SOLUTION BRIEF

CRITICAL**START** Managed Detection & Response Services for CrowdStrike Falcon EDR

KEY BENEFITS

- ✓ Comprehensive threat detection and response coverage for CrowdStrike Falcon EDR
- ✓ Extend your team with threat detection and response expertise
- ✓ Reduce risk acceptance
- ✓ Speed up investigation and response in one portal
- ✓ Reduce attacker dwell time
- ✓ Triage and contain alerts from anywhere with MOBILE**SOC**
- ✓ Accelerate value from CrowdStrike Falcon EDR

Endpoint visibility, detection, and response to reduce attacker dwell time and accelerate time to remediation

We do what others don't. Endpoint data is good, but not enough to investigate all alerts. CRITICAL**START** Managed Detection & Response (MDR) service integrates with CrowdStrike Falcon EDR® to quickly detect every event, resolve every alert, and respond to breaches. This trust-oriented approach helps customers reduce risk acceptance, eliminate alert fatigue, and demonstrate value from their Falcon EDR investment – on day one.

Why CRITICAL**START**

Resolving alerts is good. Resolving all alerts is better.

- ✓ Our trust-oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We auto-resolve more than 99% of alerts
- ✓ We escalate less than 0.01% of alerts – the alerts that really require the attention of your security team

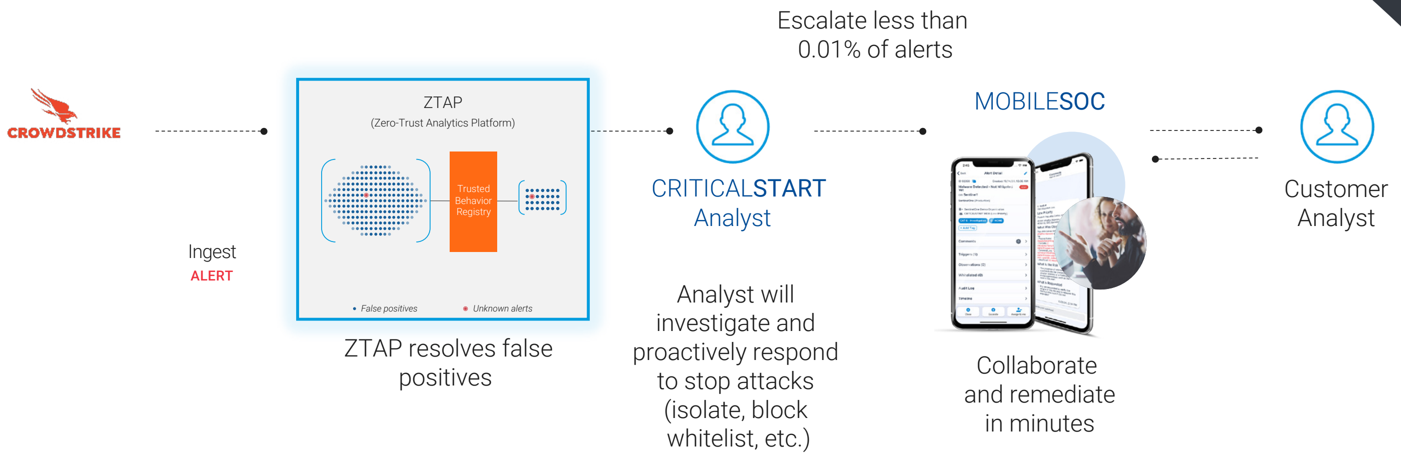
Not more resources. Better ones.

Leverage the collective experience of security experts with backgrounds in threat detection and response
and expertise across a broad range of security domains.

- ✓ Falcon EDR experts' setup and manage the environment in weeks, not months
- ✓ Security analysts are rigorously trained: Complete 200 hours of training during onboarding and another 40-80 hours annually
- ✓ Provide 24x7x365 end-to-end monitoring, investigation, and response

How we do it. (Resolve all alerts, that is.)

We take every alert from Falcon EDR into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates and proactively responds to stop the attack on your behalf. Our analysts then collaborate with you to remediate in minutes.


CROWDSTRIKE
Ingest
ALERT
ZTAP
(Zero-Trust Analytics Platform)
Trusted Behavior Registry
False positives
Unknown alerts
ZTAP resolves false positives
CRITICALSTART Analyst
Analyst will investigate and proactively respond to stop attacks (isolate, block whitelist, etc.)
Escalate less than 0.01% of alerts
MOBILESOC
Collaborate and remediate in minutes
Customer Analyst

So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service for Falcon EDR is IOC management. IOCs are constantly published and updated. The process of publication and application of additional detections can be hard to manage and a full-time job, so we added this feature in the service for *no additional cost.*

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILE**SOC** application. An industry-leading first, MOBILE**SOC** puts the power of our ZTAP platform in your hands, allowing you to contain breaches right from your phone. Our iOS and Android app features 100% transparency, with full alert detail and a timeline of all actions taken.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✗ NO OFFERING

	CRITICAL**START** MDR with Falcon EDR	Other MDR Providers
24x7x365 monitoring, investigation, and response by security analysts	●	●
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts, regardless of priority level	●	✗
Native iOS and Android applications for alert investigation, collaboration, and response	●	✗
Customer and vendor work from the same platform and see the same information	●	◐
Custom Indicator of Attack (IOA) Monitoring	●	✗
Two-person integrity review process that provides quality control of SOC orchestration for every customer	●	✗
Manage and maintain cross-ecosystem Indicators of Compromise (IOCs)	●	✗
Continuous threat hunting	●	◐
Perform configuration, deployment, and health checks without requiring additional professional services	●	●
Alert notifications that include both security event data and expert analysis	●	◐
Analyst will proactively respond to stop attacks (isolate, block whitelist, etc.)	●	●
Managed response, policy tuning, and updating of agents	●	●
Investigate all operating systems without agent deployment	●	✗
IOCs for Windows, Mac, and Linux	●	✗
PowerShell Live Response library	●	✗
Multi-Tenant so customer can have multiple organizations with N-level hierarchy	●	✗
Manage and report on all alerts from SIEM and EDR in one platform	●	✗

Goodbye, alert fatigue. Hello, CRITICALSTART.

Contact Us

Request a Free Assessment

CRITICALSTART
They're good. We're better.