

# TREND MICRO VISION ONE™

See more. Respond faster.

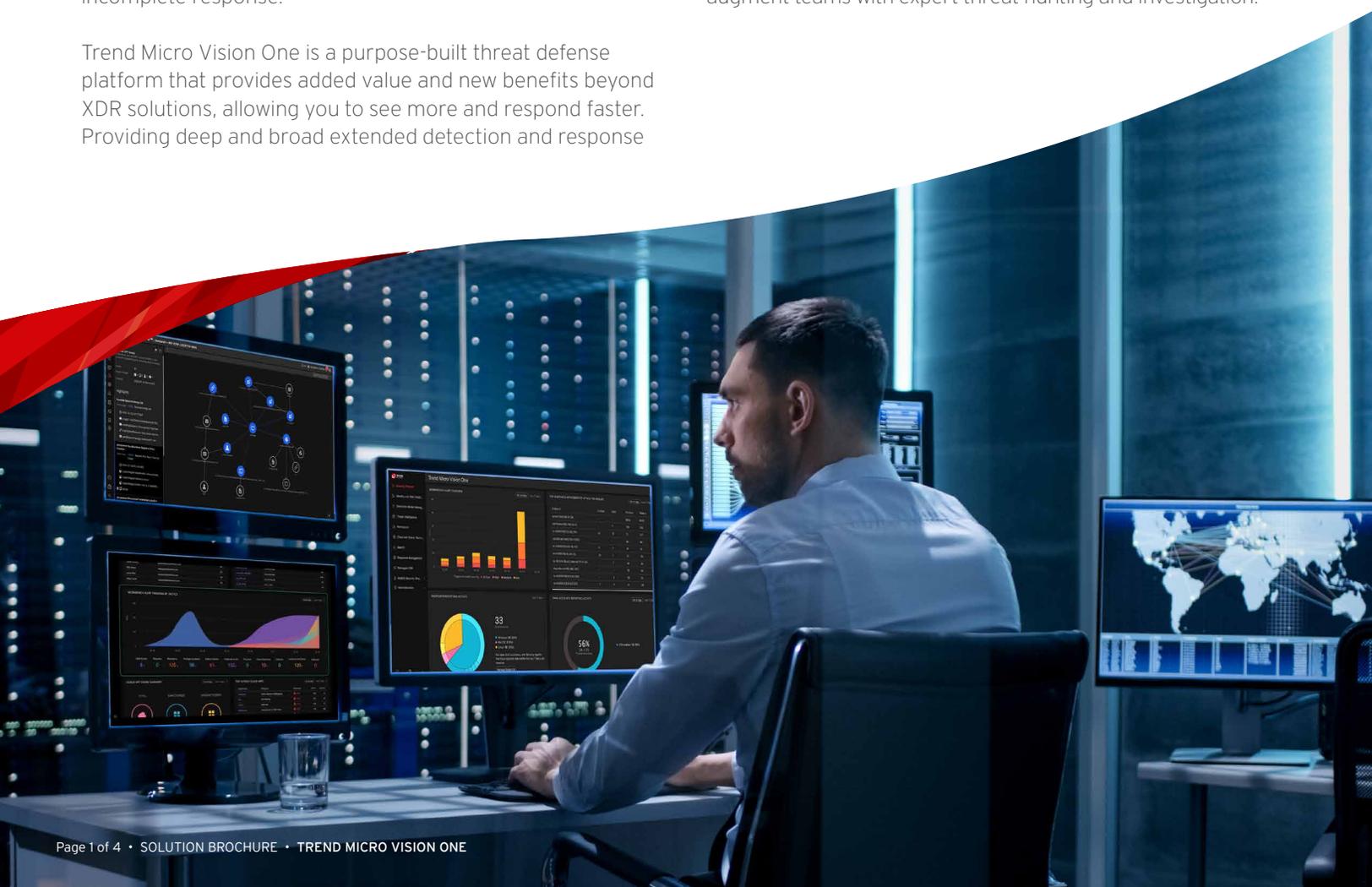
With today's ever-evolving threat landscape, you need capabilities in place to help you detect and respond rapidly to threats that may breach your defenses. Today, many organizations use multiple, separate security layers to detect threats across their email, endpoints, servers, cloud infrastructure, 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, incomplete response.

