Trend Micro™

XDR FOR NETWORKS

Prioritized actionable threat intelligence to mitigate current and existing threats

We call on security products and services to keep our businesses and organizations safe. Most of the time they do exactly what we want them to do; detect, alert, and block threats trying to land a successful attack. However, the downside is that they produce a lot of data, some of it relevant, some of it not. It is up to the security professional(s) in the organization to comb through the potential thousands of alerts or events each day to determine what is actually a threat and decide whether or not they need to respond. Compounding this problem is a worldwide shortage of cybersecurity staff or personnel that needs to be trained to decipher these events.

Trend Micro™ XDR for Networks (formerly Trend Micro™ Deep Discovery™ Network Analytics) automates the correlation of advanced threat events. This provides faster resolution with fewer people involved, while providing an in-depth picture of the full attack. In some cases, you may believe the attack started today, but in fact, the initial breach happened weeks or months ago.

XDR for Networks:

- Continuously analyzes current and historical network metadata and correlates these related threat events into a single view for full visibility of the attack cycle.
- Uses advanced and sophisticated machine learning techniques to detect network traffic anomalies.
- Correlates the events and maps out every step of the attack, quickly answering the questions of of "what", "who", and "where". Giving you a better idea of how to respond and prevent future attacks.
- Combines with other Trend Micro products for correlated detection and integrated investigation and response across email, endpoints, servers, cloud workloads, and networks.

KEY CAPABILITIES

- **See the full attack lifecycle.** An attack isn't just a point in time. Advanced or targeted attacks take time and use multiple attack vectors to execute. XDR for Networks gives you the chronological order of correlated threat events to easily visualize the entire life cycle and truly understand the attack and protect yourself from future attacks.
- **Full visibility into the "what", "who", and "where".** XDR for Networks will correlate and help simplify threat events to show you: **What** was the first point of entry of the attack? **Who** else in the organization has been impacted by the attack? **Where** was the threat calling out to? (i.e. command and control (C&C) communication). With visibility and answers into these three questions, you will have a better understanding of the threat's impact on your organization and how to prioritize your response.

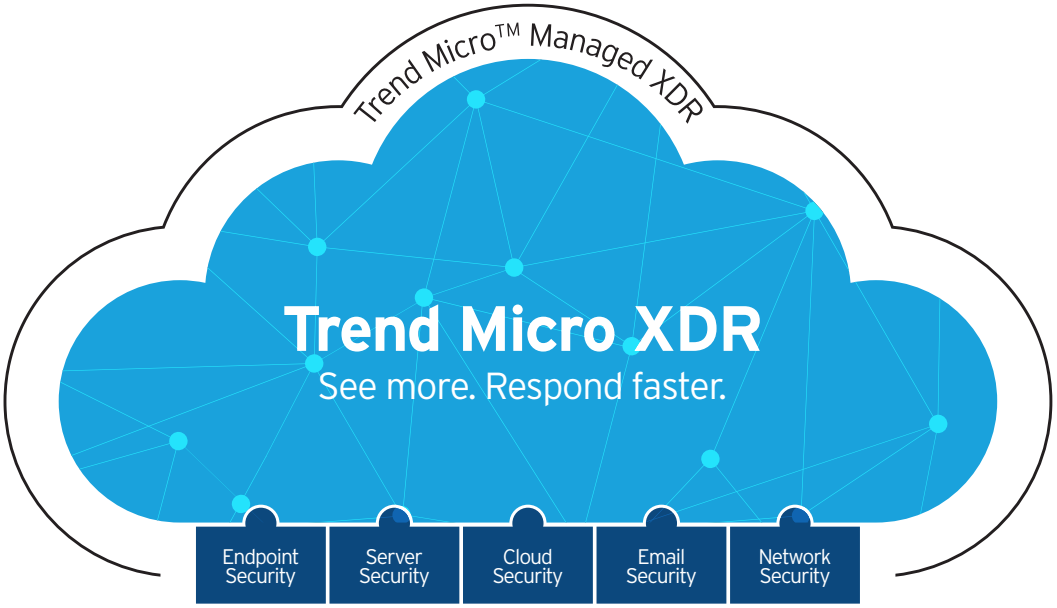
Attack Visibility

- Correlate six months of events
- See the full attack lifecycle
- Go beyond the infection point
- Watch the attack play back
- Learn the methods used in the attack

Prioritization of Response

- Understand the scope of the attack
- Know the attack severity
- Gain quick detection and analysis of comprehensive attacks

