Trend Vision One™ - XDR for OT

Bridging the gap between OT and IT with centralized visibility

Security is paramount for industries that rely on specialized operational technologies (OT) to support essential processes, from critical infrastructure and energy services to manufacturing, transportation, and healthcare. As organizations increasingly connect their OT and IT devices and networks, new challenges are arising that put their productivity, safety, and security at risk.

Modern industrial environments include hardware and software, IT networking equipment, and virtual infrastructure. With most OT breaches originating in IT networks, and with visibility challenged by the speed and evolution of threats, organizations are at risk of IP theft, ransomware, and extensive damage to systems, facilities, and even people.

To protect themselves, organizations need to determine their own unique security risk levels based on their specific compliance and regulatory standards, industrial control systems (ICS), and supply chain requirements. Their security operations center (SOC) teams must be able to handle alerts, identify threats, and make informed decisions about when and how to respond swiftly, which is a strain, given the worldwide shortage of skilled cybersecurity personnel.

Trend Micro meets the unique needs of diverse ICS verticals in device inspection, endpoint protection and network defense to secure your OT workforce, workload, and workplace. The Trend Vision One – XDR for OT solution provides a holistic overview of OT and IT environments in a single dashboard.

XDR for OT: Device and Network

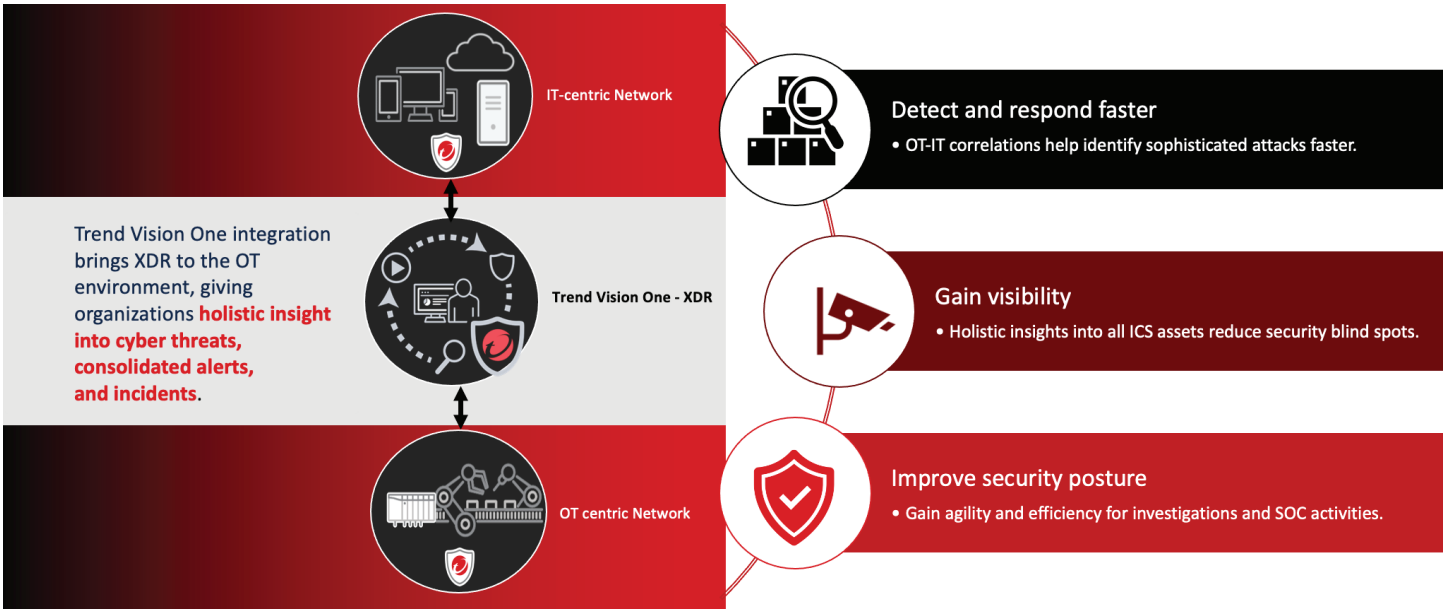
Trend Vision One – XDR for OT increases visibility at both the device and network levels:

- **XDR for OT – Device** leverages OT/Windows endpoint security software to send logs to the Trend Vision One™ platform and unlock XDR capabilities.
- **XDR for OT – Network** connects to network security products in the OT network and sends logs to Trend Vision One for XDR functionality

With the Trend Vision One platform, organizations gain complete visibility into cyber threats, consolidated alerts, and incidents, making investigations more agile and SOC teams more efficient across OT and IT environments.

