TREND MICRO™ XDR: SALES FAQ

September 2019

IN THIS DOCUMENT...

ABOUT XDR

1. What is XDR?

- For Trend Micro, XDR refers to the ability to do detection and response across email, endpoint, server, cloud workloads, and network via a single platform or through managed services.
- X refers to the multiple layers. XDR extends beyond the endpoint, so we are using the XDR term to differentiate from single player for EDR. However Trend Micro EDR is part of our XDR message.
- The XDR platform or the Managed XDR services sit on top of the relevant Trend Micro products in a customers' environment and offers consolidated visibility and investigation of events across security layers, leading to earlier detections and faster response.
- XDR enables better context and deeper analysis, so customers can respond more effectively and efficiently to threats, minimizing the severity and scope of a breach on the organization.

2. Is XDR another product?

- XDR is the concept of performing detection and response across multiple security layers, and this capability can be obtained in a few ways as XDR is rolled out in phases between now and then end of 1H 2020.
- XDR functionality is coming first for endpoint and email. This is built on top of our current EDR capabilities by extending detection and response support across endpoints and basic servers (using Trend Micro™ Endpoint Sensor SaaS, XDR Edition) and email (using Trend Micro™ Cloud App Security), with Trend Micro Apex Central™ SaaS being the visibility and investigation platform. There is a new SaaS bundle available called 'XDR for Users' combining these solutions/capabilities. See next section for details.
- In 1H 2020, there will be a new XDR platform available for customers that will consolidate and enhance detection, investigation and response capabilities across email, endpoint, server, cloud workloads, and network in a single console.
- Available today, customers can subscribe to Trend Micro Managed XDR services (rebranding of existing MDR services) to gain the benefits of cross-correlation detection and investigation across email, endpoint, server, cloud workloads, and network.
- It is important to note that depending on the products a customer has/buys, they can leverage the XDR platform and employ the Managed XDR services across one or more of the available layers. Customers don't have to buy every associated product or Managed XDR service to gain value. Of course, the more layers they employ, the more sources there are to correlate and analyze, and the better the insight customers will obtain.

3. Does XDR work with Trend products only, or can it be integrated with other products?

- For right now, we are focusing on integrating Trend Micro products into XDR. In the future, we will start integrating with third-party solutions.
- We will have integration with SIEM. XDR provides the advantage of sending fewer, prioritized alerts to SIEM based on the correlation and analysis of the data from the Trend Micro products in the environment. This reduces the noise for security analysts and helps them to narrow in on what is critical.

4. What is the difference/relationship between XDR and SIEM?

- Organizations use SIEMs to collect logs and alerts from multiple solutions and stores them for compliance. While it allows companies to bring together a lot of information from multiple places for centralized visibility, the reality is that it results in an overwhelming number of individual alerts, that are difficult to sort through to understand what is critical and needs attention. Correlating and connecting all of the logs of information to gain a view of the bigger picture is challenging, if not impossible to do.
- Conversely, XDR collects activity and detection data from multiple Trend Micro products and correlates the data, applying AI and expert analytics to provide context rich alerts, which can be further investigated in the XDR platform and can be sent to a company's SIEM solution.
- XDR doesn't replace the SIEM, but instead can augment the SIEM, reducing the amount of effort required by security analysts to analyze alerts and logs from the Trend Micro products.
- XDR also enables response actions across multiple product, which is not a function of a SIEM.

5. What size of company is the target for XDR?

- XDR is available down to 250 user organizations but the solution is ideally targeted to mid-size to large enterprises (500+ users).
- The Managed XDR service is a great option for organizations who want the benefits of XDR but may not have the internal resources to fully capitalize on it in-house, or who need to augment their resources for 24/7 monitoring and alerts.

