NETCorp IT SOLUTIONS

WHAT IS TREND MICRO™ MANAGED XDR?

TREND MICRO™

24x7 Monitoring and Detection

Continuous alert monitoring and prioritization, using automation and analytics. Proactive 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 products

Expert Threat Identification and Hunting

Uncover complex targeted threats using cutting-edge techniques and Trend Micro security experts

Managed XDR serves multiple objectives

- If you are concerned about having an incident and wants 24/7 alert monitoring
- If you want the threats to be analyzed in-depth to prevent them from recurring
- If you want the world's top security experts for the cost of a anti-virus product
- Using multiple Trend Micro products and wants the benefits of cross-layered detection and response—the XDR advantage

Why Trend Micro?

Breadth of Layers

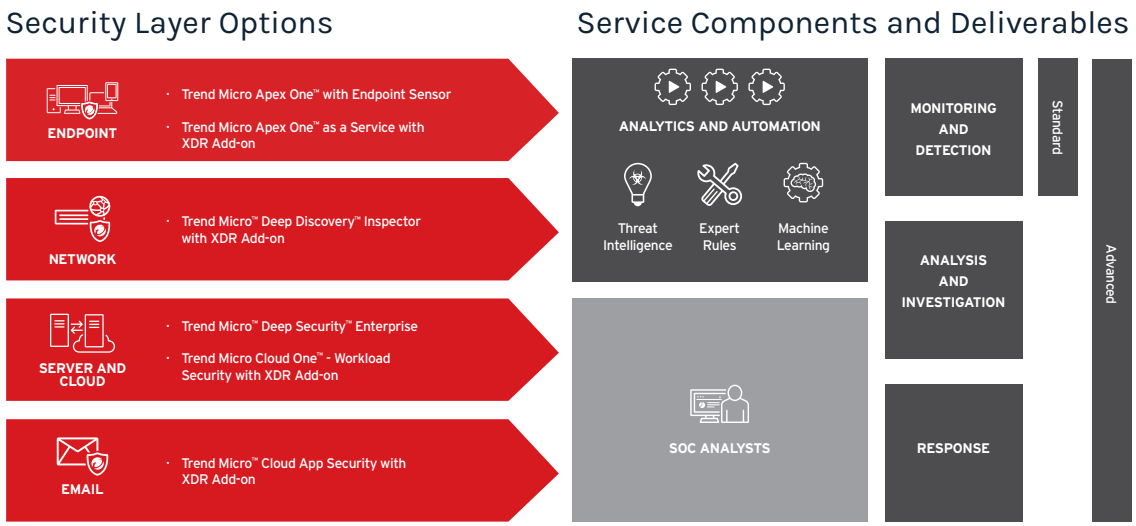
- Monitors and correlates more threat vectors for better detection
- Provides broader context to uncover complex targeted attacks

Techniques and Analytics

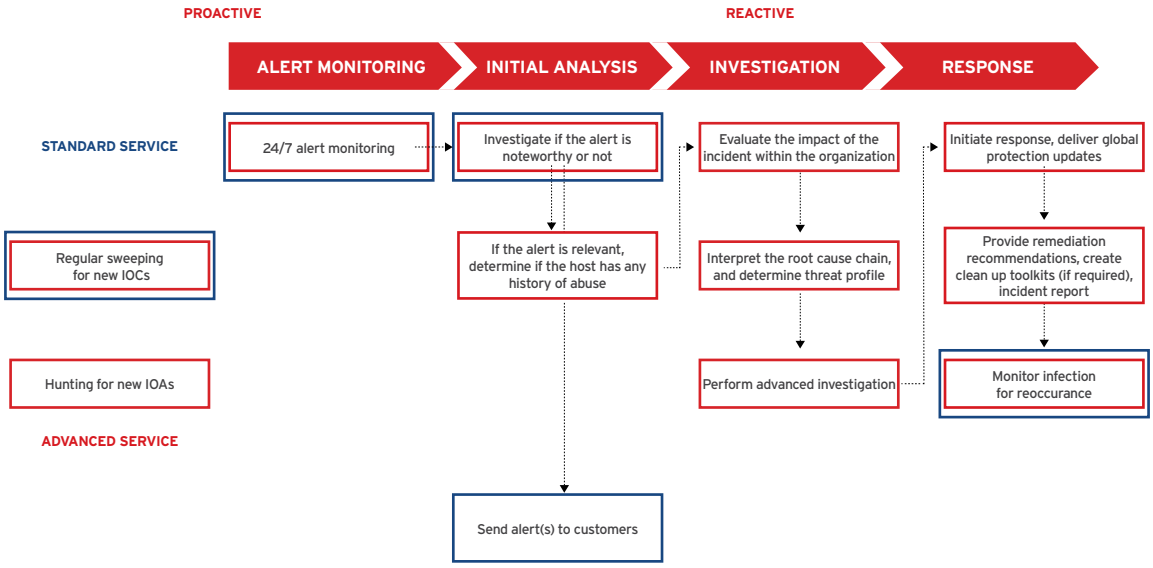
- Leverages expert rules, machine learning, and security analytics to quickly distill alerts down to events that need investigation
- Managed XDR customers benefit from being the first to use new techniques being developed for Trend Micro products

Threat Expertise and Intelligence

- Managed XDR operations team are all Trend Micro employees with various types of expertise and rich experience within threat research, threat response, and technical support
- The service leverages the Trend Micro™ Smart Protection Network ™ and threat researchers across 15 have a deep collective knowledge of threat techniques and actors.



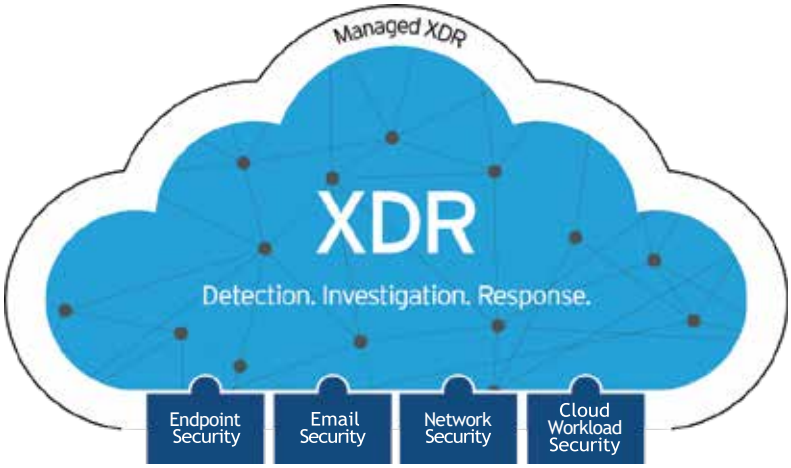
How it works



XDR is ideally suited for customers who struggle with the following:

- Are security conscious, but haven't achieved security maturity, in terms of having the proper processes in place.
- Constrained security expertise or resources— they may not have a full SOC, but have security analysts that are tasked with performing SOC-type responsibilities.
- May have a security information and event management (SIEM) in place, but it is not providing the actionable insights they expected.
- May have multiple disparate security solutions, including EDR, but are limited in their ability to integrate and combine information between data silos in each solution.

XDR provides a platform for companies in the scenarios above to gain the type of detection and response capabilities that have historically only been an option for large, mature SOC operations. In addition, the Managed XDR service is a great option for organizations who want the benefits of XDR and recognize the need and advantages of having Trend Micro resources help them fully capitalize on it.



What problems does XDR solve?

- Missed detections due to the abundance of alerts. SOC teams and analysts are overwhelmed with the number of threat alerts they see daily.
- XDR offers powerful detection rules to correlate multiple low confidence events, behaviors, and actions—across one or multiple security layers—to identify malicious activity and surface fewer higher-confidence alerts.
- Lack of visibility across the entire organization. Security analysts can't easily connect alerts they see across disparate solutions to identify and investigate a targeted attack.
- The XDR approach delivers better, faster detection and response across the customer's environment. XDR breaks down the silos and tells a complete story of the attack path, as opposed to using a SIEM or multiple point solutions that require security analysts, or SOC team to dig through noisy alerts and an abundance of logs to build it themselves. This improves the time to detect and time to respond to attacks.

What are the Key Differentiators of XDR?

1. Goes beyond the single vector approach to detection and response—combining investigations across email, endpoints, servers, cloud workloads, and networks.
2. Discovers more with correlated detection, which means multiple low-level alerts can be combined to surface higher-priority alerts with a high degree of confidence.
3. Provides integrated investigations and rapid response actions to stop complex threats faster and mitigate any damage across the organization.

FAQ

1. **I already have a Worry-free Advanced , I don't need the XDR platform.**
    a. XDR isn't meant to replace a solution, it's a complementary solution that can augment the security already in your environment. XDR will correlate and combine multiple alerts associated with the same incident, which means fewer higher-confidence alerts are sent to the SIEM—reducing the amount of triage effort required by security analysts.

2. **I don't want to rely on a single vendor for all my protection, detection, and response.**
    a. Having multiple vendors means having multiple management consoles and siloed views, which results in a lack of complete visibility throughout the entire security infrastructure. XDR offers a means for business to consolidate security products into a cohesive protection, detection, and response solution that is available without extensive integration efforts. Consolidation across Trend Micro products can offer operational efficiencies and reduce the level of complexity that having multiple solutions can present.

3. **I already have a different endpoint/cloud/network security solution, I am not ready to replace all those solutions to benefit from XDR.**
    a. While XDR benefits from the ability to provide true cross-layered detection and response by combining and correlating alerts across multiple security layers, there is huge value in having XDR for a single security layer (whether it be endpoints, email, servers, cloud workloads, or networks):

    i. XDR for Endpoints: Most attacks involve user devices; XDR allows you to find threats hidden amongst endpoint telemetry. With XDR for Endpoints, analysts can investigate attacks that happen on the endpoint, find out how it arrived on the endpoint, and how it propagated to other areas.

    ii. XDR for Networks: Sees any unmanaged endpoints that are not protected by next-gen anti-virus, as well as certain IoT, IIoT, and legacy devices. With XDR for Networks, analysts can investigate how an attacker moves across the organization and communicates with external sources.

    iii. XDR for Email: Monitors alerts that are detected in user emails. This security layer is very important, as 94% of malware starts at the email.1 With XDR for Email, analysts can determine who received the malicious email, and if there are any compromised accounts sending phishing emails and other threats.

    iv. XDR for Servers and Cloud Workloads: Monitors alerts found across server environments that are critical to business operations. With XDR for Servers and Cloud Workloads, analysts benefit from high-fidelity detections that can tell them what happened across their server workloads and container environments.

If you wish to learn further about Trend Micro XDR - I am just a call away

NETCorp IT SOLUTIONS

NETCorp IT Solutions
Unit3, 33 Archer Street, Carlisle, WA, 6101
+1800 951 054 sales@netcorp.net.au www.netcorp.net.au