Key Benefits:

- Control risks in OT-IT environments
- Detect and analyze comprehensive attacks
- Comply with regulations
- Gain visibility into threats and incidents
- Shorten mean-time-to-respond across the OT-IT environment



Key Capabilities of XDR for OT

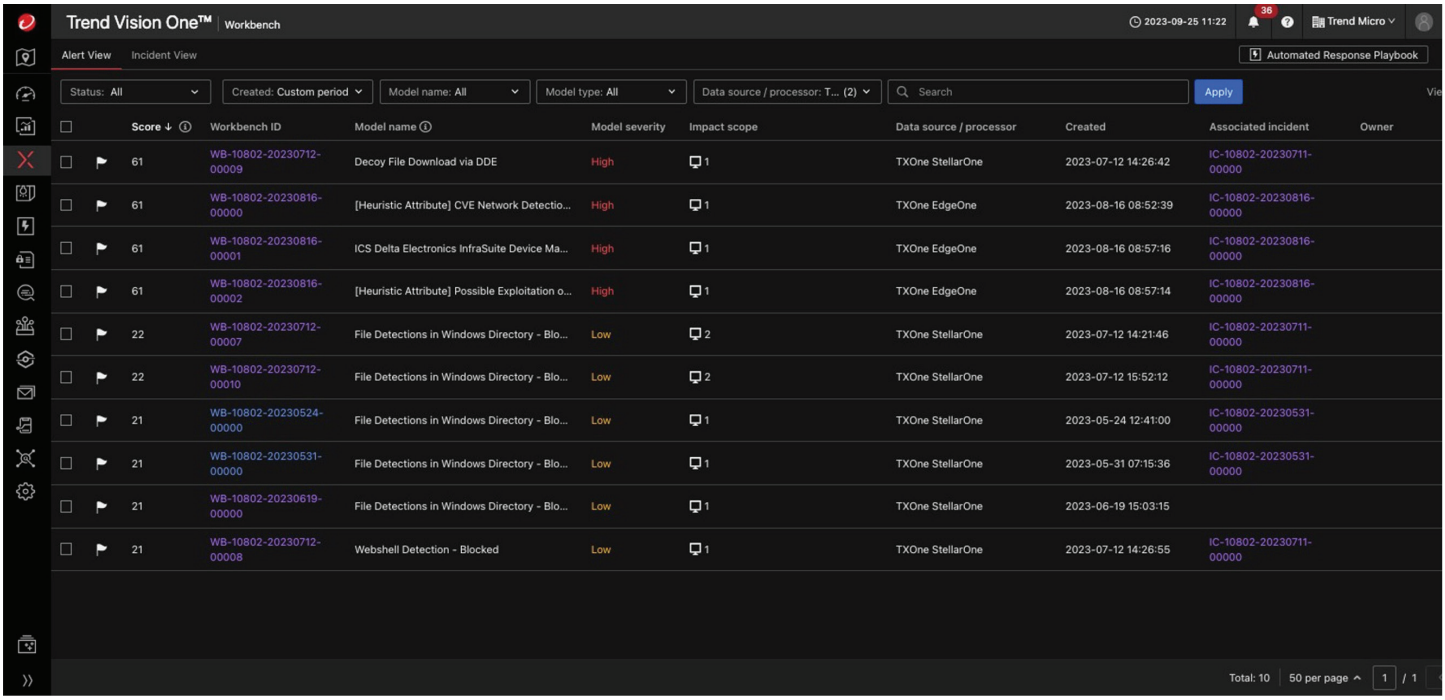
Full visibility into what, who, and where

XDR for OT displays correlated threat events in chronological order to visualize:

- What was an attack's first point of entry?
- Who or what else in the organization has been affected?
- Where did the threat call out to (e.g., production facility, equipment, machine, or infrastructure)?