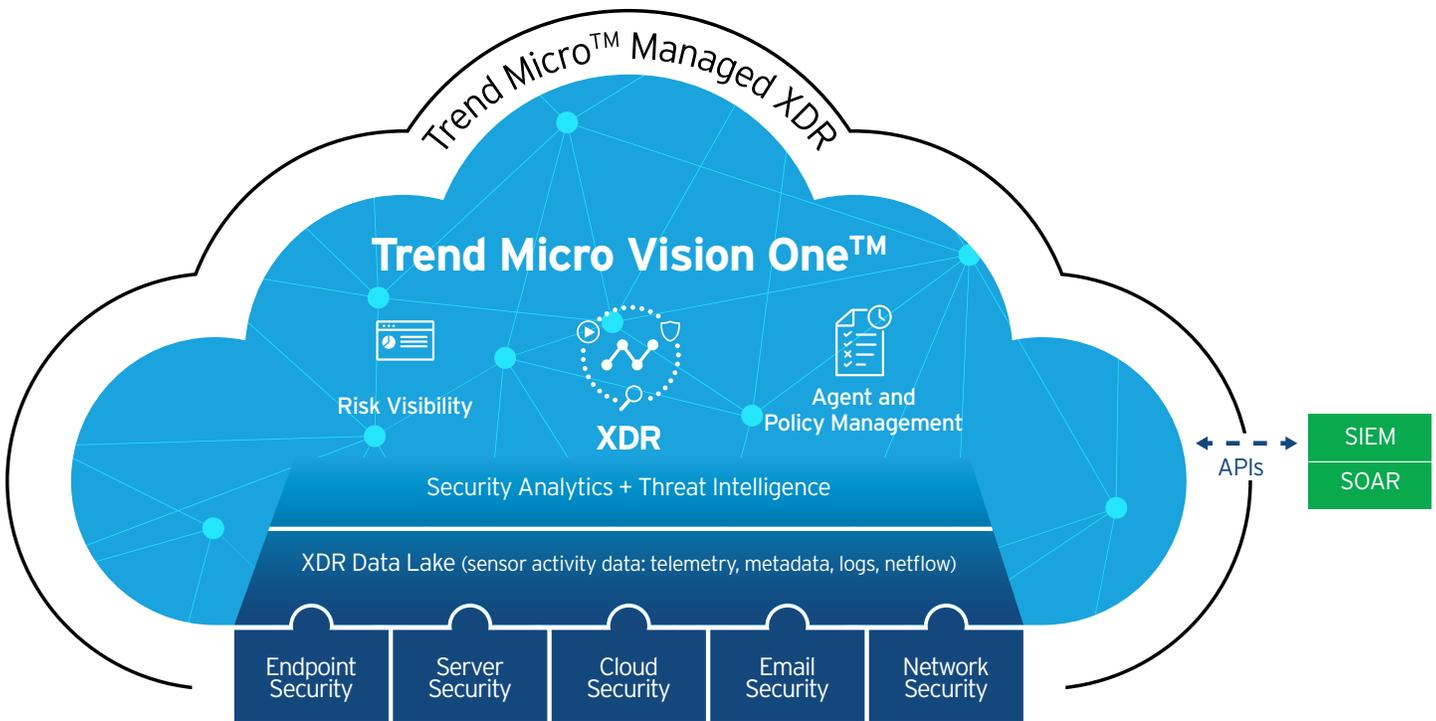
Trend Micro Vision One is a purpose-built threat defense platform that provides added value and new benefits beyond XDR solutions, allowing you to see more and respond faster. Providing deep and broad extended detection and response

(XDR) capabilities that collect and automatically correlate data across multiple security layers—email, endpoints, servers, cloud workloads, and networks—Trend Micro Vision One prevents the majority of attacks with automated protection.

Native sensors and protection points—coupled with the XDR capabilities that stitch together threat activity across layers—allow for the quick detection of complex attacks that bypass prevention. This provides an unmatched understanding of the activity data in your environment and a balanced approach to security, as teams can quickly see the story of an attack and respond faster and more confidently. The visibility and efficiency that is provided by Trend Micro Vision One makes great security teams even better, enabling them to do more with less. In addition, the Trend Micro™ Managed XDR service can augment teams with expert threat hunting and investigation.



A PURPOSE-BUILT THREAT DEFENSE PLATFORM THAT EXCEEDS TYPICAL XDR SOLUTIONS.



### 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
- Consolidated visibility into an organization's current security status, trending over time, is hard to come by and limits the ability to know what to focus on and where action should be taken



“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

## 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.
- **Deeper data** - Integrated, native sensors deliver deep activity data, not just detections, across email, endpoints, servers, cloud workloads, and networks.
- **Faster, earlier 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 intel insights together with MITRE ATT&CK mapping enriches detection and investigation to provide a deeper understanding.
- **Greater risk visibility** - Includes role-based views of multiple risk metrics and trends that are most meaningful to your team. An intuitive dashboard provides centralized visibility and a holistic view into what is happening in your environment, including a summary of key detections, endpoints with observable attack techniques, prioritized lists of risky devices and users, along with visibility into both approved and unapproved cloud app usage and the associated risks for that.

