SOLUTION BRIEF

CRITICAL**START** Managed Detection and Response Services for Microsoft 365 Defender

KEY BENEFITS

- Comprehensive threat detection and response coverage for Microsoft 365 Defender
- Speed up investigation and response in one portal
- Reduce attacker dwell time
- Reduce risk acceptance
- Accelerate value from Microsoft 365 Defender
- Triage and contain alerts from anywhere with MOBILE**SOC**™

MDR reimagined. XDR reinvented. An integrated threat detection and response solution for the modern world that's more than good, *it's better.*

We do what others don't. Microsoft has built a best-in-class security portfolio to stop attacks across Microsoft 365 services. CRITICAL**START**™ Managed Detection & Response (MDR) services for Microsoft 365 Defender quickly detect every event, resolve every alert, and respond to breaches across all your resources.

Why CRITICAL**START**

Resolving alerts is good. Resolving all alerts is better.

- ✓ Our trust-oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We auto-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.

MDR services for Microsoft 365 Defender leverage:

- ✓ Microsoft Azure Sentinel for ingestion of alerts across your enterprise, automated investigations, and actionable incidents
- ✓ Microsoft User and Entity Behavior Analytics (UEBA) which increases the likelihood of detecting a true positive at multiple parts of the kill chain
- ✓ Azure Active Directory as an identity provider, single-sign on and user provisioning management

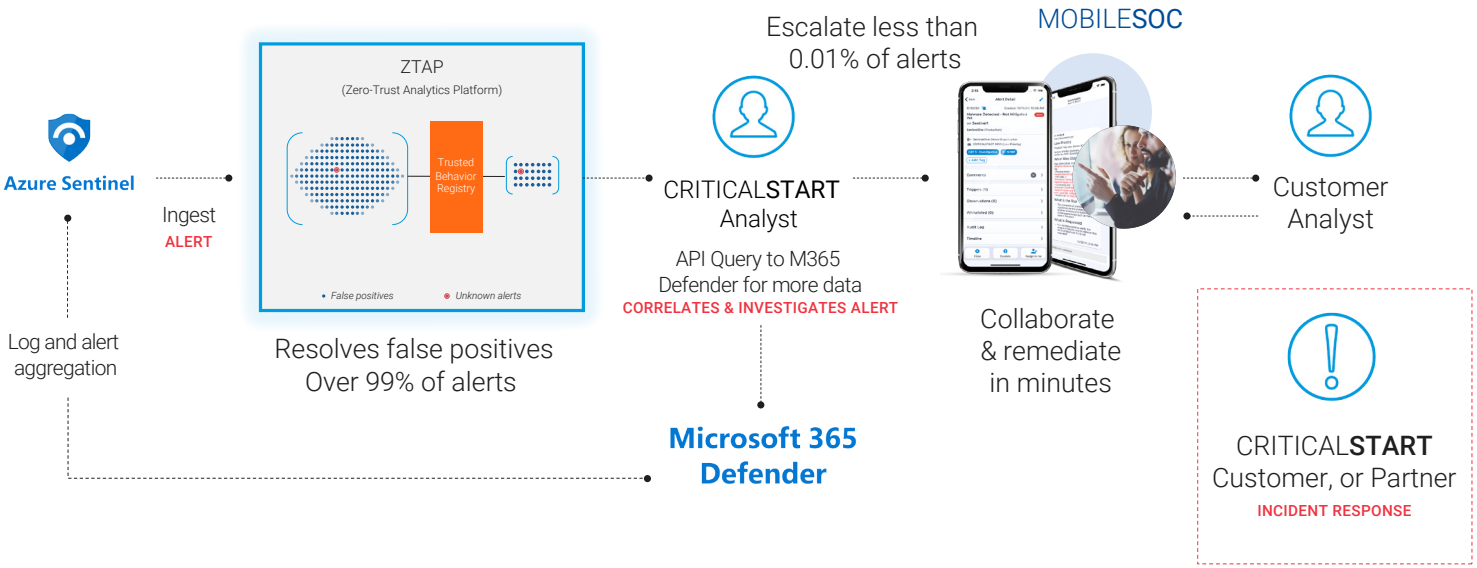
Not more resources. Better ones.

- ✓ Security analysts have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications
- ✓ We use Microsoft Security Best Practices to deploy Azure Sentinel and Microsoft 365 Defender tools to optimize Microsoft content for both Scheduled Query Rules and Indicators of Compromise (IOCs)
- ✓ Our team provides 24x7x365 end-to-end monitoring, investigation, and response by highly skilled analysts
- ✓ Threat detection content management, provided by the CRITICAL**START**™ Cyber Research Unit, leverages the CRITICAL**START**™ Threat Navigator to manage the hundreds of new detections being released daily by Microsoft.

How we do it

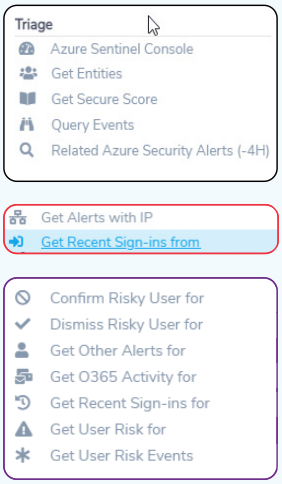
We take every alert from the Microsoft 365 Defender security suite into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates and collaborates with you to remediate the alert.

USE CASE EXAMPLE: IDENTITY-BASED ALERT – IMPOSSIBLE TRAVEL



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 built-in queries by alert/ source type. In this example, these are some of the available queries for investigating users across Microsoft 365 Defender.

CRITICALSTART
They're good. We're better.

Automated investigations. Exceptional response.

ZTAP enriches every alert with additional metadata from the Microsoft environment. Leveraging Microsoft automated investigations and actionable incidents, our MDR service modulates and adapts for identity, checks for behaviors that are trusted, and escalates risky sign-ins, logons from unfamiliar IPs, and impossible travel violations for validation with enriched data. If a user is deemed not risky, CRITICALSTART can dismiss the user's risk, allowing them access again.

So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service for Microsoft 365 Defender is IOC management. Microsoft is the fastest-moving security company today. IOCs are published and updated hourly across different locations. Leveraging the CRITICALSTART Threat Navigator, we manage, maintain and curate Microsoft 365 Defender out-of-the-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 MOBILESOC application. An industry-leading first, MOBILESOC 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.

CRITICALSTART
They're good. We're better.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICAL**START** MDR + Microsoft 365 Defender	Other MDR 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 for security event analysis	●	◐
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	●	◐
Leverage multiple Microsoft security tools for response	●	●
Perform configuration, deployment, and health checks without requiring additional professional services	●	●
Alert notifications that include both security event data and expert analysis	●	◐
Leverage Microsoft user-based detections	●	●
Automatically enable new Microsoft rules	●	✕
Investigate every user	●	✕
Use cross-Microsoft correlations in investigations	●	●
Perform cross- and multi-tenant management without requiring Azure Lighthouse	●	✕
Enable one-click enterprise enrollment consent	●	✕

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.