Trend Micro™

XDR - MANAGED DETECTION AND RESPONSE SERVICE

Monitor endpoint, email, network, and server data, prioritize alerts.

Organizations are increasingly facing stealthy targeted attacks, designed to bypass existing security defenses. These attacks can monetize stolen intellectual property, encrypt essential data for ransom, or damage the flow of information in the case of nation state attacks. Advanced threat detection tools such as endpoint detection and response (EDR) and network threat detection are effective methods for identifying attacker behavior. However, correlating and prioritizing seemingly innocuous alerts and detections from multiple sources can be a time-consuming task and requires cybersecurity skills that are difficult and expensive to find.

Trend Micro managed detection and response (MDR) service detects and responds to threats across email, endpoints, servers, cloud workloads and network, helping organizations mitigate threats while alleviating overburdened security teams. This is accomplished by using patented big data artificial intelligence (AI) techniques and expert threat intelligence, helping detect threats that may previously have been identified as "grey alerts" by themselves. Trend Micro threat researchers investigate further to determine the extent and spread of the attack through a detailed root cause analysis, working with customers to provide a detailed response plan.

KEY FEATURES

Managed XDR for Endpoints

- Managed XDR uses a lightweight agent that combines our endpoint protection solutions with Trend Micro EDR to provide a detailed recording of system behaviors and events at the kernel and user levels. MDR tracks these events in context across time, providing an in-depth history that can be accessed in real time. The service also monitors server environments on a 24/7 basis to identify specific sources of threats.

Managed XDR for Cloud Workloads

- Trend Micro™ Deep Security™ provides comprehensive security in a single solution that is purpose-built to protect your virtual, cloud, and container environments. Deep Security provides a broad range of security capabilities to protect against vulnerabilities, malware, and unauthorized changes, ensuring consistent protection regardless of the workload. Deep Security can send server activity metadata and file integrity monitoring data to the Trend Micro Managed XDR service for correlation and visibility across physical, virtual, and cloud workloads.

Managed XDR for Networks

- Trend Micro™ Deep Discovery™ Inspector is a network appliance that monitors all ports and over 100 different network protocols to discover advanced threats and targeted attacks moving in and out of the network and laterally across it. The appliance detects and analyzes malware, command and control (C&C) communications, and evasive attacker activities that are invisible to standard security defenses. Alerts are sent directly to the MDR service, while recorded metadata is collected and queried by the MDR service as needed.

Managed XDR for Messaging

- Trend Micro™ Cloud App Security is a cloud-based advanced threat protection service that secures email and cloud file sharing in Microsoft® Office 365®, Gmail, Box, Dropbox™, and Google Drive™. By using Cloud App Security, Trend Micro Managed XDR service can "sweep" or search through Office 365 for indicators of compromise (IoCs). Most advanced threats start with a phishing email, so combining advanced email protection with the ability to trace a threat to its entry point is an effective defense against the latest in email threats.

MANAGED DETECTION AND RESPONSE (MDR) GIVES YOU:

- 24/7 monitoring and investigation of alerts
- Big data correlation of events, alerts, and network data to identify potential advanced attacks, using AI and patented technology
- Proactive threat hunting as needed to validate dynamically evolving zero-day threats
- Access to an advanced team of security experts skilled in investigating advanced threats, determining the severity of any incidents, and providing actionable remediation plans and guidance
- Root cause analysis to provide an understanding of how the attack was initiated, spread, and which devices were affected

Event monitoring and alerting

- Trend Micro Managed Services will monitor the customer's XDR deployment 24/7 and will remotely investigate all critical security events using data available in the monitored products. Real-time events from endpoint and network security will be continuously sent to the Trend Micro security operations center (SOC) via event logs and alerts. If a critical event is detected and validated it will be escalated to the customer for action.

Advanced correlation

- By correlating threat data from multiple sources such as endpoints, email, networks, and servers, a clearer picture is available to determine the source and spread of advanced attacks. Trend Micro Managed XDR service can even recognize internet of things (IoT) devices or unmanaged endpoints (such as BYOD devices) that may have been compromised, making use of advanced AI to analyze and prioritize threat data.

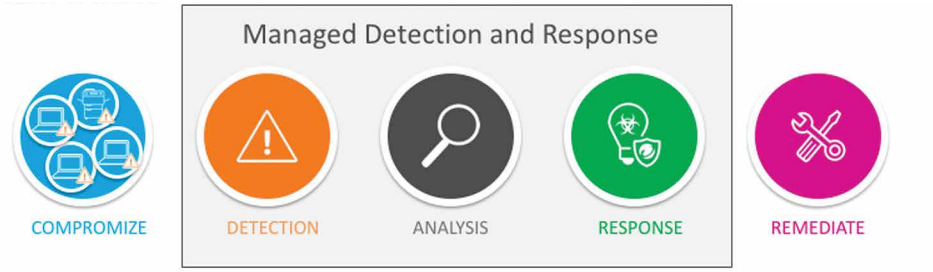
Reports

- For investigated customer threat alerts, Trend Micro reports information through incident cases, which contain details of the threat, including affected hosts, indicators of compromise (IoCs), and recommended mitigation options–wherever possible. Trend Micro also provides monthly reports to summarize case activity from the preceding month. All cases and reports are published to the Trend Micro Customer Success Portal, as well as emailed to desired recipients through the standard case support system.

Service reviews

- Trend Micro provides an opportunity for a formal service performance review at least once per month. This review examines service performance, significant events and incidents, faults and cases, change requests and execution, and recommendations.

HOW IT WORKS



DETECTION

Within an organization, endpoint sensors record system activities and behaviors and sends metadata about these recording–as well as endpoint alerts and detections–to the Managed XDR service. Network security records the network data and sends metadata to the MDR service, as well as network security alerts and detections. Server security is also monitored, as logs are sent to the service. Office 365 is also monitored, with alerts being sent to the Managed XDR service. Using advanced AI, these alerts are correlated and analyzed through the Trend Micro™ Smart Protection Network™. The resulting correlated alerts are prioritized, while notifications are sent to the Trend Micro SOC.

ANALYSIS

An incident response staff investigates the specific threats by gathering additional information (with customer approval though their management console) to determine vulnerabilities, understand what else may have been downloaded, or if the original threat has mutated and spread. The analyst investigates to determine the full root cause analysis and potential impact to the affected customer.

RESPONSE

A report is provided to customers about the incident, including recommendations on how to respond and remediate from the attack where appropriate. In some cases, tools may be provided to assist with the remediation.

Available for	Endpoints		Network		Cloud Workloads		Messaging		
	Trend Micro Apex One™ and Endpoint Sensor*		Trend Micro Deep Discovery Inspector		Trend Micro™ Deep Security™		Trend Micro™ Cloud App Security for Office 365		
	Std.	Adv.	Std.	Adv.	Std.	Adv.	Std.	Adv.	
Detection									
24/7 critical alerting and monitoring	O	O	O	O	O	O	O	O	MDR team will continuously monitor the logs for new critical alerts, investigate via automated or manual means, and deliver details on the threat. You can define the escalation path for the MDR team based on critical assets and other criteria.
IOC sweeping	O	O	O	O	O	O	O	O	The MDR team will sweep your environment's metadata stores for newly identified IoCs, including those shared via US-CERT and other third-party disclosures that Trend Micro receives.
Root cause analysis	O	O							Using the endpoint data, the MDR team will generate a root cause analysis, which shows the attack vector (email, web, USB, etc.), dwell time, and the spread and impact of the attack.
Threat source identification					O	O			If a customer is using containers, the MDR team can help identify the container with the discovered threat.
Investigation									
Incident prioritization		O		O		O		O	Using threat knowledge and customer shared environment data, the MDR team will help to prioritize which alerts or threats need to be handled first. The team escalates threats to specific high-value endpoints as requested by the customer.
Impact analysis		O		O					A new threat/IoC in a customer's environment is checked against the metadata stores to assess if that file is on any other protected system and what other systems may be compromised.
Suspicious User Activity Tracking								O	Investigate unusual user account activity that could signify a compromised account, such as spamming: sudden and large volume of outbound emails.
Container identification						O			Identify what container a specific attack originated from and/or what container(s) was targeted.
On-demand health check		O							Customers can request an aggressive endpoint scan, which uses the latest threat intel to scan for potential threats. This in-depth process is invasive, scans the endpoints themselves, and can affect their performance during the scan.
Response									
Access to MDR analysts		O		O		O		O	Customers will be able to speak to the MDR security analysts for further details or clarification beyond the report.
Threat response		O		O		O		O	To the best of their ability, the MDR team will provide detailed remediation options and, as applicable, custom cleanup tools to help recover from the threat. This includes, for messaging, the ability to lock out compromised accounts and remove IoC-matched emails.
Executive summary report – monthly		O		O		O		O	The MDR team will provide an executive summary outlining the services provided over the specific time period, including IoC sweeps completed, alerts handled, etc.
Executive summary report – quarterly	O		O		O		O		The MDR team will provide an executive summary outlining the services provided over the specific time period, including IoC sweeps completed, alerts handled, etc.

* SaaS version of Endpoint Sensor supports Microsoft® Windows® and Linux® servers.

TREND MICRO™

Securing Your Connected World

For details about what personal information we collect and why, please see our Privacy Notice on our website at:
https://www.trendmicro.com/privacy