DATASHEET

CRITICAL**START**® Managed XDR

Threat detection for user, cloud and application log sources.

KEY BENEFITS

- ✓ Unified MDR and log source management solution
- ✓ Contractual Service Level Agreements (**SLAs**) of 10-minute notifications for Critical alerts and 60-minute or less Median Time to Resolution (**MTTR**) for ALL alerts, regardless of priority
- ✓ Enhanced security coverage with data-driven threat detection and response
- ✓ Data storage and indexing (30-day log retention plus additional storage options)
- ✓ Scalable and flexible log source connectivity (e.g., add 10 now and more later at your own pace)
- ✓ **24x7x365** remote monitoring of performance, availability and capacity

Threat-centric visibility without a third-party SIEM

Critical Start Managed Extended Detection and Response (**XDR**) is a proactive defense solution that reduces cybersecurity risk by augmenting Managed Detection and Response (**MDR**) for Endpoint deployments with improved visibility, rapid delivery and enhanced security.

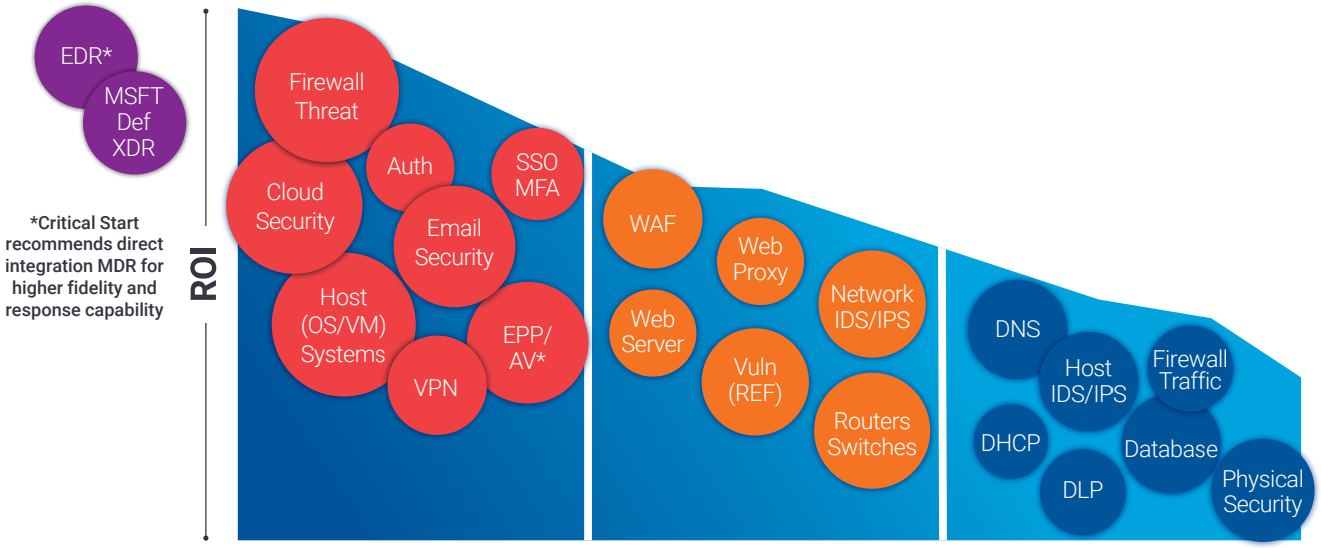
Our Managed XDR solution provides threat detection visibility across user, cloud, applications and network infrastructure by delivering the full benefits of our MDR service with an integrated log management platform that enables you to rapidly onboard hundreds of security-relevant log sources without the cost and complexity of purchasing, owning, managing, or maintaining a Security Information and Event Management (**SIEM**) while providing flexible and scalable integration for both on-prem and cloud-based log sources.

Now businesses of all sizes can address key cybersecurity pain points, including threat detection and cost optimization and elevate their security posture through efficient management, increased visibility and superior threat detection and response capabilities—all supported by a team of expert analysts monitoring customer systems **24x7x365** to ensure a fortified security posture.

How it works

Critical Start Managed XDR provides proactive defense and improves overall security effectiveness by combining data collection storage and indexing with managed and threat detection capabilities. Our integrated solution collects, aggregates, analyzes and correlates log data from various sources, such as firewalls, authentication, email security, cloud platforms and other security tools, providing timely analysis of security alerts and events generated across your organization's IT infrastructure, without the need of a third-party SIEM.

Key features include log source prioritization, log search and log visualization and flexible storage options for compliance, audit, forensics and threat-centric use cases. *(Fig 1)*



(Fig 1) Log prioritization for better security value

Discover valuable insights from your overlooked log data

Log data grows exponentially as organizations expand their tech stack and infrastructure, creating challenges around correlating events, managing triage times, identifying business impacts and more. Without visibility into your logs, you are missing out on valuable insights that can be used for better threat detection and incident resolution. Critical Start Managed XDR lets you pull all security-relevant logs into one centralized platform where you can get a better handle on threat detection, investigation and response.

Comprehensive security coverage

Now you can simplify the technologies necessary to improve your security posture without the burden of managing a SIEM platform or the need for in-house expertise. Our holistic solution allows you to address your challenges with log prioritization, data administration, and threat detection and response, all backed by the industry's only SLAs of a 10-minute notification for Critical alerts and 60-minute or less for Time to Detection (**TTD**) and MTTR. *(Fig 2)*

(Fig 2) Comprehensive security and data management for your log sources

Use our integrated approach to address use cases like:

- **Improving threat detection and response**
- **Expanding detection beyond the Endpoint (EDR/EPP)**
- **Enhancing visibility across IT infrastructure**
- **Extending visibility to Cloud Security and SaaS**
- **Addressing gaps in in-house expertise**
- **Optional long-term log storage for forensics and compliance needs**
- **Streamlining security management**
- **Increasing cost-effectiveness compared to deploying your own SIEM**

Why Critical Start Managed XDR?

Managed XDR is a cost-effective solution empowering organizations of all sizes to stay ahead of threats and focus on their core business while our team of experts handles the complex tasks of managing the data and detecting and responding to potential threats. Easily integrated with your existing log sources, it combines **24x7x365** Managed Detection and Response (**MDR**) with the scalability and flexibility you need to help you manage and streamline your security operations.

Contact us to learn how you can prevent business disruption with Critical Start

From threat detection and response to log storage, we're here to guide you every step of the way. Benefit from continuous log source management, peer benchmarking, direct access to our experienced Risk & Security Operations Center (**RSOC**) analysts, a two-person integrity review on every action to be taken, and **MITRE ATT&CK® Framework** coverage reporting. Evolve your security strategy with confidence, navigating the changing cybersecurity landscape while optimizing costs.

Click here to contact us for more information about Critical Start Managed XDR

CRITICALSTART®