CRITICAL**START**®
Elevating MDR with Direct Integrations, Comprehensive Coverage, and SLA-Backed Response

CRITICAL**START**®

Traditional Endpoint Detection and Response (EDR) solutions don't cut it against today's sophisticated cyber threats. Critical Start redefines Managed Detection and Response (MDR) with direct integrations, complete security coverage, and SLA-backed threat investigation, ensuring you stay ahead of persistent and pervasive risks.

Here's how Critical Start outperforms other providers and delivers the MDR your business needs.

2

Comprehensive Security Coverage Beyond EDR

Modern MDR must extend beyond endpoints to address the full spectrum of threat vectors. Critical Start ensures no blind spots by providing visibility and protection across diverse environments with:

Broad Threat Vector Coverage

We monitor endpoint, server, user, identity, on-premises infrastructure, applications, hybrid, cloud, and Operational Technology (**OT**)/Industrial Control Systems (**ICS**) environments.

Direct Integrations

With over 35 bi-directional integrations across EDR, identity, email, cloud, and OT (e.g., Microsoft Defender, CrowdStrike, Okta, Palo Alto), we access real-time data directly from your tools, bypassing slow SIEM pipelines for faster detection and response.

Eliminating Blind Spots

Our SOC Signal Assurance identifies hidden assets and unmonitored infrastructure, ensuring complete signal coverage.

Unlike competitors who rely on proprietary tools, Critical Start leverages your existing stack with direct integrations, maximizing your current investments without forcing new tools.

SLA-Backed Threat Investigation and Response

Speed and accountability are critical in mitigating cyber threats. Critical Start delivers industry-leading response times backed by contractual Service Level Agreements (**SLAs**).

Alert Handling

Our alert typing system classifies alerts into threat and non-threat categories. Threat alerts get human investigation, while non-threat alerts are auto-resolved or routed back with full context, reducing noise and ensuring focus.

Contractual SLAs

We guarantee a 10-minute notification for critical alerts and a 60-minute or less MTTR for all alerts, with no exceptions. These commitments are in writing, ensuring reliability.

Competitors' Vague SLAs

Many providers' SLAs are limited to notification times and lack clear resolution or containment guarantees, leaving you uncertain about the response you'll actually get.

Our precision alert handling and enforceable SLAs make your security work for you, delivering results you can count on.

Human-Driven Expertise with Direct Action

Automation alone can't tackle complex threats. Critical Start pairs technology with human expertise for superior outcomes.

24x7x365 SOC Team

Our U.S.-based analysts, trained over 18 months with a 90% retention rate, provide in-depth investigation and true mitigation, backed by a two-person integrity review.
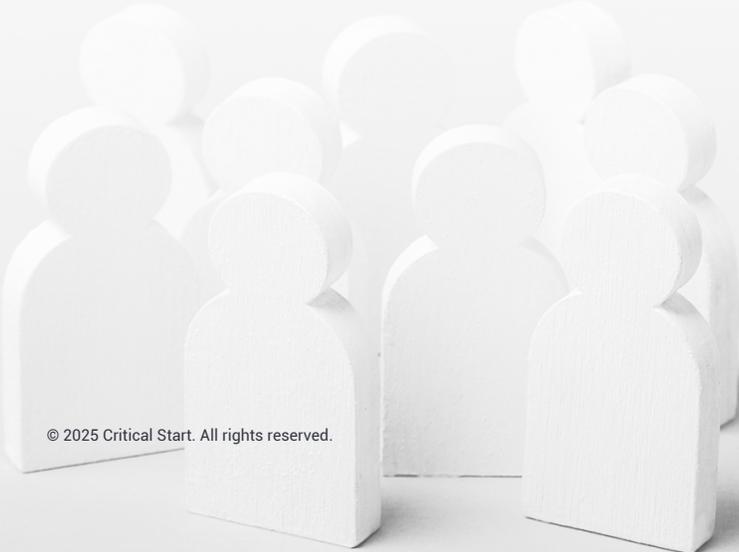
Direct Integrations for Rapid Response

We take immediate action — like isolating endpoints or blocking IPs — directly within your tools, ensuring faster containment without delays.

Competitors' Limitations

Other providers' reliance on proprietary tools can lead to high false positives and vague threat details, lacking the human nuance and direct action Critical Start delivers.

With Critical Start, you get experts who act decisively, not just notify.

Why Critical Start?

Critical Start transcends traditional MDR by integrating proactive security intelligence with responsive, tailored solutions. Our direct integrations eliminate vulnerabilities across all environments, SLA-backed response guarantees rapid action, and human-driven expertise ensures precision. Unlike competitors who lock you into proprietary tools and vague SLAs, Critical Start adapts to your stack and delivers clear, enforceable commitments.

CRITICALSTART ⏻

For more information, contact us at

https://www.criticalstart.com/contact/