Datasheet

Trend Vision One™ – XDR for Networks

Network Detection and Response (NDR)

Manage more of your attack surface with greater visibility

Organizations count on a wide array of security products and services to detect threats, raise alerts, and block cyberattacks before they do any damage. But all those tools produce a lot of data—some of it relevant, some not. Manually combing through thousands of alerts and events per day to pick out true threats—and then deciding how to respond—is a taxing process. With a global shortage of trained cybersecurity staff, this puts strain on already-stretched resources.

Network detection and response (NDR) allows you to automate the correlation of advanced threat events for faster resolution with fewer people involved. Paint an in-depth picture of the full attack and reveal ample detail, including when the initial breach occurred—which can be weeks or months earlier than suspected.

NDR use cases:

- **Increase visibility** by correlating network telemetry with other security vectors, such as endpoints and workloads, to identify potential threats
- **Gain insight** into encrypted network traffic
- **Expose the unmanaged** parts of the attack surface by analyzing all network assets, including devices not protected by an agent
- **Maintain network uptime** with faster mean times to detection and response (MTTD and MTTR), drilling down into individual network traffic, connections, and packets to identify and investigate incidents
- **Implement a response plan** by taking action inline and automating with playbooks
- **Repel targeted attacks** with cross-layered actions via our Trend Vision One™ – Endpoint Security solution

Key capabilities

See how cyberattacks unfold

A cyberattack isn't just a point-in-time event. Advanced and targeted attacks can occur over days, weeks, and even longer, taking advantage of multiple attack vectors. NDR reveals the chronological order of correlated threat events so you can easily visualize the entire lifecycle and understand how an attack played out, helping you ensure optimal protection in the future.

Gain full visibility into what, who, and where

NDR enables you to retrace an attack's first point of entry, identify who else within your organization has been affected, and determine where the attack was calling out to via its command-and-control (C&C) communications. These insights help you clarify the impact on your organization and lend insight into how to prioritize your response.

Attack visibility

- See the full attack lifecycle
- Decrypt and inspect traffic
- Go beyond the infection point
- Watch the attack playback
- Learn the methods used by attackers

Response prioritization

- Understand the attack scope
- Determine attack severity
- Detect and analyze comprehensive attacks quickly
- Take action inline

Proven leadership

Recognized in 2024 Voice of the Customer for Network Detection and Response, Midsize Enterprise ($50M - $1B)

Named a Leader in the Forrester Wave™, Network Analysis and Visibility, Q2 2023

Deepen your context and understanding

Collect and correlate deep activity data for singular and multiple vectors including email, endpoints, servers, cloud workloads, and networks. This comprehensive data collection gives you a level of threat hunting and investigation analysis that is often difficult or impossible to achieve otherwise.

In addition, enhance threat detection with our Trend Vision One™ – Sandbox Analysis solution by extracting content from inspected traffic including URLs or files. This enables improved advanced threat and targeted attack identification.

Enabling visibility into decrypted traffic further enhances your extended detection and response (XDR) capabilities, allowing you access to more detailed inspection and analyses of network communications. This addition also ensures that even your encrypted traffic can be monitored and analyzed, enabling a more complete security posture—and more effective threat detection and response capabilities.

Prioritize your response

Knowing the full extent and severity of attacks makes it easier for you to determine which threats require immediate response and which ones may be able to wait. Using Endpoint Security and automated playbooks, your security operations center (SOC) professionals can easily and effectively mitigate risk by blocking threats inline while creating playbooks to combat future attacks.

Flexible deployment options

There are multiple ways to take advantage of NDR:

- Inline NDR: Enable the network sensor on a Trend Micro™ TippingPoint™ TXE appliance
- Out-of-band NDR: Enable the network sensor within your existing Trend Micro™ Deep Discovery™ Inspector, or install a standalone virtual network sensor within a virtual machine or cloud provider platform

Access all the details you need

By hovering your mouse over an attack event within our Trend Vision One™ – XDR for Networks solution, you can immediately see key network and endpoint-level event details. These include the protocol used, severity, triggered rules, Secure Hash Algorithm 1 (SHA-1), and the number of transactions and dates covered in the attack span.

