VECTRA

BEST PRACTICES

Go beyond your IDS with the integrated hybrid attack signal

An IDS replacement strategy — integrated hybrid attack signal at speed and scale.

The Problem

IDS (Intrusion Detection Systems) solutions aren't fit to detect sophisticated attacks across today's hybrid cloud attack surface. SOC teams need security tools that aren't just perimeter focused, but rather provide visibility and coverage for the entire hybrid cloud infrastructure. Today's attackers can wreak havoc on your organization, meanwhile adding solutions to manage and monitor, can significantly slow down your security team with an abundance of noise and false positives.

The attack surface enterprises face today is becoming more hazardous by the minute and the siloed view provided by IDS isn't enough in a modern hybrid cloud environment that encompasses the data center network, public cloud, SaaS and identity. Security teams need to replace their IDS with integrated signal across the entire hybrid attack surface.

Key challenges to consider

IDS challenges

- **IDS is not everywhere:** IDS solutions do not have visibility across the entire hybrid cloud infrastructure, leaving significant gaps across the enterprise.
- **IDS is noisy:** IDS tools operate based on a reactive approach, leaving SOC teams sifting through thousands of alerts and requiring dedicated head count and expertise to analyze and assess each alert before acting.
- **IDS is not entity-centric:** IDS is not entity-centric and can't provide the pivotal insights needed to protect your entire hybrid cloud environment or deliver advanced investigation, or response capabilities.

Key benefits of an integrated hybrid attack signal

- Eliminate 90% of 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.
- See 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.[1]

Where have hybrid attackers already infiltrated your 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 IDS, networks (NDR), IaaS, PaaS, SaaS (CDR), and identity (ITDR) making threat detection an increasingly complex problem to solve. 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 in among a sea of 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 is your hybrid attack signal? The more siloed and fragmented the signal, the greater the latency detecting hybrid attacks. Attackers thrive in SOC latency.

Moving at hybrid attacker speed

71% Nearly three quarters of analysts admit their organization may be compromised and they don't know it yet.[2]

Where are hybrid attackers moving laterally and 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. Too many tools slows investigation and response. The more SOC and CSIRT teams need to jump from tool to tool, the longer it takes them to piece together the narrative of an 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.

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, reduces 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 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 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.

The Vectra AI Platform is the only security solution that identifies threats in real-time. Vectra AI provides AI-driven Attack Signal Intelligence™ to produce the most integrated hybrid attack signal to zero in on tactics, techniques and procedures (TTPs) attackers use to hide. Go beyond IDS solutions and truly deliver a comprehensive hybrid cloud Threat Detection Identity and Response (TDIR) solution right out of the box.

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.

*Source 1 & 2: 2023 State of Threat Detection Report, The Defenders' Dilemma

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