Trend Micro™

XDR

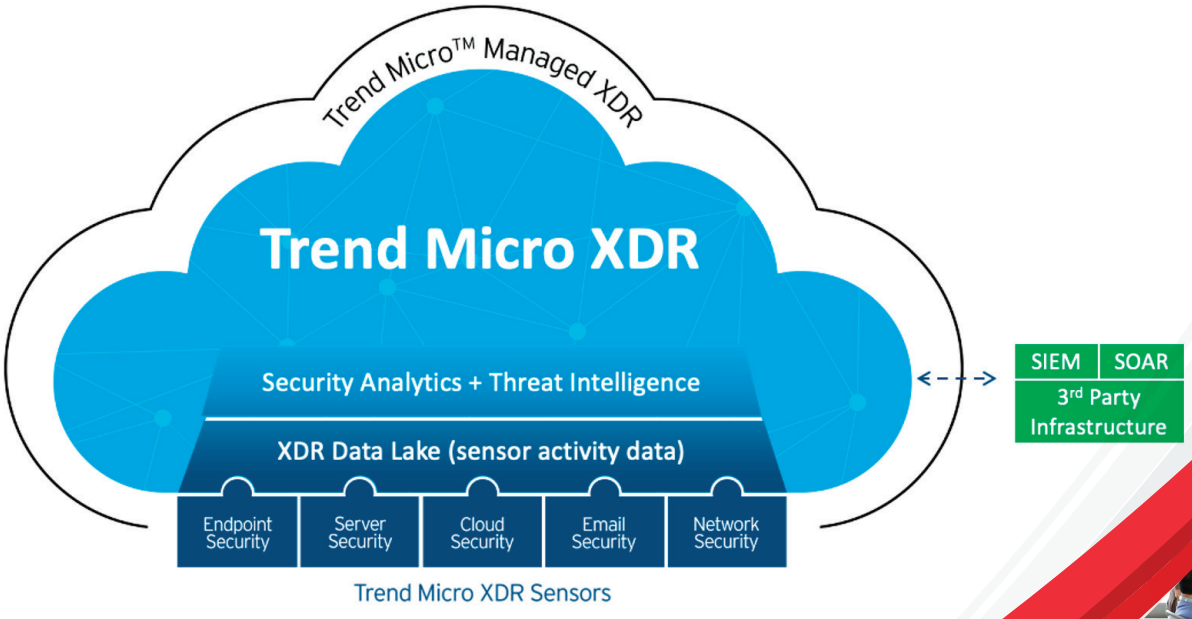
See more. Respond faster.

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, it is important 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 email, endpoints, servers, cloud infrastructure, and networks, 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, servers, cloud workloads, and networks. 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. Trend Micro quickly prevents the majority of attacks, with automated protection and XDR stitching together threat activity across layers to detect attackers. Security teams can quickly see the story of an attack and respond faster and more confidently. The efficiency of XDR makes great security teams even better by enabling them to do more with less. In addition, the Trend Micro™ Managed XDR service can augment teams with expert threat hunting and investigation.



ADVANTAGES

See More.

- **Comprehensive protection** - Trend Micro detection and prevention (including web reputation, application control, and IPS) automatically stops more attacks before they take hold.
- **More insight** - Pre-integrated, native sensors deliver deep activity data, not just detections, across email, endpoints, servers, cloud workloads, and networks.
- **Faster detection** – XDR automatically ties together a series of lower-confidence activities into a higher-confidence event, surfacing fewer, prioritized alerts for action and graphically presents the story of the attack.
- **More context, less noise** - Incorporating Trend Micro Threat Research insights together with MITRE ATT&CK mapping enriches detection and investigation to provide a deeper understanding.

