Whitepaper

cynet

# XDR: Redefining the Game for MSSPs

Learn how the three different XDR approaches can help MSSPs boost their profitability from SMB and SME and improve their protections.

SMBs and SMEs are increasingly turning to MSSPs to secure their businesses because they simply do not have the budgets or skills to design, acquire, integrate, operate and manage an effective security technology stack. However, it's also challenging for MSSPs to piece together an effective but manageable security technology stack to protect their clients, especially at an affordable price point.

Fortunately, the emerging technology category Extended Detection and Response (XDR) can help MSSPs consolidate security products while providing superior protection, all at a much lower cost than the traditional multi-product technology stack. With the surge in interest in XDR, the vendor community is scrambling to align their offerings within this burgeoning category.

Below we provide an overview of the three predominant approaches technology vendors are using to provide XDR so MSSPs can better understand the benefits and shortcomings of each.

# What is XDR?

Most security professionals are at least partially familiar with the concept of XDR.  XDR is generally seen as the evolution of Endpoint Detection and Response (EDR) solutions, extending EDR threat detection and response beyond the endpoint. While we may argue that this is the aim of security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools, these tools never quite lived up to the promise. With a laser focus on threat detection and incident response, XDR is now poised to deliver what these other technologies couldn't – a unified, workable detection and response platform.

Generally, XDR should provide the following capabilities - at a minimum:

- Extend telemetry beyond endpoint signals
- Correlate security data to improve accuracy and consolidate alerts into incidents
- Expand, coordinate and automate response actions across the environment

Based on these requirements, we can see how an XDR platform might be considered as an improvement and/or replacement of other security technologies – assuming that the particular XDR solution actually delivers on its promise. For example, if an XDR platform natively provides network telemetry signals, it might allow a company to replace their current NDR solution. The added benefit, which we'll discuss below, is that network telemetry is fully integrated into the XDR platform out of the box. This obviates the need for expensive and complex integration and ultimately can lead to better protection due to the signals being natively built into the XDR analytics engine.

Taking the key XDR capabilities above, we can see how each might replace existing technology or add capabilities that may otherwise be missing.

- Extended telemetry – potentially provide signals and data that would otherwise require additional technologies such as NDR, UBA Rules, CASB, CSPM, Deception, etc.
- Correlate security data – potentially replace expensive and complex SIEM technology
- Expand response actions – potentially replace expensive and complex SOAR technology

Consolidating these technologies into a single, unified offering also makes these technologies accessible to security teams that might otherwise not have the budget or bandwidth to deploy and support them.

# What's The Current State of XDR Technology?

Although XDR was initially envisioned as an improvement and expansion of EDR, the actual manifestation of XDR in the market is highly dependent on the solution providers' core capabilities. Because many market participants want to align with a burgeoning technology, it seems that any vendor that is tangentially associated with any element of XDR wants to be an XDR provider. This, unfortunately, has led to considerable market confusion and worse, a pile of solutions that will likely not deliver on the initial promise of XDR.

As Jon Oltsik of Enterprise Strategy Group (ESG) adroitly pointed out, "No one owns the definition of XDR". However, from reading leading industry analyst and technology vendor reports and interviews it is obvious that everyone wants to own the definition of XDR. Technology vendors, of course, have their own agenda to sell their solutions. For emerging technologies, some Industry analysts typically only see what technology vendors feed them, leading them to mimic vendor viewpoints. So caveat emptor – in this new market buyers must do far more due diligence and comparative analysis than normal before selecting an XDR provider.

Generally speaking, there are three main technology approaches to XDR, each with benefits and drawbacks.

Each approach is fundamentally based on the current set of offerings provided by major market participants.

## Native XDR

A single vendor that offers all components of an XDR solution is considered Native XDR. This means that the buyer will not need to purchase and integrate additional technology solutions into the Native XDR platform to enjoy the benefits.

### Advantages

On the positive side, a Native XDR platform is fully integrated and operational out of the box. Everything works seamlessly – no signal normalization and integration is required, no complex application and integration testing is required every time a platform component is updated, no training and operating multiple solutions, and no extra expense. A Native XDR will allow organizations to replace one or more existing security tools (such as EDR, NGAV, NDR, etc.) to make the purchase more cost efficient. It also allowsorganizations to benefit from additional protections (such as EDR, NGAV, NDR, etc.) that they otherwise could not afford to purchase and/or operate.

### Disadvantages

On the other side, a Native XDR platform is what it is. Whatever telemetry, analytics and response capabilities provided in the platform is what you get.

