SOLUTION BRIEF

CRITICAL**START** Managed Detection & Response Services for SentinelOne Singularity Complete

KEY BENEFITS

- Extend your team with threat detection and response expertise
- Complete visibility and just-in-time information
- Consolidate automation containment and recovery playbooks
- Accelerate value from SentinelOne® Singularity Complete
- Triage and contain alerts from anywhere with MOBILE**SOC**™

Strategic and tactical detection, investigation and response capabilities that adapt to the unique needs of your environment.

We do what others don't. The CRITICAL**START** Managed Detection & Response (MDR) services seamlessly integrate with your existing SentinelOne Singularity Complete deployment to provide monitoring, investigation, and response, helping reduce and mitigate risk and improve security operations center (SOC) productivity. We adapt our services to your unique environment to provide high-fidelity detections, rapid investigation to provide context into decision making, and expertise available to make faster, more accurate decisions on which response actions to choose.

Why CRITICAL**START**

Comprehensive threat detection, analysis, and response capabilities

CRITICAL**START** MDR services for SentinelOne Singularity Complete provides:

- ✓ 24x7x365 end-to-end monitoring, investigation, and proactive response to stop attacks
- ✓ Simplified deployment across a diverse set of operating systems (including Mac, Windows, and Linux)
- ✓ Full real-time visibility into every data point collected, every alert resolved or escalated, every playbook
- ✓ Access to every operation and historical data for deeper visibility and faster response
- ✓ Ability to contextualize and identify threat actors in real-time to help drive down dwell time

Resolving alerts is good. Resolving all alerts is better.

- ✓ Trust oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We resolve more than 99% of alerts
- ✓ We escalate less than 0.1% of alerts – the alerts that really require the attention of your security team

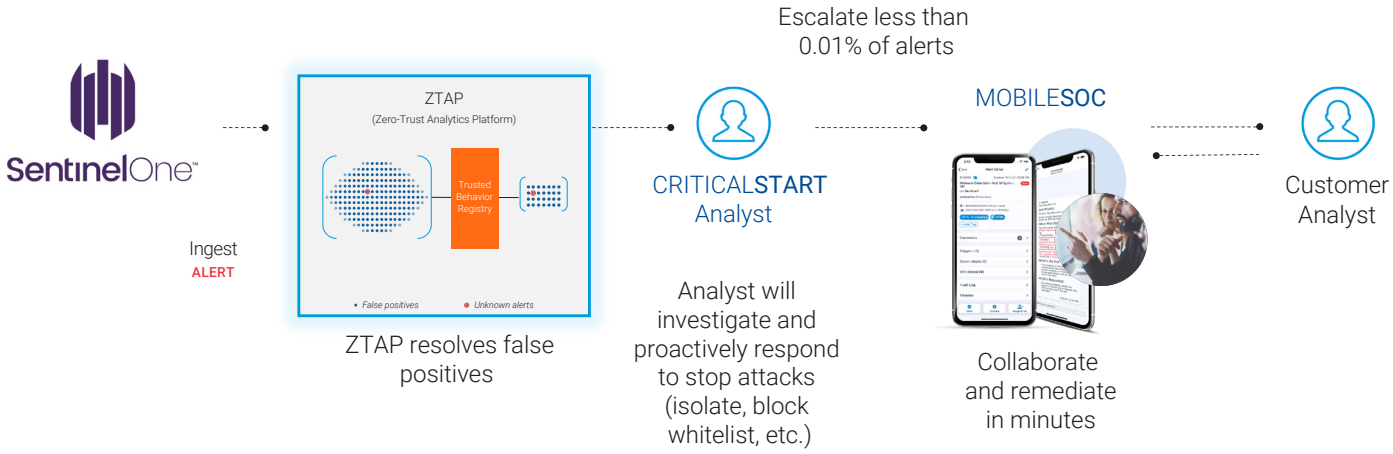
Not more resources. Better ones.

Extend your security team with the collective experience of our security experts who have backgrounds in threat detection and response and expertise across a broad range of security domains.

- ✓ Singularity Complete experts setup and manage the environment in weeks, not months
- ✓ Security analysts are rigorously trained: Complete 300 hours of training during onboarding and another 40-80 hours annually
- ✓ CRITICAL**START**™ Cyber Research Unit (CRU)--Elite team, comprised of Cyber Threat Intelligence (CTI) and Detection Engineering (DE). Our CTI team curates original and third-party intel that our DE team uses to develop new detections
- ✓ Dedicated Customer Success Manager for continuous optimization of your threat detection and response service

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

We take every alert from Singularity Complete 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.



So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service for Singularity Complete 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. The CRITICAL**START** Detection Engineering team enhances out-of-the box detection capabilities by developing and adding proprietary IOCs and behavioral detections from curated threat intelligence, previous SOC investigations, Incident Response team investigations and external threat intelligence feeds. Leveraging the The CRITICAL**START** Threat Navigator, we manage, maintain, and curate SentinelOne out-of-box detections and Indicators of Compromise (IOCs). Detection content is also mapped to the industry leading, MITRE ATT&CK™ framework.

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILE**SOC** application. An industry-leading first, CRITICAL**START** 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 SentinelOne Singularity Complete	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, CRITICAL**START.**

Contact Us

Request a Free Assessment

CRITICAL**START**
They're good. We're better.