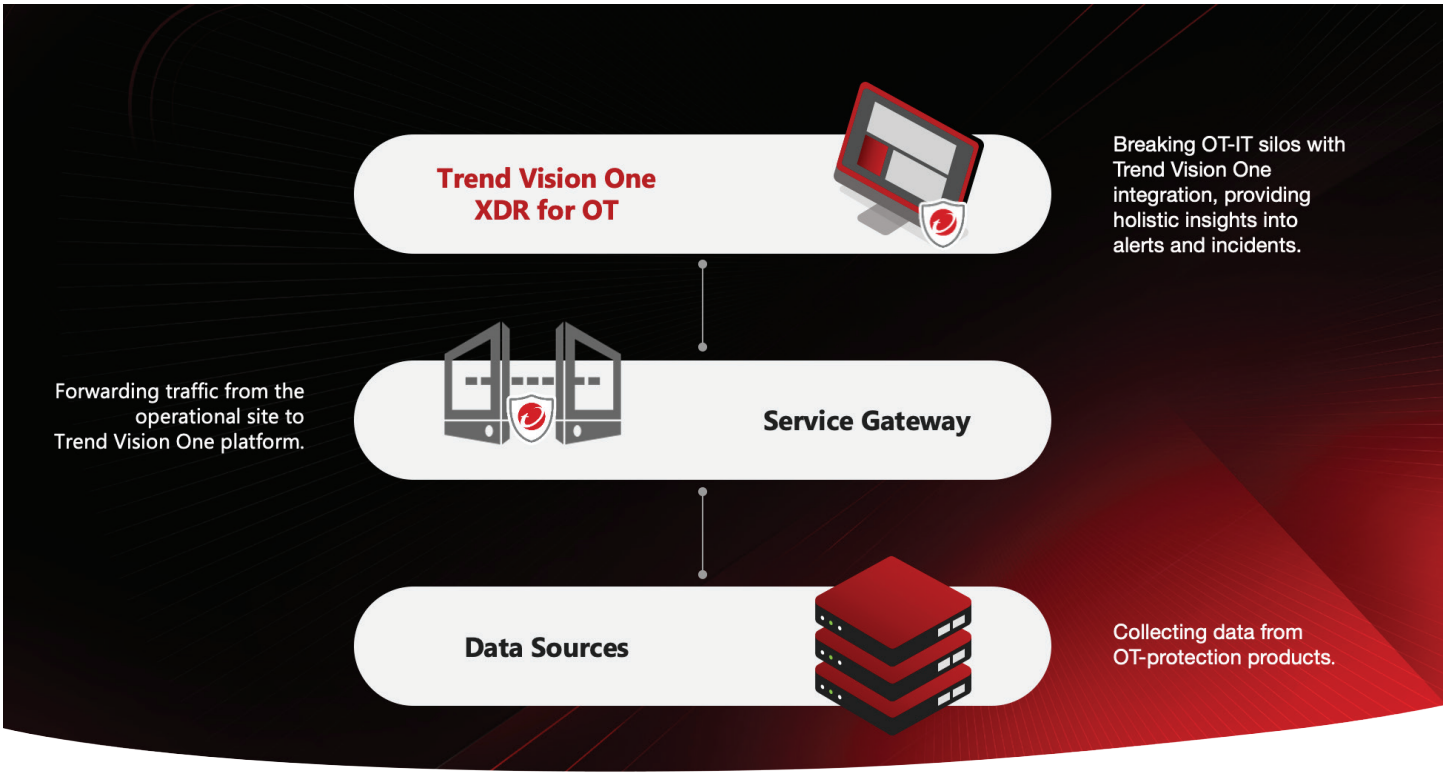
The answers to these questions help clarify the impact of any given threat and how to prioritize the response.
XDR for OT provides these insights by:

- Continuously analyzing current and historical device/network logs and correlating threat events into a single view to make the full attack cycle visible.
- Mapping every step of an attack to inform how to respond and prevent future attacks of the same type.
- Integrating Trend Micro threat intelligence for correlated detection and integrated investigation and response across OT and IT environments, including endpoints, networks, servers, cloud workloads, and emails.



Trend Vision One platform workbench for advanced detection

XDR for OT Solution Architecture



XDR for OT Features and Specifications

	TREND VISION ONE - XDR FOR OT – DEVICE	TREND VISION ONE - XDR FOR OT – NETWORK
Filter and Search	●	●
Workbench for Advanced Detection	●	●
Observed Attack Techniques: MITRE Attack Matrix Mapping		●
Event Data Retention	30 days included, extendable on request to 365 days	30 days included, extendable on request to 365 days
OT Integrations Supported Sensor	Third-party OT device security protection (including TXOne Stellar)	Third-party OT network security protection (including TXOne Edge)

XDR for OT is built on Trend Vision One™ - XDR

With Trend Vision One – XDR, you can:

Understand more with better context

Trend Vision One - XDR collects and correlates deep activity data across endpoints, networks, servers, cloud workloads, and emails—enabling more thorough hunting and investigation analysis than can be achieved otherwise.