6. Are any other vendors offering an equivalent to XDR? What do they offer?

- Nearly all endpoint vendors offer detection and response for endpoints (EDR). While EDR is necessary, we argue it is no longer enough.
- EDR-first vendors like CrowdStrike and Carbon Black may supplement their EDR with integrations with network and email vendors but these third-party integrations are not the equivalent to integrating data from solutions native to the vendor. As example:

    1. The type of data being pulled is different. Often, they will get only alert data and not full activity data (telemetry, metadata, netflow). This means there is less to feed into the analytical models for correlation and prioritization, etc.
    2. Definitions of detections and severity indicators can vary as each vendor defines their data differently. A vendor will never have the same depth of understanding of a third-party vendor's alerts, as they would their own. This can make it difficult to reconcile/understand the data to get the combined story and assess the overall risk.

7. Where is my customers' data stored? Will it be compliant with GDPR?

- Trend Micro acts GDPR compliant.
- XDR will leverage data stored in secure Trend Micro data lakes.
- Data from individual organizations is carefully protected from any cross-contamination with any other organizations' data.
- Data lakes will be located in both the US and Europe for data residency compliance.

8. XDR is going to be another console, how will that work with Trend Micro Apex Central™ and other product consoles?

- XDR will be the single console for integrated detection and response across multiple layers.
- There will be single-sign-on (SSO) capabilities between the XDR console and the other product consoles, including Apex Central.
- SSO will allow users to switch to a product's console as/when required, e.g. to make a policy change.
- As a general rule, the different consoles serve different users. The XDR console will be used primarily by SOC analysts, whereas the individual products consoles would be used by analysts in specific areas, whether that is cloud and data center, network or IT security. The XDR console is intended to provide centralized visibility and investigation across security layers and individual products.

9. Is XDR available for on-premises products?

- The XDR platform will only be available as a cloud offering because the volume of storage and processing capacity required for the XDR data lake and AI/data analytics, can only be accomplished in the cloud.
- As of its release in 1H 2020, it will integrate with Trend Micro Apex One™ SaaS, Trend Micro™ Deep Security™ as a Service, Cloud App Security and Trend Micro™ Deep Discovery™.
- Managed XDR services are available for on-premises products (such as Deep Security and Apex One) and can provide cross-layer detection and response as a managed service.

MANAGED XDR SERVICE

10. What is the difference between XDR and Managed XDR capabilities?

- Managed XDR is the renamed Trend Micro MDR service. The existing services remain the same, it is simply a new name.
- Analogy: XDR is like providing tools for you to monitor and fix your car. Managed XDR is like providing a trained automotive service technician to monitor and fix your car if you don't have the expertise or time to do it yourself.
- Managed XDR is delivered by Trend Micro incident response experts and provides:
    - 24/7 critical alerting and monitoring
    - Root cause and impact analysis
    - Incident prioritization and investigation
    - Response plans and recommendations on remediation and preventative measures
    - Incident reporting and executive reporting on security posture
- The Managed XDR services can be sold on top of email, endpoint, server, cloud workloads, and network protection products.
- There is one Managed XDR Service only. The more protection products a customer adds to the service the better their ROI.
- The Managed XDR services are a great option for:
    - For channel partners to add to their portfolio especially if the do not offer services yet.
    - Organizations who want the full benefits of XDR across all security layers right away (prior to the XDR platform's introduction in 1H 2020)
    - Organizations who may not have the internal resources to fully capitalize on XDR in-house
    - Organizations with SOCs who may want additional detection and response support (second set of eyes, 24/7 monitoring and alerting)

11. How does the current MDR service change, if at all?

- The current MDR services have been renamed as Managed XDR.
- A new service bundle called "Managed XDR for Users" will be available to add MDR on top of the "XDR for Users" product bundle and combines the current managed services for endpoint and messaging.