- **Get greater context for greater understanding.** XDR collects and correlates deep activity data for one or more vectors—email, endpoints, servers, cloud workloads, and networks—enabling a level of hunting and investigation analysis that is difficult or impossible to achieve otherwise.
- **Prioritize your response** By knowing the extent of an attack and its severity you can determine which threat requires immediate response and which threats may be able to wait.
- **Play out the attack** With the click of a button you can see the entire attack play out chronologically from the URL redirects, to the initial infection point, to the lateral spread across the network. See every movement or scale it down to just view what happened this morning or over a weekend.
- **Dig deeper into each step of the attack quickly** It is great to have visibility into an attack but sometimes you need the details. Just by hovering your mouse over an attack event, you can immediately see pertinent details of the attack at network and endpoint event levels such as; protocol used, severity, triggered rule, SHA1, number of transactions and dates they span, etc.
- **Correlate retroactively against historical network data** The average threat can go undetected for over three months once it slips past your existing security. In most cases, when you finally see it you may never know when it first entered your network or how. By storing the events for six months or more you can look back at delayed attacks and see not only how it spread, but also the infection point to make sure you put the right safeguards in place so it doesn't happen again.
- **Flexible deployment options.** Prefer to keep everything in-house? Want to offload everything to the cloud? Choose the deployment option to meet your needs, offered as an on-premises solution (Deep Discovery Network Analytics) or an "as-a-service" solution (XDR for Networks) hosted in the cloud. If you keep it on-premises you will benefit from integration with the endpoint (Trend Micro Apex One™) to add more context around each attack. For full XDR, the as-a-service solution will provide broader visibility across endpoints, servers, cloud workloads, and email.



Trend Micro XDR Sensors

Trend Micro™ XDR delivers extended detection and response for email, endpoints, servers, cloud workloads, and networks. It offers broader visibility and expert security analytics leading to fewer alerts and higher-confidence detections for earlier, faster response. With XDR, customers can identify and respond more effectively and efficiently to threats, minimizing the severity and scope of an attack on the organization. XDR for Networks is a valuable part of the Trend Micro XDR solution, providing critical logs and visibility into unmanaged systems such as; contractor/third-party systems, Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

SYSTEM REQUIREMENTS AND SPECIFICATIONS:

	XDR add-on: Trend Micro Deep Discovery Inspector	Deep Discovery Network Analytics on-premises	Deep Discovery Network Analytics 9000 series appliance
Combined Deep Discovery Inspector throughput	1 Gbps – 20 Gbps	1 Gbps – 4 Gbps	5 Gbps – 10 Gbps
Form factor	SaaS	Requires on-prem storage (~2.3 TB per Gbps)	1U rack mount, 48.26 cm (19")
Event data retention	Up to 180 days	Up to 180 days	Up to 180 days
Prerequisite solution	Trend Micro Deep Discovery Director 5.3 or later (virtual appliance) optional	Deep Discovery Director 5.8 or later (virtual appliance)	None
Dimensions (WxDxH)	N/A	N/A	43.4 (17.08") x 72.8 (28.68") x 4.28 (1.69") cm
Weight	N/A	N/A	17.5 kg (38.58 lb)
Data ports	N/A	N/A	10/100/1000 BASE-T RJ x 1
AC input voltage	N/A	N/A	100 to 240 VAC
AC input current	N/A	N/A	7.4 A to 3.7 A
Hard drives	N/A	N/A	7 x 1.92 TB
RAID configuration	N/A	N/A	RAID 5
Power supply	N/A	N/A	550 W redundant
Power consumption (Max)	N/A	N/A	604 W
Heat	N/A	N/A	2559 BTU/hr (max.)
Frequency	N/A	N/A	50/60 Hz
Operating temp	N/A	N/A	10 to 35 °C (50-95 °F)
Hardware warranty	N/A	N/A	3 years (extendable to 5 years)

INTEGRATED PRODUCTS

- Trend Micro™ Deep Discovery™ Director 3.0 or later
- Trend Micro™ Deep Discovery™ Inspector 5.1 or later

VIRTUAL APPLIANCE

Virtual machine with the following minimum specifications:

- Hypervisor: VMware vSphere ESXi 6.5, Microsoft Hyper-V in Windows Server 2016
- Deep Discovery Director Network Analytics is an appliance based on CentOS Linux 7 (64-bit)
- Network interface card: One with one Gbps adapter
- SCSI controller: LSI Logic Parallel
- CPU: 1.8 GHz (8-12 cores)
- Memory: 64 GB
- Hard disk: 6 TB (thick provisioned)

With this configuration and a typical enterprise level of network traffic, Deep Discovery Director Network Analytics can service:

Deep Discovery Network Analytics	XDR add-on: Deep Discovery Inspector
Up to 4 Gbps of combined Deep Discovery Inspector throughput E.g., 1 DDI 4000 or 4 DDI 1000	Up to 20 Gbps of combined Deep Discovery Inspector throughput E.g., 2 DDI 9000 or 5 DDI 4000

TREND MICRO™

Securing Your Connected World

DS04_XDR_for_Networks_220617US