### Respond Faster.

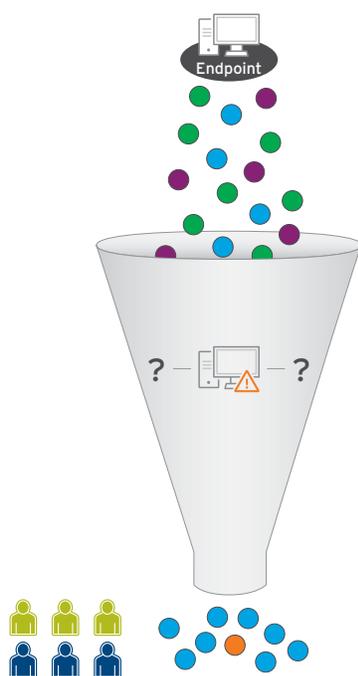
- **Timely detection models** - New expert detection rules are added regularly, based on what Trend Micro threat experts are finding in the wild. Enables automatic searching for new indicators of compromise (IoCs) with Trend Micro threat feed.
- **Faster investigation** - Quickly visualize the full attack story. XDR automatically pieces together fragments of malicious activity and paints a complete picture across security layers.
- **Automated** - Protection layer remediation capabilities deals 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 the platform.
- **Proactive policy management** - With XDR-driven insight, analysts can proactively adjust applicable product policy parameters to continually optimize defenses and provision the agent.

### Greater Security Team Efficiency.

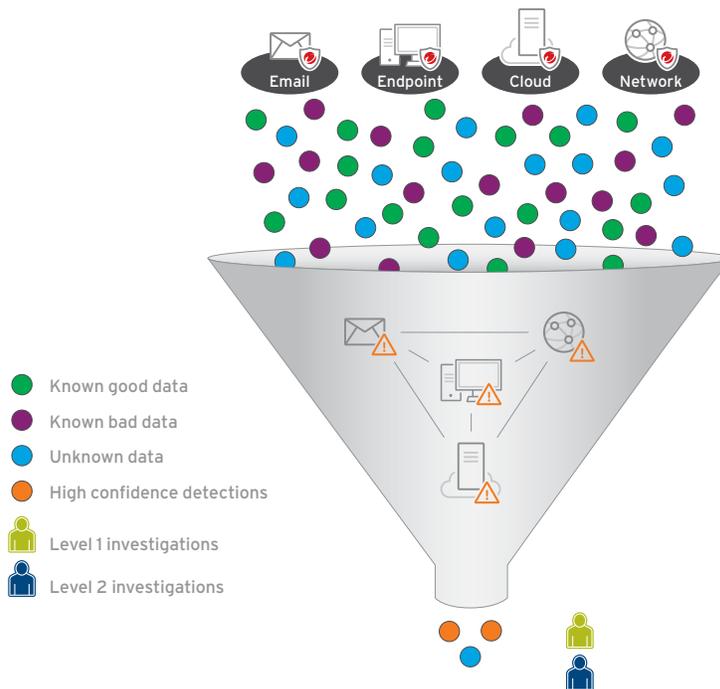
One platform to respond faster with less resources.

- **One source** of prioritized alerts to correlate and analyze data in a 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

### Legacy EDR Solutions



### Trend Micro Vision One SEE MORE.



- Known good data
- Known bad data
- Unknown data
- High confidence detections
- Level 1 investigations
- Level 2 investigations

RESPOND FASTER.

## KEY BENEFITS OF XDR WITH TREND MICRO VISION ONE

### Prioritized view of threats across the organization:

Organizations without an XDR approach ignore nearly double the security alerts as those with XDR capabilities<sup>1</sup>. 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 combined with continuously updated detection rules and global threat intelligence from Trend Micro Research, compared to having third-party integration through application programming interfaces (APIs). Organizations with an XDR approach suffered half as many successful attacks.<sup>1</sup>

### 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, simplifying the steps towards achieving an attack-centric view of an entire chain of events across security layers and take response actions from one place. This 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<sup>2</sup>.

### 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<sup>3</sup>.

### 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<sup>1</sup>.

### Integrated with third-party systems

As you may have other security tools and technologies deployed in your environment, we offer a growing portfolio of open APIs and integrations to third-party systems like SIEM and SOAR. Trend Micro Vision One has the ability to fit within these ecosystems and security operations workflows, acquiring meaningful data from your infrastructure to further enrich and validate your XDR capabilities.

## TREND MICRO™ MANAGED XDR

### Alleviate security operations teams

Managed XDR provides 24/7 alert monitoring and prioritization, incident investigation, and threat hunting to Trend Micro customers as a managed service. Customers leverage the resources and knowledge of Trend Micro security experts to improve time to detection and time to respond. This service provides teams with efficient alert monitoring, in-depth investigations into advanced threats and threat hunting via proprietary techniques. Our threat investigators can initiate respective product response options to contain threats, while providing a step-by-step response plan on actions needed to remediate, along with custom cleanup tools, where applicable, to help recover from the threat.

The Managed XDR service can be applied to email, endpoints, network, and server/cloud workload security.

1 - [The XDR Payoff: Better Security Posture, ESG Research Insights Report](#)

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>



Securing Your Connected World

©2021 Trend Micro Incorporated and/or its affiliates. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. [SB04\_Trend\_Micro\_Vision\_One\_Solution\_Brochure\_210309US]