13. What are the licensing pre-requisites for Managed XDR?

- There is one Managed XDR Service only. The more protection products a customer adds to the service the better their ROI.
- Standard and Advanced services are offered for:

Service	Pre-Requisites	Other Requirements
Managed XDR for Users **(Combines Managed XDR for Endpoints and Managed XDR for Messaging)**	• XDR for Users SaaS bundle	• Minimum 251 users
Trend Micro™ Managed XDR for Endpoints **(Incl. basic server agents available with Apex One + Endpoint Sensor, does not cover Deep Security)**	• Apex One + Endpoint Sensor	• Minimum 251 users • MDR quantity must match corresponding Apex One and Endpoint Sensor quantity
Trend Micro™ Managed XDR for Messaging (email)	• Cloud App Security	• Minimum 251 users • MDR quantity must match corresponding CAS quantity
Trend Micro™ Managed XDR for Cloud Workloads	• Deep Security Enterprise is available today, and Deep Security as a Service will be supported in September.	• Minimum 50 servers • MDR quantity must match corresponding DS quantity • Advanced service only available with Managed XDR for Endpoint/Server or Managed XDR for Networks (cannot buy standalone)
Trend Micro™ Managed XDR for Networks	• Deep Discovery Inspector (DDI) or Virtual Deep Discovery Inspector (VDDI)	• MDR quantity must match corresponding DD quantity

13. What is the difference between Managed XDR Standard and Advanced?

	Endpoints		Network		Cloud Workloads		Messaging		
	Std.	Adv.	Std.	Adv.	Std.	Adv.	Std.	Adv.	
Detection									
24/7 critical alerting and monitoring	O	O	O	O	O	O	O	O	MDR team will continuously monitor the logs for new critical alerts, investigate via automated or manual means, and deliver details on the threat. You can define the escalation path for the MDR team based on critical assets and other criteria.
IoC sweeping	O	O	O	O	O	O	O	O	The MDR team will sweep your environment's metadata stores for newly identified IoCs, including those shared via US-CERT and other third-party disclosures that Trend Micro receives.
Root cause analysis	O	O							Using the endpoint data, the MDR team will generate a root cause analysis, which shows the attack vector (email, web, USB, etc.), dwell time, and the spread and impact of the attack.
Threat source identification					O	O			If a customer is using containers, the MDR team can help identify the container with the discovered threat.
Investigation									
Incident prioritization		O		O		O		O	Using threat knowledge and customer shared environment data, the MDR team will help to prioritize which alerts or threats need to be handled first. The team escalates threats to specific high-value endpoints as requested by the customer.
Impact analysis		O		O					A new threat/IoC in a customer's environment is checked against the metadata stores to assess if that file is on any other protected system and what other systems may be compromised.
Suspicious user activity tracking								O	Investigate unusual user account activity that could signify a compromised account, such as spamming: sudden and large volume of outbound emails.
Container identification						O			Identify what container a specific attack originated from and/or what container(s) was targeted.
On-demand health check		O							Customers can request an aggressive endpoint scan, which uses the latest threat intel to scan for potential threats. This in-depth process is invasive, scans the endpoints themselves, and can affect their performance during the scan.
Response									
Access to MDR analysts		O		O		O		O	Customers will be able to speak to the MDR security analysts for further details or clarification beyond the report.
Threat response		O		O		O		O	To the best of their ability, the MDR team will provide detailed remediation options and, as applicable, custom cleanup tools to help recover from the threat. This includes, for messaging, the ability to lock out compromised accounts and remove IoC-matched emails.
Executive summary report – monthly		O		O		O		O	The MDR team will provide an executive summary outlining the services provided over the specific time period, including IoC sweeps completed, alerts handled, etc.
Executive summary report – quarterly	O		O		O		O		The MDR team will provide an executive summary outlining the services provided over the specific time period, including IoC sweeps completed, alerts handled, etc.

* SaaS version of Endpoint Sensor supports Microsoft® Windows® and Linux® servers.