Prioritize your responses

Knowing the extent and severity of an attack makes it easier to determine which threats require an immediate response and which ones may be able to wait.

Play out attacks

With the click of a button, you can watch the entire attack play out chronologically—from URL redirects to the initial infection point and lateral spread across the network. See every movement or scale down to view only what happened in a given time window such as this morning or over a weekend.

Dig deeper into each step of an attack

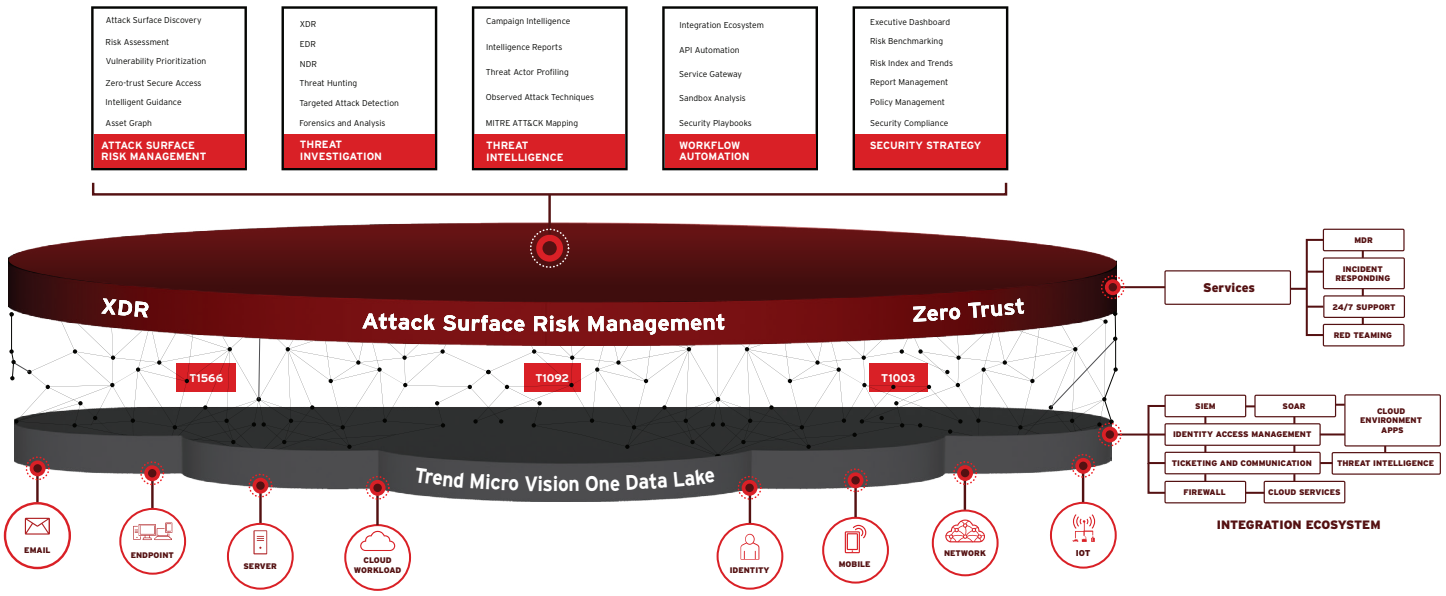
Hovering your mouse over an attack event immediately brings up pertinent network- and endpoint-level event details such as protocol used, severity, triggered rule, SHA1, number of transactions, and transaction dates spanned.

Correlate against historical network data

The average threat can go undetected for more than three months once it slips past existing security—often making it impossible to determine when it first entered the network or how. By storing events for six months or more, Trend Vision One – XDR allows you to review delayed attacks and see not only how they spread but also the infection points, enabling you to put the right safeguards in place so the same attack does not happen again.

Take advantage of a broad integration ecosystem

With a growing portfolio of open APIs and third-party systems, Trend Vision One - XDR fits within a broad range of ecosystems and security operations workflows, acquiring meaningful data from infrastructure to further enrich and validate XDR capabilities.



XDR for OT is a valuable part of the Trend Vision One platform, providing critical logs and visibility into OT devices and networks. Trend Vision One delivers extended detection and response (XDR) across OT and IT, with broad visibility and expert security analytics to minimize alerts, enable higher-confidence detections, and support for earlier, faster responses. With XDR, organizations can identify and respond more effectively and efficiently to threats, minimizing the severity and scope of an attack

©2023 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, Trend Vision One, Zero Day Initiative, and Trend Service One are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS01_XDR_for_OT_datasheet_231018US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy