CRITICALSTART

Managed Detection and Response for Microsoft Defender for Endpoint

A simple yet comprehensive approach to stop breaches for Microsoft security customers.

CRITICALSTART™ Managed Detection and Response (MDR) services with Microsoft Defender for Endpoint compound the security value provided by Microsoft security tools by leveraging our considerable multi-platform MDR expertise, comprehensive Microsoft integration, and our trust-oriented approach which eliminates false positives at scale.

The Key Benefits of the Integration

For customers already using Microsoft security tools, CRITICAL**START** provides seamless integration across services and attack vectors to stop advanced threats and quickly detect anomalous behavior. Integrated detection across Endpoints, Identities, and Office 365 helps to reduce false positives by contextually aggregating alerts together to identify attacks and create unique insights.

Transparency

Full visibility into every data point collected, every alert resolved or escalated, every playbook. Your team sees the same dashboard as the CRITICAL**START** SOC. Our comprehensive cross-SaaS solution also brings deep visibility, strong data controls, and enhanced threat detection to your Microsoft Cloud Applications.

Trust-Oriented MDR Approach

The Trusted Behavior Registry (TBR) automatically resolves what is known-good and can be safely addressed first – shifting focus to unknown alerts for triage and quick resolution. With 24x7x365 monitoring, our highly skilled analysts work in a SOC 2 Type 2 certified Security Operations Center (SOC) to investigate, escalate, contain, and respond to threats – helping to significantly reduce attacker dwell time.

Comprehensive Integration

Unlike other managed security services, our Microsoft Defender for Endpoint MDR service uses the Microsoft ecosystem of tools to provide a unique solution for effective threat detection and response. Integration with Microsoft security tools is focused on principals of least privilege and investigations that take advantage of user-based detections in Azure Active Directory. This all-in on security approach is applied at every security layer – least privilege, rule creation and integration points.

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

> MOBILE**SOC**
>
> CRITICAL**START** offers native iOS and Android apps to give analysts full access to their MDR toolset on the go. Within the fully featured app, analysts can investigate alerts, communicate with CRITICAL**START** Security Experts, and respond, all without needing a computer.

CRITICAL**START**

Capability Comparison

	CRITICAL**START** MDR + Microsoft Defender for Endpoint	Other MDR Providers
Trusted Behavior Registry that resolves 100% of alerts	●	✕
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 Indications of Attack (IOA) Monitoring	●	●
24x7 monitoring by Cybersecurity Analysts (Security Alert Investigation and Notification performed 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	●	●
Privacy Shield Certified	●	●
SSAE 18 SOC 2 (TYPE 2) Certified	●	●

● Complete Offering ○ Partial Offering ✕ No offering

Want more information on CRITICAL**START?**
To see how we can help, contact us at www.criticalstart.com

CRITICALSTART