If you want additional sources of telemetry, additional technologies will need to be purchased separately. If you want the additional telemetry integrated with signals from the Native XDR platform, you'll have to figure out how to accomplish that separately. Of course, the Native XDR solution could provide all the capabilities needed.

## Open XDR

An XDR platform that requires integration with multiple third-party providers, especially for telemetry, is considered an Open XDR platform. An Open XDR platform integrates and correlates signals from 3rd party tools for threat detection and also relies on the 3rd party tools to implement suggested response actions. An Open XDR platform essentially provides the analytics engine that orchestrates the various signals and response actions. Some Open XDR platforms integrate with existing SOAR tools and some provide SOAR functionality directly.

### Advantages

Open XDR platforms allow companies to continue using current security solutions or whichever 3rd party solutions they choose – as long as the tools can integrate with the XDR platform. This provides tremendous flexibility and allows organizations to select so-called best of breed tool components.

### Disadvantages

The notion of an Open XDR platform that seamlessly fuses multiple 3rd party tools sounds appealing, but there are several drawbacks to consider with this approach. Remember, openness and flexibility were key attributes of SIEM systems, and look where that got us. One of the core drivers for developing XDR is the failure of a centralized collection and correlation engine (namely SIEM) to deliver on its promise. SIEMs are expensive, complex, fail to detect threats and are replete with false positive alerts. Why would an Open XDR system fair differently?

While a core driver of XDR is cost and complexity reduction, an Open XDR adds the cost of yet another new technology. And it requires the organization to keep most of the technologies already in place, and maybe even add additional tools. It also requires extensive integration with 3rd part tools but does claim to be easier to integrate than SIEM solutions.

However, when 3rd party tools change or upgrade, further integration and testing cycles are inevitable.

In this way Open XDR is more of an upgraded SIEM vs. an extended EDR solution.

## Hybrid XDR

A single vendor offering all (or most) components of an XDR solution, while also allowing 3rd party tool integration is considered Hybrid XDR. This means that the buyer will not necessarily need to purchase and integrate additional technology solutions into the XDR platform to enjoy the benefits, but can do so to extend or replace the technologies native to the platform.

### Advantages

A Hybrid XDR can essentially provide the benefits of both Native and Open XDR platforms. With the inclusion of native tools, a Hybrid XDR platform may be fully integrated and functional out of the box. If different or additional security technologies are desired, 3rd party tools can be integrated into the Hybrid XDR platform. Clients may be able to initially leverage a Hybrid XDR out of the box and then potentially augment the solution with additional tools if desired.

### Disadvantages

While most Hybrid XDR providers claim that natively provided tools are seamlessly integrated into the platform, sometimes the level of integration is no better than that provided by the Open XDR providers. Because most large technology vendors with a

library of security offerings originally developed (or acquired) the tools to be sold separately, they have to back-integrate their toolset. This can lead to substandard detection when telemetry sources are not properly correlated and analyzed as well as disjointed response capabilities due to actions being driven from individual components.

Additionally, most Hybrid XDR providers offer a limited set of native capabilities, relying on 3rd party integrations to fill out coverage gaps. This means that some Hybrid XDR providers suffer the same disadvantages as Open XDR providers, including added costs for additional 3rd party solutions and tool integration issues.

# What Does This Mean for MSSPs

If XDR delivers on its promise, it can provide multiple benefits to MSSPs. Today, MSSPs source, purchase, integrate and maintain multiple security solutions to protect their clients' environments. Simplifying, automating and reducing the cost of this effort leads to meaningful efficiencies and cost savings. Moreover, an integrated, fully functioning security toolset also improves protection capabilities.

## Cost savings

MSSPs can significantly reduce security technology costs through tool consolidation. This manifests in multiple benefits, including:

- Lower vendor cost.
- Lower integration time and cost.
- Additional capabilities potentially included at no extra cost.
- Resource efficiencies through extensive automation, single pane of glass management, improved detection and remediation accuracy.

## Improved protection

Leveraging a consolidated, integrated XDR platform also leads to better threat protection, including:

- Expanded visibility across client environments.
- Better and faster signal correlation.
- Reduced manual analysis and tracking.
- Automated response actions, potentially including incident investigation and remediation across the environment.
- Vendor updates automatically propagated through system.

