SOLUTIONS SHEET

CRITICAL**START**® MDR Use Cases

From alert to containment without the guesswork: MDR that drives faster, clearer outcomes across your environment.

The Problem Isn't Just Alerts. It's What Happens After.

If you're still drowning in alerts, it's not because your tools aren't working — it's because your Managed Detection and Response (**MDR**) isn't.

Critical Start reduces noise and dwell time. Through Direct Integrations with the tools you already own, we deliver continuity, trust, and better security outcomes.

Response Isn't a Feature. It's the Foundation.

Whether **ransomware on an endpoint, privilege abuse in identity**, **or phishing in email**, we respond fast to threats: investigated by expert SOC analysts, contained in minutes, and resolved with clear accountability.

Across your critical technologies, you get:

- **Rapid escalations & swift SOC analyst support**
- **≤60 minutes contractual SLAs for Mean Time to Detect (MTTD) & Median Time to Resolution (MTTR)**
- **Tailored response playbooks**
- **Full audit trail transparency**

Our Promise: Clarity, Control, Confidence, and Commitment to Your Security Outcomes

Every action across your security tools is visible — what was done, why, and who did it.

- CISOs can report confidently across their entire ecosystem.
- Analysts get the context they need to resolve threats faster and work smarter.

Direct Integrations Include:

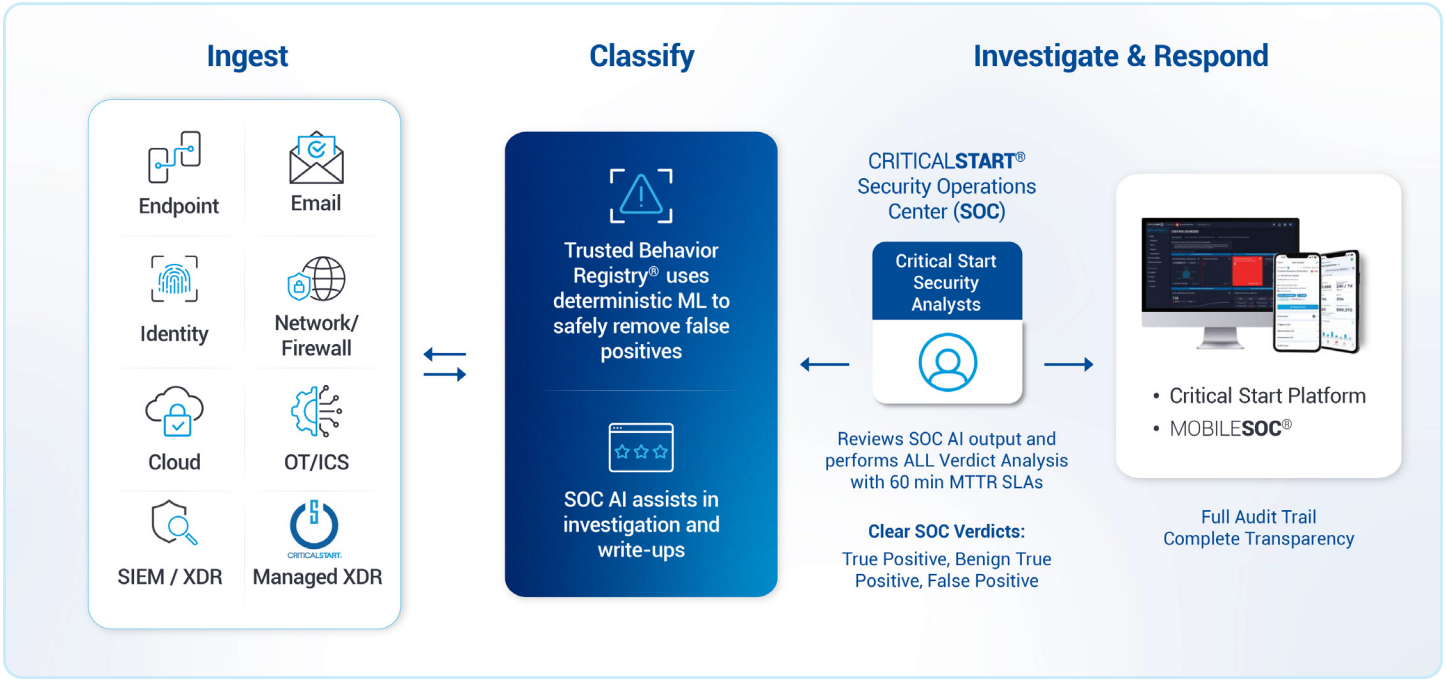
ENDPOINT	IDENTITY	EMAIL	NETWORK	CLOUD
Microsoft Defender for Endpoint	Microsoft Defender for Identity	Microsoft Defender for Office 365	paloalto NETWORKS	AWS GuardDuty
SentinelOne	Microsoft Entra ID/ Entra ID Protection	Abnormal	FORTINET	Microsoft Defender for Servers
paloalto NETWORKS	okta	proofpoint.	zscaler	
CROWDSTRIKE	CROWDSTRIKE		cisco Cisco Umbrella	

OT and SIEM Integrations: We support OT technologies through both direct integrations and indirect ingestion via SIEM, and also integrate directly with leading SIEM platforms, enabling coverage across 100s of additional technologies.

