SOLUTIONS OVERVIEW

CRITICAL**START** Managed Detection and Response Services for Microsoft Security

Microsoft Security

We do what others don't.

CRITICAL**START**™ provides deep integration with the Microsoft security suite to detect every event, resolve every alert, and respond to breaches. We reduce risk acceptance and magnify security visibility by leveraging the deep cybersecurity insights and capabilities that make the Microsoft security stack different from other extended detection and response (XDR) solutions.

Unified managed detection and response (MDR) services with Microsoft Security tools that's more than good. *It's better.*

Integration, the better way.

Our services integrate with, leverage, and optimize Microsoft security solutions for enhanced threat detection and response outcomes. Integration with the Microsoft security suite is engineered to enforce secure access. We only request the minimum level of permissions needed, and we never ask for highly privileged roles such as Global Administrator.

Resolving alerts is good. Resolving all alerts *is better.*

MDR services leverage the Zero Trust Analytics Platform (ZTAP) to collect, understand, and resolve every incident across the Microsoft environment. ZTAP enriches every alert with additional metadata from the Microsoft environment. Our service also features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives), delivering the scalability to resolve every alert.

Not more resources. Better ones.

Extend your team with highly skilled Microsoft Security experts for 24x7x365 threat detection and response coverage backed by contractual service licensing agreements (SLAs) for Time to Detect (TTD) and Median Time to Resolution (MTTR). Several security analysts have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Azure Security Technologies certifications.

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with the MOBILE**SOC**™ application. An industry-leading first, MOBILE**SOC** puts the power of the ZTAP platform in your hands, giving you the ability to contain breaches right from your phone.

We resolve more than **99%** of alerts

We escalate less than **0.01%** of alerts to customers

We reduce customer investigation time by an average of **99.3%***

*Assumption of workload based on average of 7-minute CRITICALSTART alert investigation time. Customer workload with ZTAP and MDR is 22 hours/week. For the same volume of alert resolution without CRITICAL**START** MDR service and ZTAP platform, it would take 3,179 hours/week.

How we do it

Managed Detection and Response Services for Microsoft 365 Defender

CRITICALSTART MDR services for Microsoft 365 Defender leverage:

- ✓ Queries within the ZTAP platform to pull in additional data from multiple Microsoft consoles into one single pane of glass
- ✓ 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
- ✓ Threat detection content management, provided by the CRITICALSTART™ Cyber Research Unit, leverages the CRITICALSTART™ Threat Navigator to manage the hundreds of new detections being released daily by Microsoft.

We also manage the Indicators of Compromise (IOC) published by Microsoft on an hourly basis to improve detection performance.

LEARN MORE CRITICALSTART Managed Detection and Response Services for Microsoft 365 Defender

Managed Detection and Response Services for Microsoft Defender for Endpoint

CRITICALSTART has a deep integration with Microsoft Defender for Endpoint that enables us to analyze every alert by matching it against ZTAP and providing unmatched transparency and automated security and control. Our service is built on comprehensive insights into operating system threats and shared signals across devices, identities, and information to identify and contain compromised accounts. These features, combined with 24x7x265 monitoring by a team of highly skilled analysts

LEARN MORE CRITICALSTART Managed Detection and Response Services for Microsoft Defender for Endpoint

Managed Detection and Response Services for Microsoft Azure Sentinel

CRITICALSTART MDR services integrate with Microsoft Azure Sentinel to detect every event, resolve every alert, and escalate only the alerts that matter to you. In our MDR service, we:

- ✓ Investigate and resolve all security alerts generated by Azure Sentinel
- ✓ Use the CRITICALSTART Threat Navigator to manage, maintain, and curate Azure Sentinel out-of-box detections and Indicators of Compromise (IOCs)
- ✓ Map detection content to the industry approved MITRE ATT&CK® framework
- ✓ Include CRITICALSTART proprietary detections and IOCs
- ✓ Ingest all source data across all users, devices, applications and infrastructures for investigation and automatic resolution of what is known-good (false-positives)

LEARN MORE CRITICALSTART Managed Detection and Response Services for Microsoft Azure Sentinel

KEY BENEFITS

- ✓ Comprehensive threat detection and response coverage for the Microsoft Security suite
- ✓ Reduce risk acceptance
- ✓ Extend your team with Microsoft security expertise
- ✓ Speed up investigation and response and consolidate visibility in one portal
- ✓ Reduce attacker dwell time
- ✓ Accelerate value from your Microsoft security tools
- ✓ Triage and contain alerts on-the-go with MOBILESOC

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.