See the Managed XDR datasheet for more information

XDR FOR USERS SALES BUNDLE

14. What is XDR for Users, how is different than XDR?

- We are enhancing our current EDR capabilities by extending detection and response across endpoint and servers (using Apex One/Endpoint Sensor SaaS) and email (using Cloud App Security for Microsoft® Office 365® or Google G Suite™), with Apex Central SaaS being the visibility and investigation platform.
- XDR for Users is a new SaaS bundle that enables customers to adopt the products required to benefit from these capabilities. It includes:
    - Apex Central SaaS
    - Apex One SaaS (incl. vulnerability protection, app control, DLP)
    - Cloud App Security
    - Endpoint Sensor as a Service – XDR Edition (formerly called Trend Micro™ Apex One SaaS, Endpoint Sensor Add-On)
- It is important to note that the server component of this bundle uses the Endpoint Sensor agent for Windows and Linux® servers; it is a SENSOR ONLY, and does not include any protection components. Deep Security remains the solution for advanced server and cloud workload protection.
- There is an associated Managed XDR for Users service that can be purchased on top of the XDR for Users bundle.

15. Is XDR for Users available via SaaS and on-premises?

- The components of the XDR for Users bundle are SaaS only

16. What is the difference between Endpoint Sensor: XDR Edition and Endpoint Sensor?

- Endpoint Sensor as a Service, XDR Edition (formerly called Apex One SaaS, Endpoint Sensor Add-On) is the SaaS version of endpoint sensor, which will now support Apex One SaaS, Microsoft® Windows® and Linux servers (Oct 2019).
- Endpoint Sensor is the on-premises endpoint sensor which supports Apex One on-premises.

17. Does an existing Endpoint Sensor SaaS customer get XDR capabilities?

- Yes, existing customers with the SaaS version of Endpoint Sensor will have the ability to add Windows and Linux servers if they wish, and should they have Cloud App Security, will be able to trace a root cause analysis back into email to determine who else received a phishing attack or has an IoC in their inbox.

18. Is root cause analysis coming for Mac OS endpoints?

- Yes, in October 2019.

19. What is the server piece of Endpoint Sensor as a Service, XDR Edition - what does it do? What is its relationship with Deep Security?

- The server piece of Endpoint Sensor as a Service, XDR Edition sends server telemetry data to a data lake for detection and response. It works with Windows and Linux servers.
- The Endpoint Sensor as a Service, XDR Edition does not provide protection for servers.
- Deep Security provides protection for servers. XDR for Deep Security will come in 1H 2020 and Managed XDR is available now for Trend Micro™ Deep Security™ Enterprise.
- It is an option for customers who currently have no protection on servers and are only interested in doing detection and response. Customers looking for a more complete solution for their servers and workloads should be encouraged to wait for XDR with Deep Security in 1H 2020, or leverage the Managed XDR service.

20. How can a customer on a legacy suite get XDR for Users?

- Legacy suite customers can purchase XDR for Users and it will be co-termed with their existing renewal. If the customer needs a transition period to migrate to the cloud, we can extend their existing license. Or if they require components in the Trend Micro™ Smart Protection™ Suites, they can purchase the appropriate Smart Protection Suite and add Endpoint Sensor as a Service, XDR Edition.
- For legacy customer who want to stay on-premises, Managed XDR is available.

21. Will customers who purchase XDR for Users have access to new XDR capabilities that become available in H1 2020?

- Yes, "XDR for Users" will receive the equivalent (and more) detection and response capabilities in the new XDR platform when it is introduced.

SALES MOTION

22. If a customer wants XDR, what do I sell in 2019?

New Endpoint Prospect	• XDR for Users (SaaS only) • Managed XDR
Legacy Endpoint Customer	• Open to SaaS – XDR for Users • On-premises-add Endpoint Sensor on-premises • Managed XDR
Smart Protection Suite Customer	• SaaS – add Endpoint Sensor, XDR Edition • On-premises - Endpoint Sensor, On-Premises • Managed XDR
New or Existing Cloud/Data Center Customer	• Lead with Deep Security • Only bring up XDR if it is a requirement • Managed XDR or vision
New or Existing Network (DDI Customer)	• Trend Micro™ Deep Discovery™ Network Analytics as a Service • Vision of XDR in 2020 • Managed XDR

TREND MICRO™

Securing Your Connected World