

SOLUTION QUICK CARD

CRITICALSTART® Managed Detection and Response Services for VMware Carbon Black Endpoint and Enterprise Endpoint Detection and Response

KEY BENEFITS

- ✓ **Increase team efficacy**
Rely on 24x7x365 threat detection and response security expertise at your side or on the go with our MOBILESOC® app
- ✓ **Guaranteed quick response**
Contractual SLAs of 10-minute notification for Critical alerts and a 60-minute or less Median Time to Resolution (MTTR) for all alerts, regardless of criticality
- ✓ **Ensure security controls are in place and working**
Endpoint Coverage Gaps ensures all expected threat signals are received
- ✓ **Focus only on true-positives**
Fewer false positives over time results in reduced alert fatigue and enables your team to prioritize true-positive alerts
- ✓ **Reduce risk & improve security posture**
Expanded detection, mapped to the MITRE ATT&CK® Framework
- ✓ **Increase in-house SOC efficiency & productivity**
Between our CORR platform, Risk & Security Operations Center (RSOC) analysts, and threat intelligence experts, we do all the heavy lifting for you

At Critical Start, we take a risk-based approach to Managed Detection and Response (MDR) to prevent breaches and stop business disruption. With **24x7x365** expert security analysts at the ready, the only technology in the industry that resolves every alert regardless of criticality, and threat detections and intelligence from our Cyber Research Unit (CRU) continuously added to your VMware Carbon Black security tool, we help you reduce cyber risk and increase your security posture.

Solution

Critical Start MDR Services for VMware Carbon Black allows you to:

- Ensure security controls are in place and working as expected
- Investigate and respond to threats to prevent breaches
- Increase Security Operations Center (SOC) efficiency
- Boost the effectiveness of your security tools to mature your VMware Carbon Black investment

How it works

Every alert is ingested from VMware Carbon Black into our **Cyber Operations Risk & Response™ (CORR) platform**, the backbone of our MDR service. Alerts are compared against known good behaviors in the **Trusted Behavior Registry® (TBR®)** where playbooks auto-resolve known good alerts. Alerts not identified by the TBR are escalated to the Critical Start **RSOC** for further enrichment and investigation enabling you to make a more accurate decision on which response action to take. Critical Start can take response actions on your behalf and we work with you until remediation is complete.

