DATASHEET

CRITICAL**START**® Managed Detection and Response (**MDR**) Services for Microsoft Defender for Servers

Threat detection and response for dynamic server workloads.

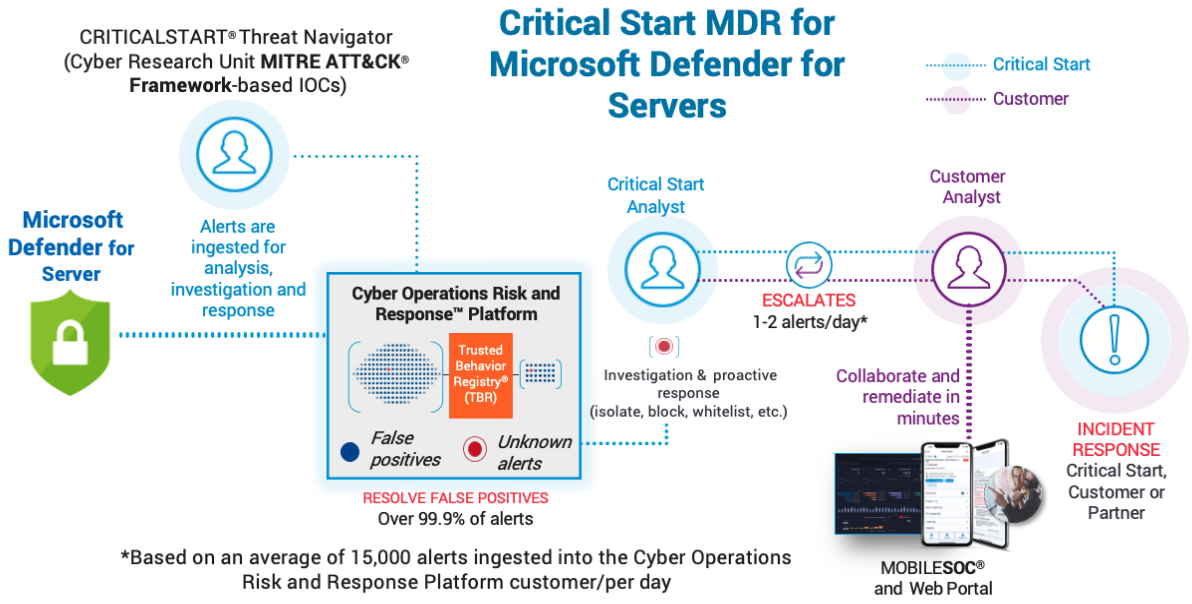
KEY BENEFITS

- ✓ Adaptable threat protection for dynamic multi-cloud server environments
- ✓ Monitoring of dynamic server workloads with support for automatic provisioning
- ✓ Tailored protection for critical servers with personalized playbooks
- ✓ Streamline endpoint and server security with consolidated visibility in a single portal
- ✓ Triage and contain attacks anytime, from anywhere with MOBILE**SOC**®
- ✓ NIST Cyber Security Framework maturity and MITRE ATT&CK® Framework coverage reporting

Managing security in rapidly changing server environments, with evolving configurations and dynamic workloads, can be challenging. Critical Start Managed Detection and Response (**MDR**) services for Microsoft Defender for Servers is essential in today's threat landscape, as it adapts to the dynamic nature of server environments, providing continuous protection and ensuring security remains up-to-date with the latest changes. Our service dynamically adjusts to the evolving server configurations and workloads, ensuring that your servers are always protected against emerging threats and costs are optimized.

Critical Start MDR services for Microsoft Defender for Servers allow you to:

- Streamline the deployment process ensuring consistent, reliable protection across all servers
- Ensure optimal security for business-critical resources with customized responses based on server criticality
- Identify and mitigate threats quickly with monitoring, investigation, and response across every alert, regardless of priority or severity with **15-min alert-to-fix and a contractual 60-min or less Median Time to Resolution (MTTR) service level agreement (SLA)**



How We Do It

Deploying and configuring endpoint protection for servers can be time-consuming and prone to errors. Critical Start MDR for Defender for Servers offers support for automatic provisioning, streamlining the deployment process and ensuring consistent, reliable protection across servers. The service automates monitoring during the provisioning and configuration of Microsoft Defender for Servers, saving time and eliminating the possibility of human error during the deployment process.

Tailored protection for critical servers

Different types of servers have varying levels of criticality and require tailored security measures and responses to protect sensitive data and applications. Critical Start MDR for Defender for Servers delivers customized responses based on the unique requirements of each server type - database, DNA or Webserver - providing targeted protection and response to safeguard your most critical assets.

Streamline endpoint and server security management

Managing breach prevention across endpoint and server security across various environments and multiple security tools can be complex, time-consuming, and prone to errors. Critical Start MDR services for Defender for Servers integrates seamlessly with other Critical Start MDR services for Microsoft Security, like MDR for Defender for Endpoint simplifying endpoint and server security management, lessening the load on your security teams, providing a unified view of your security posture and streamlining security operations.

Enhanced threat detection with resolution of every alert

Detecting advanced and evolving threats in a timely manner is crucial for effective security. Critical Start MDR combines 24x7x365 expert threat detection, investigation, and response, enabling organizations to identify and mitigate threats quickly. Best of all, we leverage our platform.

Detect and investigate every alert.

Critical Start does this by ingesting Microsoft Defender for Servers alerts into the Cyber Operations Risk and Response™ Platform, the backbone of our MDR service. We compare alerts against known good behaviors in the Trusted Behavior Registry® (**TBR**) where playbooks auto-resolve known good incidents. Alerts not identified by the TBR are escalated for investigation to the SOC where our experts can help you make more accurate, context and criticality-based decisions and take response actions on your behalf.Best of all, we stand at your side and work with you until remediation is complete.

CRITICALSTART®