Trend Micro

WHAT IS XDR?

XDR is:
XDR is cross-layered detection and response. XDR collects and automatically correlates data across multiple security layers – email, endpoint, server, cloud workloads, and network – so threats can be detected faster and security analysts can improve investigation and response times.

XDR
XDR provides cross-layered threat detection and response.

Stealthy threats evade detection. They hide in between security silos amid disconnected solution alerts and propagate as time passes, while security analysts try to triage and investigate with narrow, disconnected attack viewpoints.

XDR breaks down these silos using a holistic approach to detection and response. XDR collects and correlates detections and deep activity data across multiple security layers – email, endpoint, server, cloud workloads, and network. Automated analysis of this superset of rich data means threats are detected faster, and security analysts are equipped to do more thorough investigations and take quick, subsequent action.

Learn more about the security layers that can feed into XDR.

XDR SOC challenges
When it comes to detection and response, SOC analysts are faced with the daunting responsibility of quickly identifying critical threats to limit the risk and damage to the organisation, and yet they must do so amid less than ideal circumstances.

Alert overload
It is no surprise that IT and security teams are often overwhelmed with alerts getting triggered by different solutions. A company with an average of 1000 employees can see a peak of up to 22,000 events per second enter their SIEM. That's almost 2 million events in a day.[1] Confronted with an abundant volume of alerts with little means to correlate and prioritise them, even the most skilled analysts struggle to quickly or effectively weed through the noise to find the critical events. XDR can automatically tie together a series of lower-confidence activities into a higher-confidence event, surfacing fewer, prioritised alerts for action.

Visibility gaps
While many security products provide visibility into alerts and activity, each product offers a specific perspective and collects/provides data as relevant and useful for that function. Integration between security products can enable data exchange and consolidation, but the value is often limited by the type and depth of the data collected and the level of correlated analysis possible. This means there are gaps in what you can see and do. XDR, by contrast, collects and provides access to a full data lake of activity data (detections, telemetry, metadata, netflow, etc.) across individual security tools. Applying sophisticated analytics and threat intelligence, XDR supplies the full context needed for an attack-centric view of an entire chain of events across security layers.

Difficulty doing investigations

Faced with many logs and alerts but no clear indicators, it's difficult to know what to look for. If you find an issue or a threat, it's hard to map out its path and impact across the organisation. Performing an investigation can be a time-consuming, manual effort, if there are even the resources to do it. XDR automates processes by eliminating manual steps and provides rich data and tools for analysis that would be impossible otherwise. Consider, for example, automated root cause analysis, in which an analyst can clearly see the timeline and attack path (that may cross email, endpoints, servers, cloud and network) and dive down to assess each step of the attack in order to enact the necessary response.

And ultimately … slow detection and response times

The result of the challenges mentioned is that threats go undetected for too long, subsequently increasing the response time, which raises the risk and consequence of an attack. Cross-layered detection and response ultimately leads to much needed improvements in threat detection rates and response times. Increasingly, mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) are measured and monitored as key performance metrics for security organisations. Likewise, solution value and investments are evaluated in terms of how they drive these metrics and thus reduce the enterprise's business risks.

XDR vs. EDR

XDR provides the evolution of detection and response beyond the current point-solution, single-vector approach.

Clearly, endpoint detection and response (EDR) has been enormously valuable. However, despite the depth of its capability, EDR is ultimately restricted because it can only look at managed endpoints. This limits the scope of threats that can be detected as well as the view of who and what is affected and thus, how best to respond.

Likewise, Network Traffic Analysis (NTA) tools' purview is limited to the network and monitored network segments. NTA solutions tend to drive a massive amount of logs, so the correlation between network alerts and other activity data is critical in order to make sense and drive value from network alerts.

The industry has made great strides in detection and response, but to date, capabilities have been delivered via an individual solution and security layer; thus, data collection and analysis benefits have remained siloed. XDR evolves detection and response into a consolidated, centralised activity that delivers results that are greater than the sum of the parts.

Augmenting the SIEM

Organisations use SIEMs to collect logs and alerts from multiple solutions. While SIEMs allow companies to bring together a lot of information from multiple places for centralised visibility, it results in an overwhelming number of individual alerts. Those alerts are difficult to sort through in order to understand what is critical and needs attention. Correlating and connecting all of the information logs to gain a view of the larger context is challenging with SIEM alone.

Conversely, XDR collects deep activity data and feeds that information into a data lake for cross-layer sweeping, hunting, and investigation. Applying AI and expert analytics to the rich data set enables fewer, context-rich alerts, which can be sent to a company's SIEM solution. XDR doesn't replace the SIEM but augments the SIEM, reducing the time required by security analysts to assess relevant alerts and logs and decide what needs attention and warrants deeper investigations.

Capability imperatives

Multiple security layers beyond the endpoint

- To perform cross-layered detection and response, you need at least two layers, and the more the better: endpoint, email, network, servers and cloud workloads.
- XDR broadens the scope of detection and response across more than just endpoints. It extends EDR to important additional activity areas. Email, for example, is critical given it is the No. 1 attack source.
- XDR feeds activity data from multiple layers to a data lake so all the information that is applicable, in the most relevant structure, is made available for effective correlation and analysis.
- Pulling from a single vendor's native security stack prevents vendor/solution proliferation and provides for an unmatched depth of integration and interaction between detection, investigation, and response capabilities.

Purpose-built AI and expert security analytics

- Collecting data is one benefit of XDR, but applying analytics and intelligence to drive better, faster detection is XDR's end goal.
- As collecting telemetry becomes a commodity, value is driven by security analytics combined with threat intelligence that can turn information into insight and action.is critical given it is the No. 1 attack source.
- An analytics engine fed by native, intelligent sensors provides for more effective security analytics than can otherwise be achieved on top of third-party products/telemetry. Any given vendor will have much deeper understanding of their own products' data than a third-party's data. Priority should be given to XDR solutions that are purpose-built for a vendor's native security stack to ensure optimised analytical capabilities.

Single, integrated and automated platform for complete visibility

- XDR enables more insightful investigations because you can make logical connections from the data provided within a single view.
- Having a graphical, attack-centric timeline view can provide answers in one place, including:

  How the user got infected
  What was the first point of entry
  What/who else is part of the same attack
  Where the threat originated
  How the threat spread

- XDR augments security analysts' capabilities and streamline workflows; it optimises teams' efforts by speeding up or removing manual steps, and enables views and analyses that can't be done immediately.
- Integration with SIEM and SOAR enables analysts to orchestrate XDR insight with the broader security ecosystem.