TREND MICRO™

Securing Your Connected World

WHAT IS TREND MICRO™ MANAGED XDR?

24x7 Monitoring and Detection

Continuous alert monitoring and prioritization, using automation and analytics. Proactive indicators of compromise (IoC) sweeping of email, endpoints, servers, cloud workloads, and networks.

Rapid Investigation and Mitigation

In-depth investigation and a detailed response plan, with remote response actions through Trend Micro solutions.

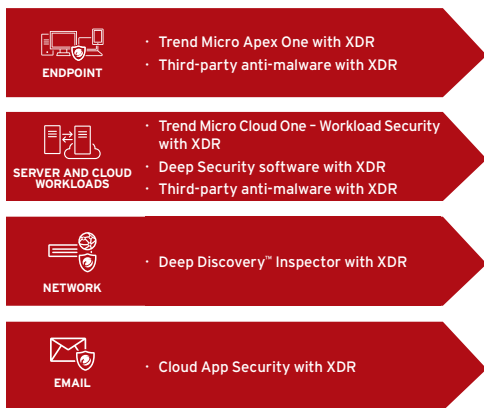### Expert Threat Identification and Hunting

Complex targeted threats uncovered utilizing cutting-edge techniques and Trend Micro security experts.

MANAGED XDR SERVES MULTIPLE CUSTOMER OBJECTIVES

The customer is:

- Looking for detection and response that can be managed on their behalf
- Looking to supplement in-house activities (augment detection, added threat expertise/ intelligence, proactive threat hunting)
- Concerned about having an incident and wants 24/7 alert monitoring
- Using multiple Trend Micro solutions and wants the benefits of extended detection and response—the XDR advantage

Why Trend Micro?

Breadth of Layers

- Monitors and correlates more threat vectors for better detection
- Provides broader context to uncover complex targeted attacks

Techniques and Analytics

- Leverages expert rules, machine learning, and security analytics to quickly distill alerts down to events that require investigation
- Managed XDR customers benefit from being the first to use new techniques being developed for Trend Micro solutions

Threat Expertise and Intelligence

- Managed XDR operations teams are made up of Trend Micro employees possessing various types of expertise, with rich experiences within threat research, threat response, and technical support
- This service leverages the Trend Micro™ Smart Protection Network™ and threat researchers across 15 global threat research centers, sharing a deep collective knowledge of threat techniques and actors

Security Layer Options

ENDPOINT
- Trend Micro Apex One with XDR
- Third-party anti-malware with XDR

SERVER AND CLOUD WORKLOADS
- Trend Micro Cloud One – Workload Security with XDR
- Deep Security software with XDR
- Third-party anti-malware with XDR

NETWORK
- Deep Discovery™ Inspector with XDR

EMAIL
- Cloud App Security with XDR

Service Components and Deliverables

ANALYTICS AND AUTOMATION

Threat Intelligence | Expert Rules | Machine Learning

SOC ANALYSTS

MONITORING AND DETECTION

ANALYSIS AND INVESTIGATION

RESPONSE

Standard

Advanced

HOW IT WORKS

PROACTIVE

REACTIVE

ALERT MONITORING | INITIAL ANALYSIS | INVESTIGATION | RESPONSE

STANDARD SERVICE

24/7 alert monitoring → Investigate if the alert is noteworthy or not → Evaluate the impact of the incident within the organization → Initiate response, deliver global protection updates

Regular sweeping for new IOCs

If the alert is relevant, determine if the host has any history of abuse → Interpret the root cause chain, and determine threat profile → Provide remediation recommendations, create clean up toolkits (if required), incident report

Hunting for new IOAs

Perform advanced investigation → Monitor infection for reoccurance

ADVANCED SERVICE

Send alert(s) to customers