Shifting from legacy PCAP to AI-driven threat detection

Why you can't rely on yesterday's PCAP for today's threats.

The Problem

According to The State of Threat Detection 2023, 97% of security analysts worry they'll miss a relevant security event[1]. As new, evasive threats are being conducted daily — threat detection and response is a top priority for cybersecurity teams securing hybrid cloud environments. In fact, nearly two-thirds of analysts say the size of their attack surface has increased in the past three years.[2]

Enterprises leveraging Packet Capture (PCAP) solutions are relying on a primarily network permitter monitoring solution that takes more space than needed and cannot address hybrid attacks happening in real-time that span the data center, identity, SaaS and public cloud infrastructure.

In an evolving hybrid cloud world, including both on-premises and cloud infrastructure — PCAP does not cut it. PCAP strengths primarily rely on network monitoring for on-premises environments, leaving huge gaps and vulnerabilities for bad actors to exploit.

PCAP Challenges

- **Operational inefficiency:** Constantly maintaining and managing the massive storage volumes that impact performance and slow down SOC teams. Additionally, PCAP solutions only utilize a very limited subset of metadata.
- **Seeing through encryption:** 97% of internet traffic is encrypted. Getting any real value from PCAP requires full decryption for north and south traffic, which requires various resources and time.
- **Modern threat detection:** Lack of AI-driven detection — threat detection models are mainly based on known attacks and cannot accurately detect modern live-off-the-land attacks. PCAP is mainly implemented as a network monitoring and response system — not functioning in real-time.
- **Investigation challenges:** PCAP solutions do not enable investigation for today's hybrid cloud threats and are based on reactive models. They do not enable instant or advanced investigation for today's hybrid cloud attacks.
- **Costs constraints:** Storing petabytes of PCAP data is extremely expensive and oftentimes not a good use of resources. PCAP solutions offer malware analysis, but not more effectively than other cybersecurity solutions such as Endpoint Detection and Response (EDR), among others.
- **Integration restrictions:** PCAP systems don't integrate well with other solutions such as SIEMs, forcing SOC teams to constantly toggle between various solutions that don't communicate, contributing to tool sprawl and analyst burnout.
- **Privacy concerns:** By collecting all of an organization's sensitive data, PCAP solutions can contribute to privacy violations by having to run encryption methods on data in order to provide forensics back to the SOC.

Key criteria to consider

Thinking like a hybrid attacker

SOC teams must put on their attacker thinking caps and assess where hybrid attackers have or would target and infiltrate. Today, SOC teams rely on various detection and response technologies such as IDS and PCAP solutions that primarily focus on the network perimeter — making threat detection a complex challenge. There are too may siloed solutions sending too many threat detection signals to SOC analysts. Security teams need to shift their focus from specific attack surfaces, and start thinking like attackers who see one giant attack surface. The more siloed and separate your attack signal, the more you increase latency when detecting hybrid attacks that are looking to execute malware or a successful data breach.

Moving at hybrid attacker speed

Hybrid attackers who want to bypass your legacy PCAP solutions focus on the metadata that you might not be parsing through in that specific instance. Attackers are also looking to move north, south, east and west across your environment in lateral movement attempts. When an attacker has penetrated your environment, the correlation and context around all of their movement is pivotal to assess the attack progression within your hybrid cloud. Parsing through the vast amount of metadata, then relying on encryption before being able to really investigate an incident, tremendously slows down your investigation and response process. Moving at attacker speed requires removing as much latency early in the detection process and then scaling on top of that with triage, prioritization, investigation and response. Detection latency is what gives the attackers an advantage to move fast across the attack kill chain.

1 & 2 — Global Report: 2023 State of Threat Detection, The Defender's Dilemma

Keys to success:

To keep pace with today's evolving hybrid attacks, SOC teams can focus on prioritizing attacks in real-time by focusing on three key areas:

- **Attack surface coverage:** Integrated and consolidated attack telemetry across your entire hybrid attack surface that provides comprehensive visibility across identity, public cloud, SaaS and data center networks. In addition to unified signature-based detection, AI-driven behavior-based detection, and threat intelligence across the hybrid cloud for complete coverage on all hybrid attacker methods.
- **Attack signal clarity:** Integrated, real-time AI-driven attack signal. Harness AI to automate threat detection, triage and prioritization across your hybrid cloud environment in real-time. Take the focus off of event-centric threat detection to entity-centric attack signal. Entity-centric attack signal provides high-fidelity alerts on hosts and accounts under attack at any given moment. In doing so, this drastically reduces analyst burnout and helps improve overall productivity. Moving to an entity-centric approach reduces the hybrid attack prioritization latency.
- **Integrated control:** 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 from your analyst's workflow by putting all the context and controls right at their fingertips 24/7. In addition, leverage co-managed services to add reinforcements to your SOC team when talent resources are scarce, and skillsets are lacking. By integrating and consolidating all of the hybrid attack context, controls and co-managed resources — you can reduce hybrid attack investigation and response latency.

When it comes to retiring your PCAP for 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 attack surface coverage across public cloud, identity, SaaS and data center networks. Patented Attack Signal Intelligence™ prioritizes entities under attack, along with an 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