

Can Your XDR Stop a Hybrid Attack?

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

Why is it so difficult to defend against hybrid attacks?

Ci: Exposure

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

280 Latency

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

Noise

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

But with the right Al-driven XDR you have:





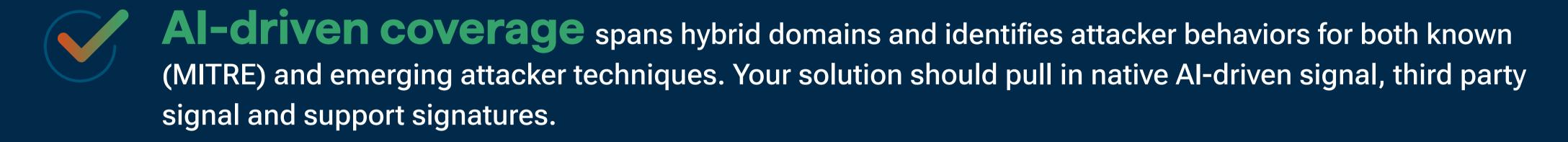


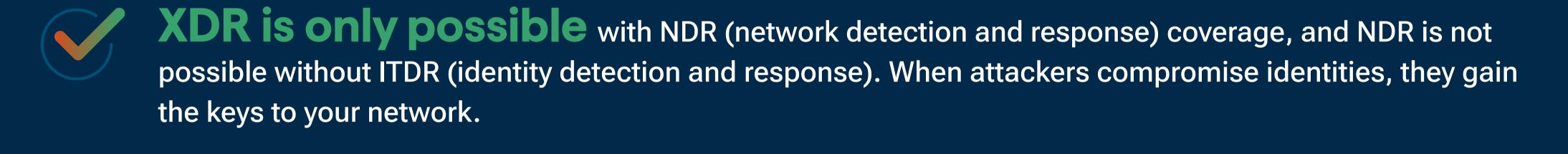
So, how does an Al-driven XDR reduce exposure, remove latency, and help your SOC move past security alert noise to stop hybrid attacks?

Make sure your solution delivers the following:

Reduces exposure with the right Coverage:







Removes latency with accurate signal Clarity:

Al-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.

Al / ML should automatically analyze detection patterns, score event relevance, and distinguish malicious from benign. You should effortlessly know exactly what malicious activities are happening.

Al-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 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.

Managed Extended Detection and Response (MXDR) availability for 24x7

more about Al-driven XDR?

Where can you find out

Start here

Glad you asked.