

CRITICALSTART® MDR for Microsoft Security

Microsoft Makes the Tools. Critical Start Helps You Maximize the Value.

KEY BENEFITS

- ✓ **Trust your alerts** with Managed Detection and Response (MDR) provided by an expert, Microsoft Managed Partner.
- ✓ **See rapid ROI** by eliminating false positives and focusing your security team's effort on the alerts that matter most.
- ✓ **Protect global employees** from phishing attacks, fraudulent website domains, stolen administrator credentials, technology vulnerabilities, and other security events.
- ✓ **Contain threats faster** with integrated response actions available from within your Microsoft console, the Critical Start portal, or the Critical Start MOBILESOC® mobile app.
- ✓ **Enhance proactive security controls** with a unified asset inventory across all connected sources, customizable asset criticality, and endpoint & vulnerability scanner coverage gap detection.

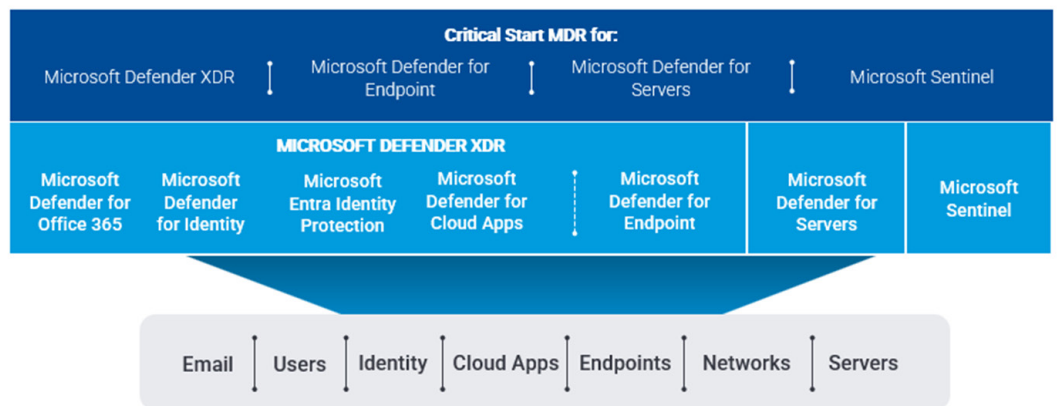
Microsoft's security tools help organizations like yours consolidate and simplify security tools and reduce spending. However, staff constraints, limited expertise, and continually shifting environments can place a significant strain on already challenged security and operations teams. How can you be certain you are fully leveraging your Microsoft security tools?

CRITICALSTART® Managed Detection and Response (MDR) for Microsoft gives you the expertise you need, with proactive security capabilities that result in immediate ROI and the ability to protect against advanced attacks.

How it works

Critical Start MDR starts with personalized and tailored onboarding. Whether you already have a Microsoft environment, or you are migrating your solutions, our onboarding and professional services teams will meet you where you are.











Once integrated with Critical Start MDR, you gain comprehensive service coverage across your Microsoft security tools. Starting with full visibility across your asset inventories, you will see customizable asset criticality and analysis of assets that lack critical security controls, such as endpoint agents and vulnerability scanners. Our 24x7x365, U.S.-based Security Operations Centers (SOCs) provides human-driven, technology-powered detection and response that ensures escalations represent true positives so you can stop threats quickly. You will see dozens of integrated response actions tailored to Microsoft and other environments, and you can customize Response Authorizations to better orchestrate the actions the Critical Start SOC takes on your behalf. Critical Start further streamlines investigations with Microsoft Lighthouse, giving you control over how our SOC works within your systems. With full SOC transparency – including contextualized justification for every alert closure, regardless of criticality – you will know exactly what is happening within your environment so you can continually improve your security posture.



Member of
Microsoft Intelligent Security Association
Microsoft

Human-driven , flexible security services that improve Microsoft security outcomes

Critical Start MDR

-  24x7x365 threat monitoring, investigation, and guided remediation via the Cyber Operations Risk and Response™ platform and expert, U.S.-based SOC analysts
-  Human-driven, AI-assisted MDR that finds threats automated systems alone might miss
-  Flexible deployment options, including tailored playbooks, detection rules, and Response Authorizations
-  Risk mitigation on-the-go through with the full-featured MobileSOC app for Android and iOS
-  Unified visibility across Microsoft Security tools, including Defender XDR, Defender for Servers, Defender for Endpoint, and Sentinel
-  Contractual SLAs for all alerts, regardless of severity
-  False-positive and benign true positive elimination to reduce alert fatigue
-  Auto-response to common threats with expert escalation and two-person quality assurance reviews for all response actions
-  Framework-aligned Risk Assessments help you measure current posture against historical data and industry peer benchmarks
-  Rapid onboarding so you can be up and running quickly

SEIM Security Services for Microsoft Sentinel

- ✓ MDR services plus management and optimization for Microsoft Sentinel performance while enriching detections through advanced threat intelligence for all third-party data sources like firewalls, including CEF, SysMon, etc.
- ✓ Includes: Ongoing management (Cost ingest analysis, Quarterly Service Reviews, and updates)
- ✓ Identifying and resolving SIEM coverage gaps (including Zero-log Ingest Alert analysis, health monitoring, and log prioritization)
- ✓ Preventing the same attacks from reoccurring by ensuring the right mitigations are implemented with MITRE ATT&CK® Mitigation recommendations
- ✓ Custom detection rules and log sources, guided response recommendations, and detailed reporting
- ✓ Detection content and Indicators of Compromise (IOCs) mapped to the MITRE ATT&CK® Framework

MDR for Microsoft Defender XDR

- ✓ Cross-domain threat protection, including real-time detection, disruption of attacks, robust identity monitoring, and SOC response actions for:
 - Microsoft Defender for Office 365 (MDO)
 - Microsoft Defender for Identity (MDI)
 - Microsoft Entra Identity Protection (ME-IDP)
 - Microsoft Defender for Cloud Apps (MDCA)

MDR for Defender for Servers

- ✓ Threat detection and response for dynamic server workloads across hybrid and multi-cloud environments
- ✓ Automated provisioning and tailored policies by asset criticality

MDR for Defender for Endpoint

- ✓ Endpoint coverage gaps identification and remediation (assets missing Endpoint Protection (EPP)/Endpoint Detection and Response (EDR)) to ensure full coverage and protection
- ✓ Visibility into threats across Windows, Mac, and Linux

Microsoft Professional Services

- ✓ Readiness assessments, deployment assistance, and optimization services for Microsoft Security Solutions
- ✓ Jumpstart Services to accelerate incident response readiness
- ✓ Breach preparedness training
- ✓ Customized exercises to practice response
- ✓ Expert incident response retainers for priority response

Learn More

Book a demo to see Critical Start MDR for Microsoft Security in your environment.