

# Can Your XDR Stop a Hybrid Attack?

Use this checklist to align your AI-driven XDR with the challenges brought on by today's hybrid attacks.

## Why is it so difficult to defend against hybrid attacks?

### 1 Exposure

Getting integrated real-time coverage across the hybrid attack surface is complex.


### 2 Latency

Correlating individual alert streams to get accurate threat signal is highly manual.

### 3 Noise

Gaining control of attacks hidden in a mess of alert noise is close to impossible.


### But with the right AI-driven XDR you have:



The **COVERAGE** to see attacks?



The attack signal **CLARITY** to keep pace with attacks?






The **CONTROL** needed to stop attacks?

So, how does an AI-driven XDR reduce exposure, remove latency, and help your SOC move past security alert noise to stop hybrid attacks? Make sure your solution delivers the following:




### Reduces exposure with the right Coverage:

-  **Integrated hybrid attack coverage** in one place — consolidated signal across network, identity, and cloud eliminates blind spots to lateral movement and hybrid attack progression. Attackers will expose any surface, so every attack surface needs coverage for post compromise activity.
-  **AI-driven coverage** spans hybrid domains and identifies attacker behaviors for both known (MITRE) and emerging attacker techniques. Your solution should pull in native AI-driven signal, third party signal and support signatures.
-  **XDR is only possible** with NDR (network detection and response) coverage, and NDR is not possible without ITDR (identity detection and response). When attackers compromise identities, they gain the keys to your network.

### Removes latency with accurate signal Clarity:

-  **AI-driven attack signal** can remove latency by automating threat identification, validation, correlation, and prioritization. SOC teams should be able to use a clear attack signal to focus their time and talent on what matters most.
-  **AI / ML** should automatically analyze detection patterns, score event relevance, and distinguish malicious from benign. You should effortlessly know exactly what malicious activities are happening.
-  **AI-driven prioritization** can evaluate each entity to prioritize hosts and/or accounts under attack so analysts know what events are urgent, eliminating hours spent on alert management and maintenance. Without digging, you get a clear view of what needs to be addressed.

### Delivers Control that maximizes talent

-  **Investigation** options that instantly help junior analysts with lighted pathways or can be used by seasoned analysts for custom queries of network, identity and cloud metadata. It's easy to investigate and hunt for real attacks.
-  **Response** controls to lock down infected entities manually or automatically, along with integrated response controls for EDR, SOAR, ITSM and firewalls to enact playbooks and remediate incidents with confidence. If you can't respond efficiently, you can't stop an attack.
-  **Managed Extended Detection and Response (MXDR)** availability for 24x7 managed detection, investigation and response support for tasks including threat monitoring, incident response, platform tuning, expertise and more. Sometimes you just need more security resources, and that's ok.

## Where can you find out more about AI-driven XDR?

Glad you asked.

[Start here](#)

COVERAGE  
CLARITY  
CONTROL