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

Microsoft Defender for Endpoint

With an attack surface that is constantly changing, where access roles are dynamic, and devices and applications request and keep more data, endpoint security tool signals alone are not enough. Gaps spread, as does your risk. CRITICAL**START** Managed Detection & Response (MDR) services with Microsoft Defender for Endpoint combine Microsoft's cross-enterprise visibility threat detection and auto investigation capabilities with radical alert reduction.

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

What sets us apart?

We do what others don't. Microsoft Defender for Endpoint provides a complete endpoint security solution with unparalleled optics and a new level of automated security. It's not only good, but ***better*** to combine that with CRITICAL**START** MDR services built on the premise that ***acceptable risk shouldn't be.***

How we do it.

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.***

Integration, the better way.

Unlike other managed detection and response services, CRITICAL**START** MDR services with Microsoft Defender for Endpoint leverage:

- ✓ Cross-operating system *(Windows, Mac, Linux)* Indicators of Compromise (IOC)
- ✓ Azure Active Directory as an identity provider, single sign-on, and privileged access management for Security Operations Center (SOC) access
- ✓ Cross-signal context in device timeline investigations
- ✓ Ability to pivot directly to the device timeline from any generated IOC

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**.

Acceptable risk shouldn't be.

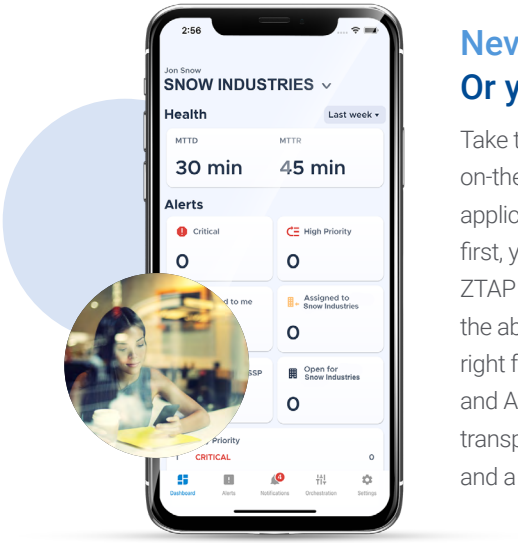
Our unique trust-oriented model is based on resolving every alert. CRITICAL**START** MDR is driven by the Zero Trust Analytics Platform (ZTAP). The platform features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives), delivering the scalability to resolve every alert.

We take every alert from your security tools into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates the alert.

Not more resources. Better ones.

Better is understanding Microsoft Security products and solutions, and helping customers leverage these tools for extended threat detection and response. We're continuously investing in training and focused Microsoft resources across our organization to help you accelerate value from your Microsoft security investment.

With 24x7x365 monitoring, our highly skilled analysts work in a SOC 2 Type 2 certified center to investigate, escalate, contain, and respond to threats – helping to significantly reduce attacker dwell time.



Never miss a threat. Or your desk.

Take threat detection and response on-the-go with the MOBILE**SOC** application. An industry-leading first, you have the power of our ZTAP platform in your hands, with the ability 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.

KEY BENEFITS OF THE INTEGRATION

- 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 your Microsoft security investments.
- Triage and contain alerts from anywhere with CRITICAL**START** MOBILE**SOC.**

DID YOU KNOW?

CRITICAL**START** is a Microsoft MSSP Program Partner, and a member of the Microsoft Intelligent Security Association (MISA).

CRITICALSTART
They're good. We're better.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICALSTART MDR + Microsoft Defender for Endpoint	Other MDR Providers
Investigate all operating systems without added agent deployment	●	✕
Resolve/confirm verdicts from auto-IR	●	✕
IOCs for Windows, Mac, and Linux	●	✕
Investigate trust levels of every device	●	✕
PowerShell Live Response library	●	✕
Granular guest user auditing	●	✕
Native iOS and Android applications for alert investigation, collaboration and response	●	✕
Multi-Tenant so client can have multiple organizations with N-level hierarchy	●	✕
Manage and report on all alerts from SIEM and EDR in one platform	●	✕
Automated SOC review process that provides quality control of analyst investigations and is available to the customer	●	✕
Contractually guaranteed Service Level Agreement for analyst Time to Detect and Respond to Alert (as compared to SLO)	●	✕
Alert notifications that include both security event data and expert analysis	●	◐
Customer and vendor work from the same platform and see the same information for security event analysis (Transparent view to all rules, comments, audit logs, and metrics)	●	◐
Custom Indicator of Attack (IOA) Monitoring	●	●
24x7 monitoring, investigation and response by security analysts	●	●
Advanced Threat Detection and Hunting	●	●
Analyst will proactively respond to stop attacks (isolate, block whitelist, etc.)	●	●
Managed response, policy tuning, and updating of agents	●	●
Incident Response	●	●
SSAE 18 SOC 2 (TYPE 2) Certified	●	●

Member of
Microsoft Intelligent Security Association

Microsoft

Goodbye, alert fatigue. Hello, CRITICALSTART.

Contact Us | Request a Free Assessment

CRITICALSTART
They're good. We're better.