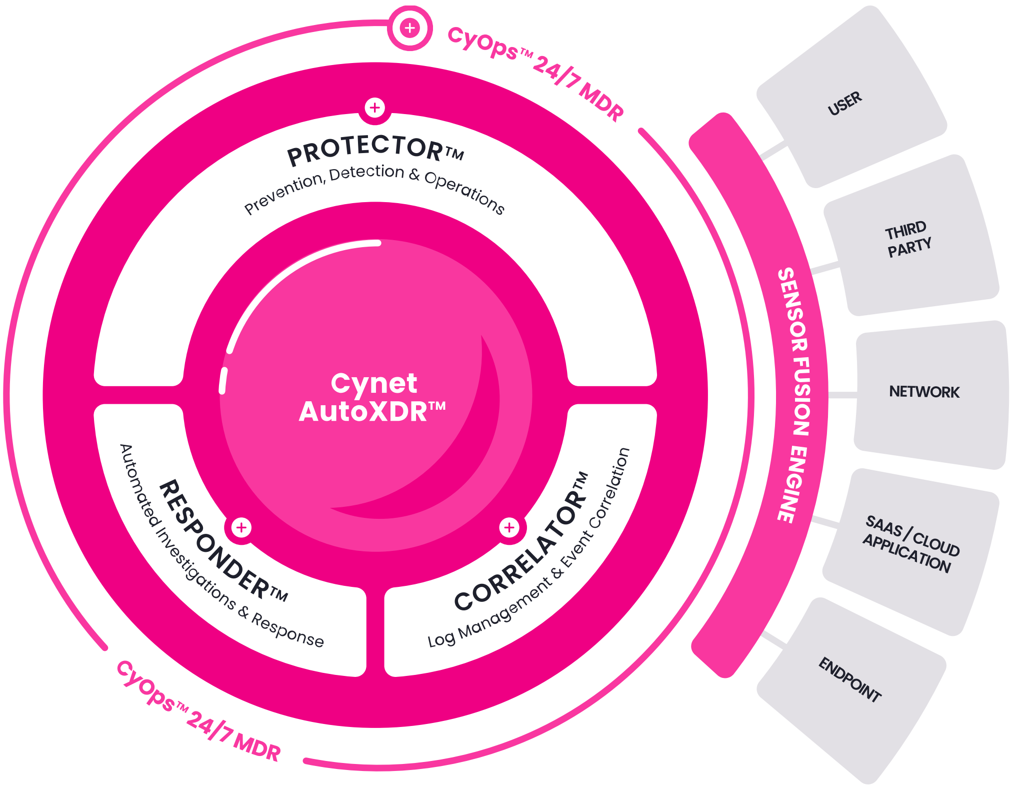
The benefits MSSPs derive from different XDR platforms will vary greatly depending on the providers approach and actual implementation of that approach. While the promise of XDR is great, MSSPs must be wary of the current crop of XDR solutions as security solution vendors are clamoring to align with this burgeoning technology, regardless of their ability to deliver.

Unfortunately, there is not one clear market definition of "XDR" yet, so available solutions vary greatly on their ability to deliver improved profitability and protections to MSSPs. Fortunately, client referrals are more available now that some XDR providers have multiple implementations operational. And, most XDR solutions, including ease of implementation, can be easily assessed with POV trials.

# About Cynet

With Cynet, MSSPs increase profitability by consolidating multiple required cybersecurity tools in a single, all-inclusive XDR platform. Cynet XDR platform provides the most extensive set of native telemetry and automated remediation capabilities available in the market. Cynet XDR natively includes EDR, NGAV, NDR, UBA Rules and Deception technologies to provide comprehensive breach protection on one unified platform. This multi-layered approach can see threats coming from any direction, even when novel or complex means of evading detection are used, thereby improving client protections.

Fully automated response capabilities turn alarms into immediate preventative actions that analyze the root cause of the attack and then remediate all attack components, all without needing action from the MSSP team. Included with the XDR platform are 24/7 MDR services that proactively look for threats and lead (or support) the incident response effort. Cynet MDR services can act as your SOC or augment your existing customer support infrastructure.



Moreover, Cynet provides SaaS Security Posture Management (SSPM) and Centralized Log Management (CLM) solutions fully integrated into the Cynet platform. With an intuitive user interface, security analysts can access all Cynet capabilities from a single pane of glass.

More than just a complete solution for autonomous breach protection, Cynet raises the bar for detection and response. By integrating more critical security tools on one seamless platform and then backing that platform with a dedicated MDR team, Cynet runs cybersecurity with unparalleled visibility, speed, and coordination. Crossed wires, missed signals, and delayed responses are not obstacles anymore once the core features of cybersecurity work in perfect sync in a single, integrated, natively built platform.

Learn More