Trend Micro™

XDR

See what you've been missing

With today's ever-evolving threat landscape, it's not enough to just have advanced security protecting your users and infrastructure, you need capabilities in place to help you respond rapidly to threats that may breach your defenses. Despite having layers of advanced protection, there is no such thing as 100 percent prevention, it only takes a single threat to make it through for your organization to be 100 percent at risk. To avoid serious and widespread damage, your goal needs to be; prevent as much as you can, and detect and respond quickly if a threat does break through.

Many organizations today 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 threats with little means to correlate and prioritize them. 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–and therefore miss threats that enter through user emails, the network, and servers–resulting in a very limited view of the breach and provides an inadequate response. To have a true picture of threats affecting your entire organization it's important to have native integration into detection and response functions across email, server, network, cloud workloads, as well as the endpoint.

Detection and response is a vital security requirement for all organizations, but the truth is most organizations are resource and skillset constrained. Modern detection and response currently requires a significant amount of time and dedicated expert resources that most organizations don't have.

Trend Micro XDR extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With XDR, customers can respond more effectively to threats, minimizing the severity and scope of a breach.

ADVANTAGES

AI and Expert Security Analytics

Built-in threat expertise and global threat intelligence to detect more:

- Combine threat and detection data from your environment with Trend Micro's global threat intelligence in the Trend Micro™ Smart Protection Network™ for richer, more meaningful alerts
- More context means faster detection and higher fidelity alerts
- Optimal AI and big data analytics provide you with a deeper understanding of data collected from Trend Micro's intelligent sensors
- Gain the power that only humans can bring to bear with new expert detection rules based on what from Trend Micro threat experts are finding in the wild

Beyond the Endpoint

Detect and respond to threats across multiple layers and gain greater context to understand better:

- Automatically correlate data from sensors from native Trend Micro solutions that collect detection and activity data across email, network, endpoint, 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, endpoint, server, cloud workloads, and network

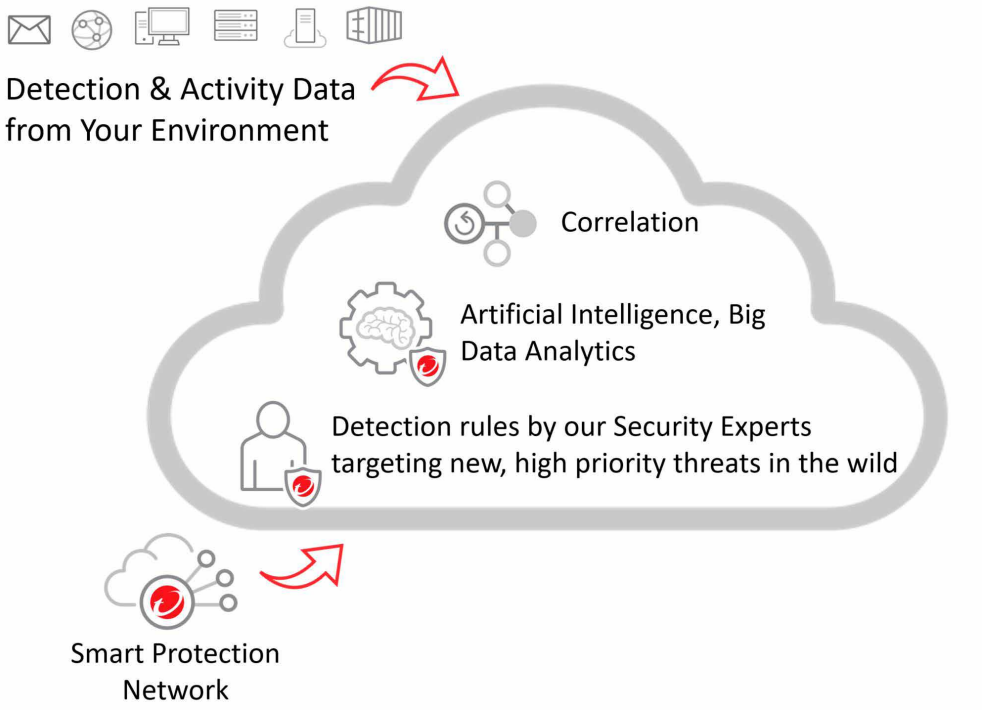
Complete Visibility

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 consolidated view to uncover events and the attack path across security layers
- ONE source for guided investigations to understand the impact and identify the path to resolution

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



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.

Increased effectiveness and efficiency of threat investigation:

By automatically correlating threat data from multiple sources, Trend Micro XDR speeds up and removes manual steps involved in investigations and enables detailed analysis that can't be done today.

Clearer contextual view of threats:

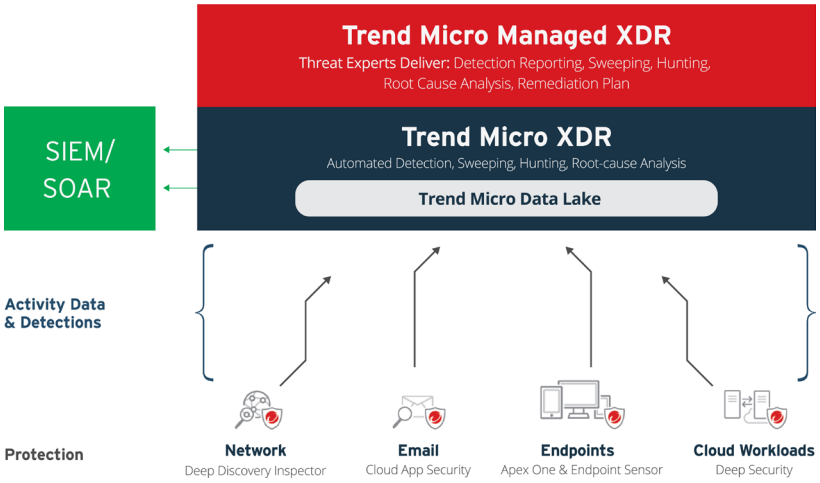
By viewing more contextual alerts across more threat vectors, events that seem benign on their own suddenly become meaningful indicators of compromise. This allows you to connect more dots into a single view, enable more insightful investigations, and gives you the ability to detect threats earlier.

Reduces time to detect threats:

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

More effective analysis:

With native integration into endpoint, email, server, network, and cloud environments, Trend Micro 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).



TREND MICRO™ MANAGED XDR

Alleviate security operations teams

With Managed XDR, customers can get the advantages of XDR; leveraging the resources and knowledge of Trend Micro security experts who are skilled in investigating advanced threats.

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

The MDR service collects data from endpoints, network security, and server security to correlate and prioritize alerts and system information and determine a full root cause analysis. Our threat investigators investigate on behalf of you and provide a full remediation plan.

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 Journey to the Cloud