# PALO ALTO NETWORKS and CRITICALSTART

Managed Detection and Response

## 99% REDUCTION IN ALERTS

## KEY BENEFITS OF THE INTEGRATIONS

**1** Take advantage of Cortex XDR as a managed service.

**2** Stop malware, exploits, and ransomware before they can compromise endpoints.

**3** Protect endpoints online or offline, on network or off.

**4** Use bidirectional integration with Traps management service to keep the console up to date with MDR activity.

**5** Coordinate enforcement with network and cloud security to prevent successful attacks.

**6** Integrate with technologies across Palo Alto Networks platforms.

## THE CHALLENGE

The cybersecurity landscape is changing by the day with the arrival of new threats and new tools designed to combat them. This creates excessive noise and confusion for security professionals to sort through, and many cybersecurity teams are drowning in complexity.

## CRITICALSTART MDR

Managed detection and response (MDR) service through CRITICALSTART lets you take advantage of:

- Faster endpoint protection deployment—weeks, not months—with an immediate reduction of alerts and accelerated ROI.

- Cortex XDR™ detection and response built into the offering for capabilities across your network, endpoint, and cloud environments.

- Cloud-based Security Operations Center (SOC) services to minimize on-site hardware and software.

- CRITICALSTART's MOBILESOC™ app for industry-leading detection and response capabilities on the go.

- 24x7x365 managed detection and response provided by highly experienced analysts and incident responders.

- 100 percent transparency—you see what CRITICALSTART sees, along with all research, notes, and escalation recommendations.

- Customized Filter based off of Behavioral Indicator of Compromise (BIOC).

## ADVANCED INSIGHTS AND PREPARATION WITH CRITICALSTART

Using a battle-tested assessment and implementation process, CRITICALSTART can assist you with deployments of all sizes. CRITICALSTART's Zero-Trust Analytics Platform (ZTAP) model investigates all security alerts until they are classified as good or normal and are safely filtered out. Using this approach, customers experience a 99 percent reduction in alerts. Zero-Trust is the only option when it comes to zero tolerance.

## PALO ALTO NETWORKS WITH MANAGED SERVICES

Cortex is the industry's only open and integrated AI-based continuous security platform. It delivers new levels of simplicity in security operations and significantly improves security outcomes through automation and unprecedented accuracy. The platform solves pain points for managed service partners, providing complete visibility from a single data source and the ability to respond as a managed service across the whole environment. Today, with Cortex XDR cloud-based detection and response, partners can provide managed threat hunting, investigation, and response across network, endpoint, and cloud environments.

## PALO ALTO NETWORKS AND CRITICALSTART

CRITICALSTART ensures that customers are protected around the clock by highly trained analysts who specialize in incident triage, malware analysis, and incident management and response. CRITICALSTART's MDR service is armed with Cortex XDR to deliver best-of-breed technology to joint customers for managed detection and response.

Cortex XDR removes security blind spots by stitching together network, endpoint, and cloud data to deliver monitoring, analysis, and coordinated response across your entire environment.

Alongside Traps™ management service, you'll get automated prevention, detection, and response capabilities through a single endpoint agent.

You can seamlessly integrate Cortex XDR as a cloud service into your security stack. Cortex allows managed services to be adapted and scaled at the speed and agility of the cloud, keeping you ahead of attackers as threats evolve.
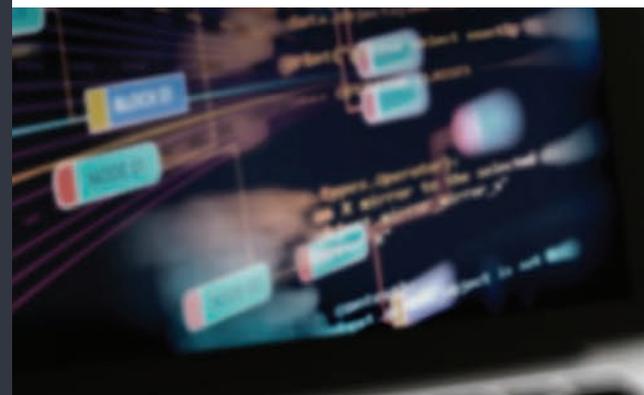
## ABOUT CRITICALSTART

CRITICALSTART is leading the way in Managed Detection and Response. Our mission is simple: protect our customers' brand while reducing their risk. We do this for organizations of all sizes through our award-winning portfolio, from the delivery of managed security services to security-readiness assessments using our proven framework, the Defendable Network, professional services, and product fulfillment. CRITICALSTART has achieved the Service Organization Control (SOC) 2 Type II compliance certification and was recently named a CRN® 2018 Triple Crown Winner. Visit www.criticalstart.com for more information.

## ABOUT PALO ALTO NETWORKS

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of changemakers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.

## START NOW

To see how we can help, contact us today at **877.684.2077** or email **info@criticalstart.com**.