Extending beyond EDR with integrated signal at speed and scale

When it comes to stopping high-speed hybrid attackers, integrated signal at speed and scale is the only answer.

Endpoint Detection and Response (EDR) tools have grown in popularity based on their ability to detect and stop attackers targeting employees via the endpoint. However, mounting evidence suggests EDR is only one piece of the threat detection and response equation. As EDRs have become a mainstay for enterprises, attackers have evolved their methods and tradecraft to get around them.

The threat landscape is getting demonstrably more hazardous and the siloed view of EDRs is not suitable for a modern hybrid cloud environment that encompasses the data center network, public cloud, SaaS and identity. Given that EDRs only provide endpoint visibility, security teams need to supplement their EDR signal with integrated signal across the entire hybrid attack surface.

Key challenges to consider

- **EDR can't be everywhere:** EDRs do not run on vendor appliances, contractor/BYOD or IT/OT equipment, which leads to significant gaps in visibility across the enterprise.
- **EDR can be bypassed:** There is an entire ecosystem highlighting the currently available EDR exploits, vulnerabilities and techniques publicly published for attackers to leverage. Once a compute asset is compromised, it is no longer reliable from an EDR perspective.
- **EDR only takes a host-centric view:** Having a host-centric view is important, but in today's growing digital footprint, hosts are connected and communicate with other systems over the network, cloud, SaaS and Identity. Relying only on EDR will not provide the pivotal insights needed to protect an entire hybrid cloud environment.
- **EDR can be noisy:** EDRs implement a reactive approach where security teams have to sift through thousands of alerts that require dedicated head count analyzing and assessing each alert before taking action.

Key benefits of integrated hybrid attack signal:

- Eliminate 90% of your attack surface blind spots, proactively identify 3x more threats
- Cover >90% of hybrid cloud MITRE ATT&CK techniques
- Reduce detection engineering time from months to days
- Automate and improve quality of threat detections over native tools
- Integrate context, workflow and response from the EDR of your choice
- Sees attacks that expose gaps and bypass prevention controls
- Provide a holistic view of attacks across all domains

Key criteria to consider

Thinking like a hybrid attacker

63% of SOC analysts say their attack surface has significantly increased in the past three years.

Where have hybrid attackers already infiltrated our environment? To move at the speed and scale of hybrid attackers, security teams need to start thinking like a hybrid attacker. Today, SOC teams rely on too many disparate detection and response technologies spanning endpoints (EDR), networks (NDR), IaaS, PaaS, SaaS (CDR), and identity (ITDR) — making threat detection an increasingly complex problem to tackle. There are simply too many siloed tools sending too many threat detection signals to SOC analysts. Hybrid attackers thrive in this complex environment often hiding from detection, or simply blending with thousands of detections. Either way, security teams need to stop thinking about individual attack surfaces (endpoint, identity, cloud, network), and start thinking like hybrid attackers who see one giant attack surface. How consolidated and integrated in your hybrid attack signal? The more siloed and fragmented the signal, the greater the latency detecting hybrid attacks. And we all know, attackers thrive in SOC latency.

Moving at hybrid attacker speed

71% Nearly three-quarters (71%) of analysts admit their organization may be compromised and they don't know about it yet.

Where are hybrid attackers moving laterally, progressing inside your environment? Once hybrid attackers have infiltrated and pose a risk to the organization, correlation and context around lateral movement and attack progression becomes critical for both SOC defenders and CSIRT responders. Again, too many tools can slow the investigation and response process. The more SOC and CSIRT teams need to jump from tool to tool, the longer it takes them to piece together the narrative of the attack, and the more time the attacker has to reach the crown jewels and exfiltrate data. Moving at hybrid attack speed requires removing as much latency in detection, triage, prioritization, investigation and response. How consolidated and integrated is your hybrid attack context? The more siloed and fragmented the threat context, the greater the latency in isolating and containing a hybrid attack in progress. Hybrid attackers thrive in SOC latency.

Keys to success:

Coverage: Integrated hybrid attack surface visibility. Unify and consolidate attack telemetry across your entire hybrid attack surface including identity, public cloud, SaaS and data center networks. In addition, unify signature-based detection, AI-driven behavior-based detection and threat intel across the hybrid attack surface for complete coverage of hybrid attacker methods. Unification of attack surface telemetry i.e. visibility and signal to reduce hybrid attack detection latency.

Clarity: Integrated, real-time, AI-driven attack signal. Harness AI to automate threat detection, triage and prioritization across your hybrid cloud domains in real-time. Shift from event-centric threat detection to entity-centric attack signal. Entity-centric attack signal provides higher-fidelity alerts on hosts and accounts under attack, removing the need to triage hundreds if not thousands of threat events per day. This cuts down on analyst burnout and has proven to boost analyst productivity more than 2x. Consolidating threat-events into attack-entities reduces hybrid attack prioritization latency.

Control: Integrated, automated, co-managed response. Arm your SOC analysts with integrated, automated and co-managed investigation and response capabilities that move at the speed and scale of hybrid attackers. Remove as much investigation and response latency in analysts' workflows by putting all of the context and controls they need at their fingertips. In addition, leverage co-managed services to add reinforcements to your SOC team when talent resources are scarce, and skills are lacking. Integrating and consolidating hybrid attack context, controls and co-managed resources reduces hybrid attack investigation and response latency.

When it comes to extending beyond EDR with integrated hybrid attack signal, and reducing hybrid attack detection, investigation and response latency, Vectra AI can help. The Vectra AI Platform delivers the integrated signal powering extended detection and response (XDR) by providing hybrid attack surface coverage across public cloud, identity, SaaS and data center networks, real-time Attack Signal Intelligence that prioritizes entities under attack, and integrated, automated and co-managed response that stops attacks from becoming breaches.

Learn more about the Vectra AI Platform

See the Vectra AI Platform in action

Explore the Vectra AI Platform

Schedule a personal demo of the Vectra AI Platform

About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai