Trend Micro™

# XDR

See what you've been missing

With today's ever-evolving threat landscape, advanced security is not enough to prevent attacks on your users and infrastructure. You need capabilities in place to help you respond rapidly to threats that may breach your defenses. To avoid serious and widespread damage, you need to prevent as much as you can and detect and respond quickly if a threat breaks through.

Today, many organizations use multiple, separate security layers to detect threats across their endpoints, servers, network, email, and cloud infrastructure, leading to siloed threat information and an overload of uncorrelated alerts. Investigating threats across all these disparate solutions makes for a very piecemeal and manual investigation process that can miss threats altogether due to lack of visibility and correlation. Many detection and response solutions only look at endpoints, missing threats that pass through user emails, the network, and servers. This results in a very limited view of the attacker's activities and an inadequate response.

Detection and response is a vital security requirement for all organizations, but the truth is, most organizations are resource and skillset constrained. Single-vector solutions make this problem more prevalent.

Trend Micro™ XDR collects and automatically correlates data across multiple security layers: email, endpoints, servers, cloud workloads, and networks. Using advanced security analytics, it detects and tracks attackers across these layers so security teams can quickly visualize the story of an attack and respond faster and more confidently. The efficiency of XDR allows resource-constrained security teams to do more with less and the Trend Micro™ Managed XDR service can augment teams with expert threat hunting and investigation.

## ADVANTAGES

### Beyond the Single Vector

Detect and respond to threats across multiple layers and gain greater context for better understanding.

- Automatically correlate data from native Trend Micro solutions' sensors that collect detection and activity data across email, networks, endpoints, and servers—eliminating manual steps
- Activity that may not seem suspicious on its own suddenly becomes a high-priority alert, allowing you to contain its impact faster
- Contain threats more easily, assess the impact, and action the response across email, endpoints, servers, cloud workloads, and networks

### Correlated Detection

Detect more with built-in security analytics combined with global threat intelligence.

- XDR analytics can automatically tie together a series of lower-confidence activities into a higher-confidence event, surfacing fewer prioritized alerts for action
- Correlate threat and detection data from your environment with Trend Micro™ Smart Protection Network™ for richer, more meaningful alerts
- More context with mapping to the MITRE ATT&CK framework for faster detection and higher fidelity alerts
- Gain new expert detection rules, based on what Trend Micro threat experts are finding in the wild

### Integrated Investigation and Response

One platform to respond faster with less resources.

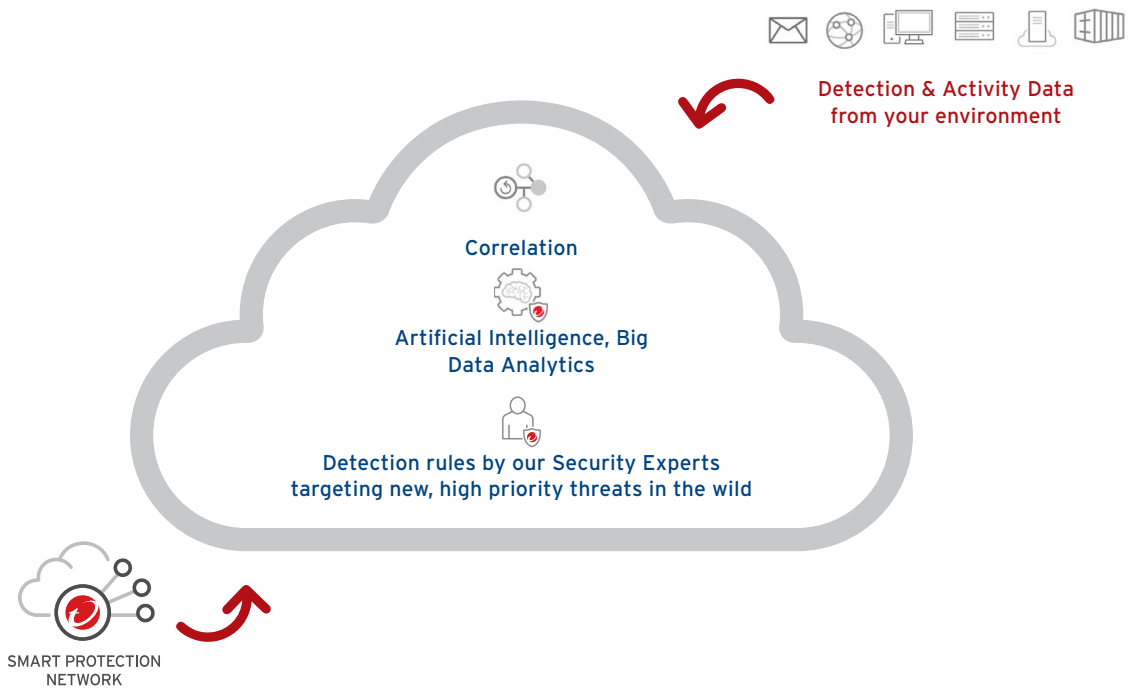
- One source of prioritized alerts, based on one expert alert schema to interpret data in a standard and meaningful way
- One place for investigations to quickly visualize the entire chain of events across security layers or drill down into an execution profile or network traffic analysis
- One location to respond using containment actions for email, endpoints, cloud/server workloads, and networks

## KEY BUSINESS ISSUES

- Stealthy threats continue to evade even the best defenses.
- Disconnected security layers with siloed tools and data sets make it difficult to correlate information and detect critical threats.
- Too many alerts and overloaded organizations don't have the time or resources to investigate.

"It is easier for my team to explain the attack and go through the sequence of events; **it's like reading a book**. Easier to digest."

Frank Bunton
CISO, MedImpact



## KEY BENEFITS OF XDR

### Prioritized view of threats across the organization:

By correlating threats across the organization and adding expert threat intelligence, AI, and big data analytics, security personnel will get fewer, more meaningful, and richer alerts—prioritized by severity.

### More effective analysis:

With native integration into email, endpoints, servers, cloud environments, and networks, XDR sensors benefit from a deep understanding of data sources. This results in more effective analytics, compared to having third-party integration through application programming interfaces (APIs).

### Clearer contextual view of threats:

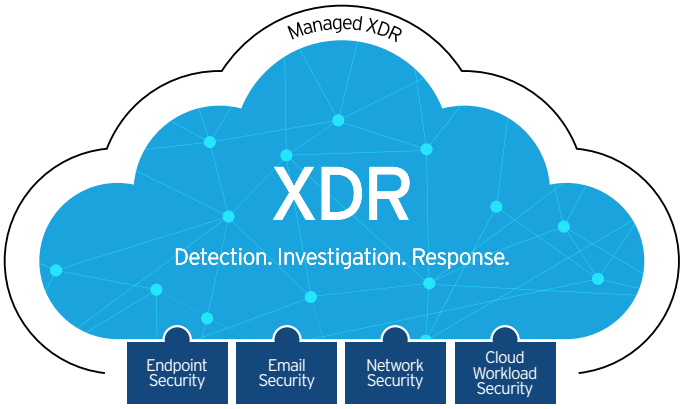
By viewing more contextual alerts across more threat vectors, events that seem benign on their own suddenly become meaningful indicators of compromise. This allows you to connect more dots into a single view, enables more insightful investigations, and gives you the ability to detect threats earlier.

### Reduces time to detect and stop threats:

Collapses the time it takes to detect, contain, and respond to threats, minimizing the severity and scope of impact.

### Increased effectiveness and efficiency of threat investigation:

By automatically correlating threat data from multiple sources, XDR speeds up and removes manual steps involved in investigations and enables security analysts to quickly find the story of an attack.




## TREND MICRO™ MANAGED XDR

### Alleviate security operations teams

With Managed XDR, customers can get the advantages of XDR and leverage the resources and knowledge of Trend Micro security experts for in-depth investigations into advanced threats and threat hunting using proprietary techniques.

Managed XDR provides 24/7 alert monitoring, alert prioritization, investigation, and threat hunting to Trend Micro customers as a managed service.

The Managed XDR service collects data from endpoints, network security, and server security to correlate and prioritize alerts and system information to determine a full root cause and impact analysis. Our threat investigators investigate on your behalf and can initiate respective product response options to contain threats while providing a step-by-step response plan on actions needed to remediate and custom cleanup tools to help recover from the threat, if applicable.

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