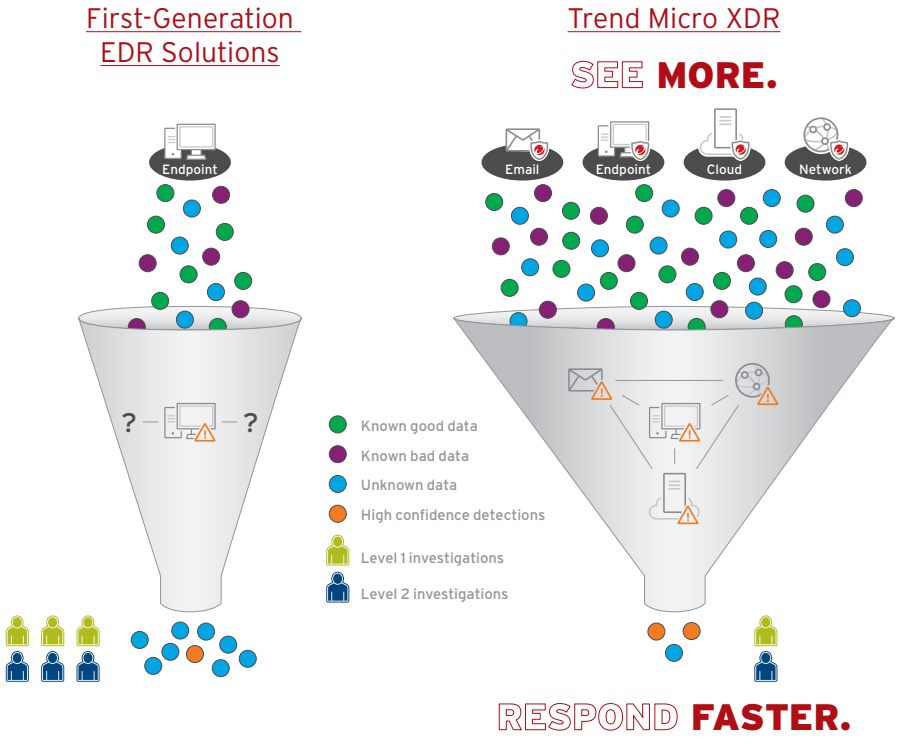
Respond Faster.

- **Timely** - New expert detection rules added regularly, based on what Trend Micro threat experts are finding in the wild. Automatic searching for new indicators of compromise (IoCs) with Trend Micro threat feed.
- **Faster investigation** - Quickly visualize the full attack story. XDR automatically pieces together fragments of malicious activity and paints a complete picture across security layers.
- **Automated** - Programmed protection layer remediation capabilities to deal with threats like ransomware (e.g. auto-restore any files damaged prior to detection) or to clean up malware automatically.
- **Complete response** - Contain threats more easily, assess the impact, and action the response across email, endpoints, servers, cloud workloads, and networks, all from within XDR.

Greater Security Team Efficiency.

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:

Organizations without an XDR approach ignore nearly double the security alerts as those with XDR capabilities1. XDR correlates and combines low level signals into high-fidelity alerts which tell the story of an attack. Security personnel can quickly understand where to focus efforts.

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). Organizations with an XDR approach suffered half as many successful attacks[1].

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.

Stops more attacks, quicker:

The net of XDR is better protection for your organization through earlier detection and faster response. According to ESG, those with XDR are 2.2 times more likely to detect a data breach or successful attack in a few days or less, versus weeks or months for those without[2].

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. ESG found that organizations with an XDR approach respond more completely to attacks and were 60% less likely to report that attack re-propagation had been an issue[3].

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. Organizations with an XDR approach stated it would take eight full time employees to replace the data correlation capabilities of XDR and also are 2.6 times less likely to report their team is overwhelmed[1].

TREND MICRO™ MANAGED XDR

Alleviate security operations teams

Managed XDR provides 24/7 alert monitoring, alert prioritization, investigation, and threat hunting to Trend Micro customers as a managed service. Customers get the advantages of XDR and leverage the resources and knowledge of Trend Micro security experts. This provides teams with in-depth investigations into advanced threats and threat hunting via proprietary techniques.

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.

1 - The XDR Payoff: Better Security Posture, ESG Research, Sep 2020
2 - The XDR Payoff, ESG Research
3 - The XDR Payoff, ESG Research

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