CRITICAL**START**
Zero-Trust Analytics Platform

They may copy our message, but they cannot copy our tech.

Resolving alerts is good. Resolving all alerts *is better.*

When combined with our elite SOC analysts, ZTAP eliminates alert fatigue, saves time and money, and lets you focus on what matters most to your business.

- ✓ Over 90% of TBR playbooks are common to all customers and applications.
- ✓ 9% of playbooks are adapted to individual customers.
- ✓ We auto-resolve 99% all alerts.
- ✓ We escalate less than 0.01% of alerts.

The backbone of highly effective managed detection and response (MDR) is the Zero Trust Analytics Platform (ZTAP) utilized by elite security analysts to resolve every alert.

Detect all events. Resolve all alerts. Stop breaches

Today's cyberattacks use hands-on techniques and purpose-built malware to scrape credentials, move laterally, exfiltrate data, and establish persistence. They employ sophisticated tactics to evade detection. A common tactic applies behaviors that generate lower priority alerts. So how do you protect your business?
By resolving every alert.

The challenge is that security tools generate tens of thousands of alerts each day. Resolving every alert creates an insurmountable scalability problem for security teams and traditional managed detection and response (MDR) service provider platforms. To reduce alerts to manageable volumes, these MDR platforms engage in alert suppression. But, at a cost – compromising the security of your data, IT assets, and your business.

Don't suppress alerts, resolve them.

CRITICAL**START** has the only solution to the scalability problem – the Zero Trust Analytics Platform (ZTAP). The only effective methodology for reducing alerts, without accepting risk, is to eliminate false positives, not unqualified lower priority alerts.

ZTAP features the Trusted Behavior Registry (TBR), the only database purpose-built to collect and identify known good behaviors. Alerts ingested into ZTAP are compared against known good behaviors in the TBR, where playbooks auto-resolve false positives. Alerts not identified by the TBR are escalated for investigation to the CRITICAL**START** Security Operations Center (SOC).

BENEFITS OVERVIEW

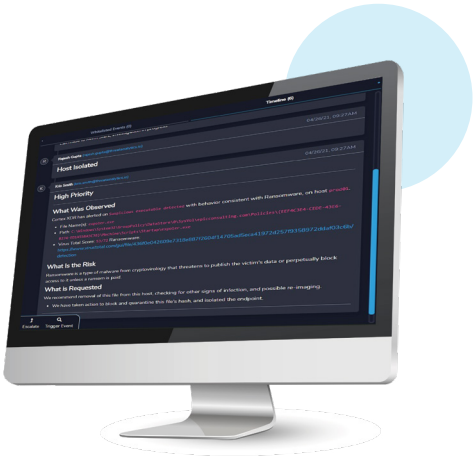
- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency and productivity
- ✓ Validate MDR service ROI
- ✓ Report on security posture
- ✓ View threat detection coverage mapped to MITRE ATT&CK framework

Collaborate and remediate through built in transparency.

ZTAP supports real-time communication and collaboration between CRITICAL**START** security analysts and our customers to resolve unknown alerts faster. Our ZTAP dashboard lets you see exactly what our analysts see.

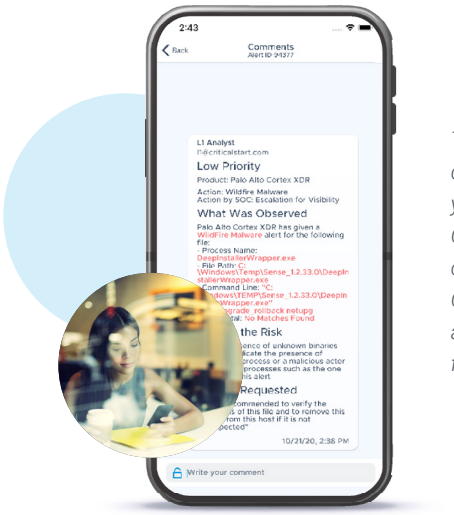
ZTAP provides:

- ✓ Immediate notification of alerts escalated by a CRITICAL**START** security analyst
- ✓ Triage information for full context and analyst recommendations
- ✓ Direct communication with our analysts to collaborate, make quick decisions, and act with confidence
- ✓ Threat analysis plug-ins to pivot to your security tools and gather more data to enhance investigation
- ✓ Visibility into threat detection and response coverage by leveraging the CRITICAL**START**™ Threat Navigator, which maps detection content to the MITRE ATT&CK® framework



*ZTAP dashboards allow CRITICAL**START** and customer analysts to communicate and collaborate in real-time to investigate and remediate unknown alerts faster.*

Threat Navigator maps security tool detections to the MITRE ATT&CK framework.



*The MOBILE**SOC** delivers ZTAP to your fingertips. Communicate and collaborate with CRITICAL**START** analysts anytime, from anywhere.*

Never miss a threat. Or your desk.

You can take ZTAP with you wherever you go, with our MOBILE**SOC**, the industry's first mobile MDR application. MOBILE**SOC** delivers the power of ZTAP via IOS or Android devices and provides visibility and direct communication with our analysts – without being tethered to a desk. You can deploy MOBILE**SOC** in minutes via our cloud-hosted platform.

CRITICALSTART
They're good. We're better.

Validate your security investments.

ZTAP delivers unrivaled transparency into your security posture. View every alert, alerts auto-resolved, alerts escalated and the actions we take on your behalf. Understand the how your security tools are performing. Validate the Value and ROI CRITICAL**START** MDR is delivering and that you expect with our real-time SLA dashboard.

*The SLA dashboard provides real-time proof of CRITICAL**START** performance, ensuring we deliver on our promises.*

We take the journey with you.

The CRITICAL**START** implementation team provisions and configures ZTAP to meet your specific needs. We take the extra step and help standup your security tools. The implementation team helps configure your security tools, tune endpoint and detection and response (EDR) policies and security information and event management (SIEM) use cases and add CRITICAL**START** Indicators of Compromise (IOC). After transitioning to live monitoring, we assign a Customer Success Manager – a dedicated point of contact to provide regular communication and advocate for your success.

Unparalleled partnerships.

ZTAP integrates with best-in-breed technologies across Endpoint, SIEM, Identity, Cloud and more. We deliver a more comprehensive security solution with the tools you already own or that best fit your environment.

CRITICALSTART
They're good. We're better.

Choose the CRITICAL**START** Difference

● COMPLETE OFFERING ✕ NO OFFERING	CRITICAL**START**	**Traditional MDR Providers**	**Outcomes**
Collect, Investigate & resolve all alerts	●	✕	Unrivaled reduction in risk acceptance to protect sensitive data and business operations
Extensive database of known good alerts	●	✕	Eliminates false positives for more efficient, scalable, and effective security operations
Complete built-in transparency	●	✕	Unmatched visibility into your security posture to support security decisions with confidence
Real-time SLA dashboards	●	✕	Unequaled visibility into MDR performance to prove value and validate ROI
Full platform functionality via mobile app	●	✕	Unmatched communication and collaboration anytime from anywhere

Goodbye, alert fatigue. Hello, CRITICAL**START.**

Contact Us **Request a Free Assessment**

CRITICALSTART
They're good. We're better.