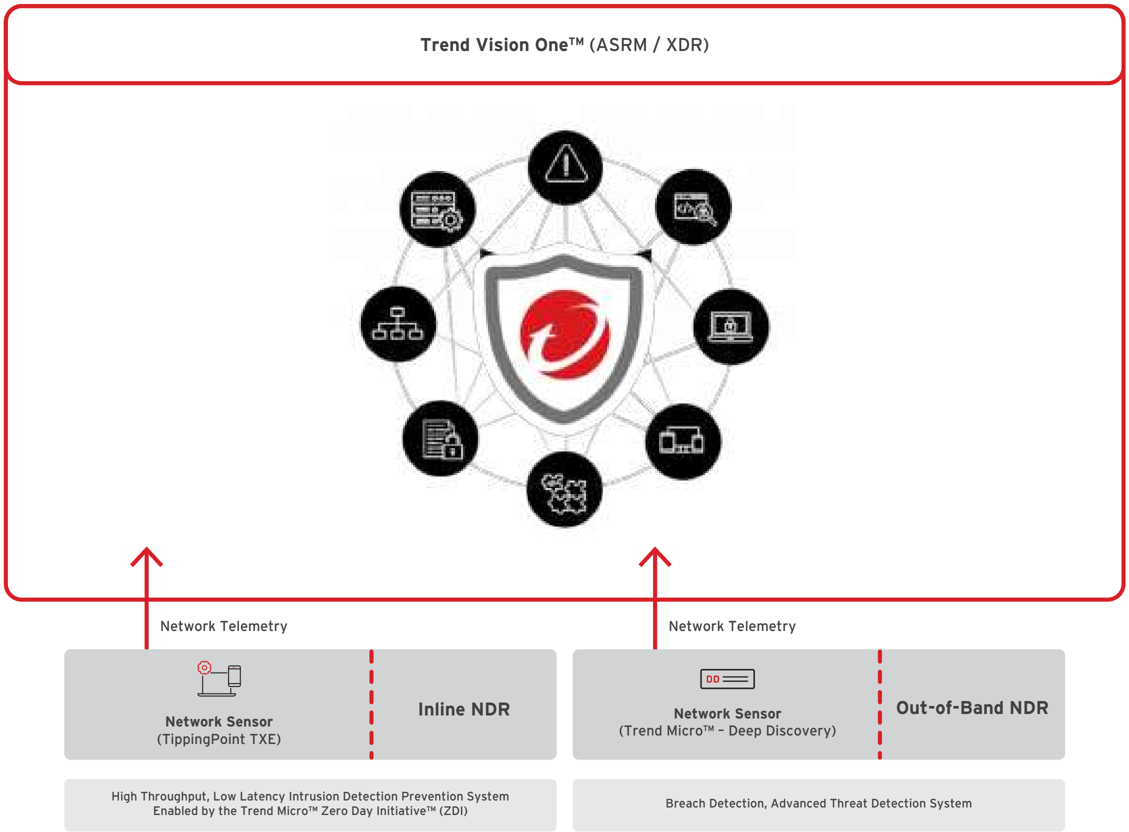
In addition, you can leverage XDR for Networks to retroactively correlate against historical network data. This is important as the average threat goes undetected for more than three months upon slipping past existing security defenses. By the time it is finally spotted, it can be difficult to determine when or how it first entered the network.

XDR for Networks stores events for six months or more, allowing you to look back at delayed attacks and see how they spread as well as the original infection point. Put proactive safeguards in place to help mitigate risk.

Play out the attack

With a single click, you can see an entire prior attack unfold chronologically, from URL redirects to the initial infection point and lateral spread across the network. Get the complete picture or scale it down to observe what happened in a specific time window.

Figure 1: Overview of deployment options


Trend Vision One™ (ASRM / XDR)
Network Telemetry
Network Telemetry
Network Sensor
(TippingPoint TXE)
Inline NDR
DD
Network Sensor
(Trend Micro™ – Deep Discovery)
Out-of-Band NDR
High Throughput, Low Latency Intrusion Detection Prevention System
Enabled by the Trend Micro™ Zero Day Initiative™ (ZDI)
Breach Detection, Advanced Threat Detection System

Our unified, AI-powered Trend Vision One platform delivers XDR for email, endpoints, servers, cloud workloads, and networks. Its broad visibility and expert security analytics allow you to reduce alerts while enabling higher-confidence detections for earlier, faster responses. Bolster your threat identification and response capabilitiies by minimizing the severity and scope of attacks. XDR for Networks is a valuable part of the platform, providing you with critical logs as well as visibility into unmanaged systems, including contractors and third parties, internet of things (IoT) and industrial internet of things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

System requirements and specifications

The combined maximum inspection capacity of XDR for Networks is 300 Gbps. This applies whether connecting from a network sensor built into Deep Discovery Inspector, a standalone virtual network sensor, or TippingPoint.

Requirements: XDR for Networks using Deep Discovery Inspector

Hardware: XDR for Networks is compatible with Deep Discovery Inspector hardware model series 500, 1,000, 4,000, and 9,000.

For more information, please visit **trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html**

Software: To get the greatest value from XDR for Networks, Trend Micro recommends Deep Discovery Inspector version 6.6 or above. The solution will support the use of Deep Discovery Inspector version 5.7 Service pack 3 or above to connect to Trend Vision One.

Requirements: XDR for Networks using a standalone virtual network sensor

This configuration requires a virtual machine with the following minimum specifications:

- VMware vSphere ESXi/vCenter 6.5 or above
- Microsoft Hyper-V on Windows Server 2016 or above
- Red Hat Enterprise Linux 9.2 with KVM
- Nutanix AHV or the following cloud provider platform:
  - AWS
  - Microsoft Azure
  - Google Cloud Platform™ (GCP)

Throughput (MBPS)	Virtual CPUs	Virtual memory (GB)	Virtual disk (GB)	Virtual NICs
100	2	8	50	2
500	4	12	50	2
1,000	6	18	50	2
2,000	8	24	100	2
5,000	16	36	150	2
10,000	26	48	200	2

Requirements: XDR for Networks with TippingPoint

Hardware: XDR for Networks is compatible with TippingPoint 8600TXE and 9200TXE

Software: SMS and TPS version v6.3.0, must first connect SMS to Trend Vision One and deploy at least one intrusion prevention filter policy.

Start free trial of Trend Vision One

Learn more at TrendMicro.com

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