Trend Micro™

MANAGED XDR - MANAGED DETECTION AND RESPONSE SERVICE

Expert Threat Detection, Investigation, and Hunting

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 extended detection and response (XDR), are effective methods for identifying and responding to attacker behavior. However, even with the right solution, security teams still struggle with constrained resources. They can gain tremendous value by leveraging a service to augment detection capabilities, add threat expertise/intelligence, and ensure proactive threat hunting and regular sweeping for indicators of compromise (IoC).

Trend Micro is the only vendor that can use its native security stack to offer an integrated managed service across email, endpoints, servers, cloud workloads, and networks. Our managed detection and response service, Trend Micro™ Managed XDR, drives unparalleled improvements in security teams' time-to-detect and time-to-respond, while minimizing the risks and impact of threats.

KEY FEATURES

Multiple Vectors

Customers can choose to monitor email, endpoints, servers, cloud workloads, and/or network security solutions:

- **Email** pprotected by Trend Micro™ Cloud App Security for Microsoft® Office 365™ or Google G Suite™.
- **Endpoints** with Trend Micro Apex One™ multi-layered endpoint security.
- **Servers and cloud workloads** protected by Trend Micro™ Deep Security™ or Trend Micro Cloud One™ – Workload Security (virtual, physical, cloud, and containers).
- **Networks** equipped with Trend Micro™ Deep Discovery™ Inspector, providing advanced network detection across over 100 protocols and all network ports.
- **Endpoints/servers** with third-party anti-malware solutions who have purchased Trend Micro Vision One™ (XDR).

Trend Micro offers standard or advanced services for one or all of the security layers above. An added advantage of the service is the ability to correlate alerts and activity data from multiple solutions—leading to better detection.

Detection

- 24/7 alert monitoring, correlation, and prioritization—using automation and analytics—quickly distills alerts down to the events which need further investigation.
- Continuously sweeps customer environments for newly identified indicators of compromise (IoCs) or indicators of attack (IoAs)—including those discovered in other customer environments or shared via US-Cert or other third-party disclosures that Trend Micro receives.
- Service capitalizes on Trend Micro product differentiators and ensures customers get the most out of their solutions' detection capabilities.
- The managed detection and response (MDR) service is the first-user of any new detection techniques being developed for Trend Micro solutions, so Managed XDR customers benefit first from the latest technologies.

Managed XDR gives you:

24/7 monitoring and detection

- Continuous alert monitoring, correlation, and prioritization using automation and analytics. Proactive sweeping of email, endpoints, servers, cloud workloads, and networks.

Rapid investigation and mitigation

- Comprehensive analysis and detailed response plan with remote response actions through Trend Micro solutions.

Expert threat identification and hunting

- Uncovering of complex targeted threats using cutting-edge techniques—with enrichment by threats experts leveraging deep threat intelligence.

Investigation

- Trend Micro experts create a full picture of the attack across the entire enterprise by generating root cause analysis to show the attack vector, dwell time, spread, and impact of the attack.
- Analysts are able to synthesize data to derive insights while leveraging Trend Micro™ Smart Protection Network™, as well as threat researchers across 15 global threat research centers—who have a deep collective knowledge of threat techniques and actors.
- Customers can work directly with Trend Micro security analysts during the investigation and response process.

Response

- Product response options are initiated to contain threats and automatically generate IoCs to prevent future attacks.
- Service provides a step-by-step response plan on actions needed to remediate and, as applicable, custom clean-up tools to help recover from the threat.
- Continually sweeps the enterprise to ensure the customer's environment remains clear of any resurgence of the threat.

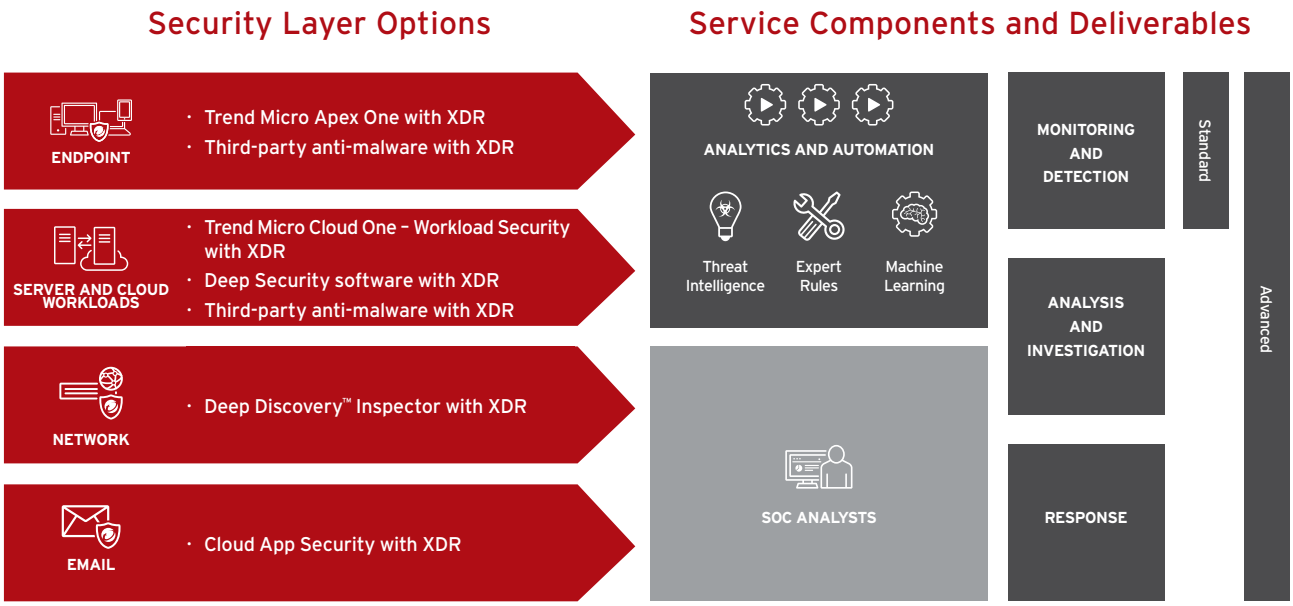
Reports

- For investigated customer threat alerts, Trend Micro reports information through incident cases which contain details of the threat, including affected hosts, 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 and are 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 quarter. This review examines service performance, significant events and incidents, faults and cases, change requests and execution, along with recommendations.

HOW IT WORKS



Managed XDR service benefits from the customers' use of Trend Micro Vision One™—an extended detection and response (XDR) platform. By leveraging the XDR data lake and the platform's analytical capabilities, the service offers added efficiencies around correlated detection and integrated detection and response.

Available for	ENDPOINT		NETWORK		SERVER AND CLOUD WORKLOADS		EMAIL		
	Std.	Adv.	Std.	Adv.	Std.	Adv.	Std.	Adv.	
Detection									
24/7 critical alerting and monitoring	O	O	O	O	O	O	O	O	Managed XDR 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 Managed XDR team based on critical assets and other criteria.
IoC sweeping	O	O	O	O	O	O	O	O	The Managed XDR 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			O	O			Using data, the Managed XDR 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.
Investigation									
Incident prioritization		O		O		O		O	Using threat knowledge and customer shared environment data, the Managed XDR team will help to prioritize which alerts or threats need to be handled first. The team escalates threats to specific high-value hosts as requested by the customer.
Impact analysis		O		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	Customers can investigate unusual user account activity that could signify a compromised account, such as spamming, where there is a sudden and large volume of outbound emails.
On-demand health check		O*							Customers can request an aggressive endpoint scan, which uses the latest threat intel to scan for potential threats.
Response									
Access to Managed XDR analysts		O		O		O		O	Customers will be able to speak to the Managed XDR security analysts for further details or clarification beyond the report.
Threat response		O		O		O		O	The Managed XDR team will provide applicable product response options and, as applicable, custom cleanup tools to help recover from the threat.
Executive summary report – monthly	O	O	O	O	O	O	O	O	The Managed XDR team will provide a monthly executive summary outlining the services provided over the specific time period, including IoC sweeps completed, alerts handled, etc.

* Not applicable for customers using third-party anti-malware solution instead of Trend Micro Apex One.

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

TREND MICRO™

Securing Your Connected World