Alert and Action Types — How We Operationalize Response with Clarity and Control

For every alert ingested, our **Critical Start Cyber Operations Risk & Response™ (CORR) platform** applies the **appropriate mix of automation** and **AI/ML,** then our SOC analysts add the **human expertise** to ensure fast, high-confidence security outcomes.

Critical Start Cyber Operations Risk & Response™ Platform



Each alert is tagged with a specific **Alert Type** as it's ingested. This classification sets expectations for investigation depth, urgency, and escalation and helps avoid wasting time on noise. Once a validated alert is confirmed, the **Action Type** guides the analyst on the allowable next steps based on the customer's Rules of Engagement (**RoE**). This is how we turn detection into resolution — not just response but results you can prove.

ALERT TYPES

- **Threat**
- **Custom Threat**
- **Control Violation**
- **Mitigated Threat**
- **Observation**
- **Posture Management**
- **Audit**
- **Compliance**
- **Operational**

ACTION TYPES

- ✓ **Response**
  - Containment
  - Eradication
  - Recovery
  - Prevention
  - Tuning
- ✓ **Investigation**
  - Threat Context
  - Impact Analysis
- ✓ **Create Ticket** (Integration)
- ✓ **External Automation** (Integrations)
- ✓ **Notification**
- ✓ **Escalation**
  - Request Information
  - Request Response Action
  - Request Response Approval

Use Cases

These use cases may seem standard, but what sets Critical Start apart is how we handle them. Every alert is classified by type and business impact before action, so your team isn't left sorting through noise. **We correlate threats across domains — like email to identity to endpoint — and act fast based on your Rules of Engagement**. It's not just what we detect. It's how we respond that makes the difference.

Endpoint Security

- Contain **malware** and **ransomware** to stop business disruption early
- Reveal **attacker persistence** and **privilege abuse** (e.g., lateral movement, abnormal user behavior)
- Identify **execution tactics** like LOLBins, suspicious binaries, and obfuscated/encoded scripts
- Disrupt **data exfiltration** and **Command and Control (C2)** (credential dumping, data staging, and outbound traffic)

Cloud Security

- Detect and block **unauthorized cloud account access**
- Catch **misuse of cloud services** (e.g., rogue workloads, SaaS abuse)
- Flag **suspicious API calls** used in automation or credential attacks
- Prevent **public exposure of cloud resources**
- Analyze and respond to **unusual data access patterns** (e.g., sudden spikes in download volume, geolocation anomalies)

Identity Security

- Detect and contain **account compromise** (e.g., failed identity verification or login anomalies)
- Disrupt **lateral movement via credential abuse** (e.g., pass-the-hash/ticket activity or correlating identity behavior with endpoint and network signals)
- Flag **Multifactor Authorization (MFA) fatigue or bypass attempts**, like repeated push notifications
- Catch **identity-based policy violations**, including unauthorized access attempts and privilege abuse

Network

- Detect and disrupt **Command and Control (C2) beaconing** (e.g., DGAs, known malware infrastructure)
- Detect **unauthorized network access** and **policy violations**
- Block or escalate **outbound connections to malicious IPs or domains**
- Detect **lateral movement** that crosses security zones or bypasses normal access paths
- Identify **port scanning or protocol violations** early

Email Security

- Detect and stop **Business Email Compromise (BEC) and impersonation** attempts before executives, payments, or supply chains are targeted
- Block **phishing and credential harvesting** via malicious links or attachments
- Investigate **email account takeover** (e.g., abnormal login behavior, suspicious inbox rules, or MFA bypass)
- Contain **malicious attachments or embedded payloads**
- Detect **abuse of trusted services**, such as malicious SharePoint or Google Docs links
- Catch **internal lateral movement** via email inbox rule abuse or peer phishing

Why Security Leaders Choose Critical Start

Intelligent MDR That Works Across All Your Security Stack

For CISOs responsible for reducing risk and demonstrating security program value, we provide measurable outcomes, SLA-backed performance, and full transparency through our **CORR platform**. From audit trails to simplified stack management through Direct Integrations, Critical Start aligns MDR with your operational goals and reporting needs.

For SOC leaders seeking real-time threat triage, fast containment, and direct access to analysts, Critical Start delivers an MDR experience built for speed and clarity. Expert analysts evaluate every threat alert, every action follows your Rules of Engagement, and MOBILE**SOC**® enables 24x7x365 responsiveness from anywhere.

What Sets Us Apart	Why It Matters
Direct Integrations	Act directly in your tools — no delays from SIEM correlation or manual escalations
SOC AI + Expert Analysts	Accelerate triage, reduce dwell time, and ensure human judgment in every decision
Trusted Behavior Registry® (TBR®)	Starting with the transparency provided by alert typing, the TBR® suppresses false positives and known good activity before it hits your queue.
Two-Person Integrity	Every response action is verified by a second analyst for accuracy and accountability
Rules of Engagement (RoE)	Every containment or escalation respects your internal policies and thresholds
Full Transparency	Never a "black box" — see what was done, why, and by whom
MOBILE**SOC**®	Triage, take real-time response actions, and contain threats from anywhere, with direct analyst communication through our mobile application for iOS and Android

Ready to respond faster and prove value across your stack?

Let us show you how Critical Start MDR works with your tools to deliver clarity, control, and confidence. **Request your personalized demo today.**