# CRITICAL**START**®  Managed Detection and Response (**MDR**) Services for Trend Micro Vision One™ for Endpoint

## KEY BENEFITS

✓ **Ensure security controls** coverage for endpoint

✓ **Optimize security investments** with an immediate reduction in false positives on the first day of production monitoring

✓ **Reduce risk exposure** with the resolution of more than 99% of endpoint OATs, escalating less than 0.01% to you

✓ **Decrease complexity** by bringing together conceptual insights across multiple security tools

### Strengthen Endpoint Security

Get the most out of your Trend Micro Vision One solution with Critical Start's risk-based approach to MDR. With **24x7x365** monitoring, investigation, and response, we help you rapidly identify and neutralize true threats and resolve every Observed Attack Technique (**OAT**).

### What you can rely on

Trend Micro Vision One customers using multiple best-of-breed security tools can rely on the consolidated interface of the **Critical Start Cyber Operations Risk & Response™ platform** dashboard to augment the efficacy and efficiency of their in-house Security Operations Center (**SOC**) personnel.

Take advantage of:
- 24x7x365 threat detection and guided response by our U.S.-based Risk & Security Operations (**RSOC**) analysts
- Actionable insights and the knowledge that all of your endpoints have security agent coverage
- Increased risk awareness with a unified Cyber Risk Dashboard
- Improved detection effectiveness with detections mapped to the **MITRE ATT&CK® Framework**

### How it works

Every endpoint OAT is ingested into our Cyber Operations Risk and Response™ platform, the backbone of our MDR service. Our purpose-built Trusted Behavior Registry® (**TBR®**) filters out known-good events, and any remaining OATs not identified by the TBR are escalated for investigation by our RSOC. After a two-person integrity review on any action to be taken, our security experts will work alongside you until remediation is complete or can even take response actions on your behalf.



CRITICAL**START**® Cyber Research Unit

MITRE ATT&CK® Framework-based IOCs

CRITICAL**START**®
Risk & Security
Operations Center

Apex One

Cloud One

Vision One

XDR Sensor

100%
of Alerts

Workbench
synchronization

Cyber Operations Risk & Response™ platform

Trusted
Behavior
Registry

Resolve false positives. Over 99.9% of alerts

● *False positives*        ● *Unknown alerts*

Critical Start
Security Analyst

1% of Alerts

Update the TBR
and IOCs

0.01%
True Positives
Excalated

MOBILE**SOC**®

Customer
Analyst

INCIDENT RESPONSE
Critical Start,
Customer or
Partner