities, get Secure Score, Sign-In Details, and related alerts – all in one portal. For each type of data source like email, identity, and endpoint, we have built queries within the platform for you to fetch other information for additional context – all within one portal.

Within the ZTAP platform, you can speed up investigation and response with the ability to pivot between the Defender 365 and Defender for Endpoint consoles – in one portal.

CRITICALSTART
They're good. We're better.

So long, tedious IOC Management. Hello optimized rules.

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

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILE**SOC** application. An industry-leading first, MOBILE**SOC** puts the power of our ZTAP platform in your hands, allowing you to contain breaches right from your phone. Our iOS and Android app features 100% transparency, with full alert detail and a timeline of all actions taken.

CRITICAL**START**
They're good. We're better.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICAL**START** MDR + Microsoft Defender for Endpoint	Other MDR/ Managed SIEM providers
24x7x365 monitoring, investigation, and response by security analysts	●	●
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts, regardless of priority level	●	✕
Native iOS and Android applications for alert investigation, collaboration, and response	●	✕
Customer and vendor work from the same platform and see the same information	●	◐
Custom Indicator of Attack (IOA) Monitoring	●	✕
Two-person integrity review process that provides quality control of SOC orchestration for every customer	●	✕
Detection content mapped to the MITRE ATT&CK™ framework	●	◐
Manage and maintain cross-ecosystem Indicators of Compromise (IOCs)	●	✕
Continuous threat hunting	●	◐
Perform configuration, deployment, and health checks without requiring additional professional services	●	●
Alert notifications that include both security event data and expert analysis	●	◐
Analyst will proactively respond to stop attacks (isolate, block whitelist, etc.)	●	●
Managed response, policy tuning, and updating of agents	●	●
Investigate all operating systems without added agent deployment	●	✕
IOCs for Windows, Mac, and Linux	●	✕
Investigate trust levels of every device	●	✕
PowerShell Live Response library	●	✕
Granular guest user auditing	●	✕
Multi-Tenant so customer can have multiple organizations with N-level hierarchy	●	✕
Manage and report on all alerts from SIEM and EDR in one platform	●	✕

Member of
Microsoft Intelligent Security Association

Microsoft

Gold
Microsoft Partner

Microsoft

Goodbye, alert fatigue. Hello, CRITICALSTART**.**

Contact Us

Request a Free Assessment

CRITICALSTART
They're good. We're better.