Using AI to Detect and Stop Lateral Movement in the Cloud

The Vectra AI Platform for AWS enables modern SOC teams to reduce risks against advanced lateral movement attacks in your hybrid cloud.

Lateral movement is a tactic used by adversaries to expand their access by moving through an environment to reach their goals or targets (e.g. exfiltrate sensitive data, commandeer workloads). For years, lateral movement has been used to target on-premises networks based on network protocols and services such as Active Directory, SMB and NTLM, but as more and more organizations move to the cloud — attackers have followed.

Post compromise, attackers pursue numerous avenues for lateral movement in the cloud. For example, stealing credentials from a compromised virtual machine to pivot to other services — or leveraging elevated permissions to deploy resources in unused and unmonitored geographic regions. There are many instances of these methods manifesting in real world attacks.

The prevalence of connected hybrid environments makes this challenge worse. Adversaries in the hybrid cloud leverage novel techniques such as account misuse, compromised credentials and vulnerabilities to exploit trusted relationships — and move laterally between connected surfaces. The Vectra AI Platform for AWS is powered by patented Attack Signal Intelligence™ that takes an entity-focused approach to detecting lateral movement in hybrid cloud deployments, surfacing the most urgent threats for SOC teams to address.

Key benefits

WHY CHOOSE A PURPOSE-BUILT MODERN CLOUD DETECTION, INVESTIGATION AND RESPONSE SOLUTION?

- **Increased visibility in hybrid environments:** A single pane of glass with prioritized entities from across connected surfaces including data-center networks, SaaS, identity and public clouds such as AWS.
- **AI-driven detections:** A portfolio of advanced detections that surface sophisticated attacker behaviors across the cloud kill-chain and provide deep protection against compromised credentials, service abuse, privilege escalation and data exfiltration.
- **Preventing lateral movement:** Provides centralized monitoring for attacker behaviors attempting lateral movement across connected surfaces, while delivering an audit trail in a centralized UI. This greatly reduces the burden on SOC teams to manually corelate data from traditionally disjointed sources.

Key Challenges:

Gaps in hybrid cloud visibility: SOC teams need to have visibility into their entire hybrid cloud deployment encompassing data center networks, identity, SaaS and public clouds such as AWS; not solely depending on a singular source such as firewalls to detect threats in inbound and outbound traffic.

Technical depth in threat detection: SOC teams need advanced behavioral analytic capabilities across various connected surfaces without investing in disjointed tooling from multiple vendors that either do not integrate or simply leave gaps that sophisticated attackers can exploit to move laterally between surfaces.

Heightened operational challenges: With more tools comes increased overhead in tooling, time and manpower for SecOps. SOC teams need to protect their hybrid cloud deployments without overspending on resources and time to manually corelate data from various sources. This adversely impacts key SOC metrics such as the mean time to investigate (MTTI) and mean time to respond (MTTR).

Key criteria to consider

Overcoming cloud challenges doesn't have to be overly complicated or create more work for SOC teams. Consider the following:

Coverage for the hybrid cloud footprint: Modern hybrid attacks span multiple connected surfaces encompassing public cloud, data center networks, identity and SaaS. There is a need for a threat detection, investigation and response solution that surfaces threats from across these surfaces.

Focus on signal clarity: Leverage AI technology that not only identifies sophisticated attacker behaviors in real time, but also prioritizes findings so your SOC team can discern the important from the urgent.

Reducing SOC overhead: Operationalizing multiple tools and training SOC personnel can lead to high security costs for an enterprise where the ideal solution should enable easy investigations and streamline workflows for threats across attack surfaces.

Keys to success

- **Broad observability across hybrid deployments:** An AI-native solution for AWS seamlessly fits into the Vectra AI platform — surfacing and prioritizing threats not just from the cloud, but also from connected surfaces in a single plane of glass.
- **Real-time signal clarity powered by Attack Signal Intelligence™:** Leveraging Vectra AI's industry leading Attack Signal Intelligence to power purpose-built AI detection models and identify sophisticated threats in real time. The Vectra AI Platform uses AI for true source attribution, so SOC analysts do not have to correlate actions across temporary credentials to identify the original actor. This saves hours in investigation time.
- **Powerful workflows to enable investigations and remediation:** The Vectra AI Platform includes powerful features to investigate threats including key aggregated insights on prioritized entities as well as the ability to query raw logs enabling analysts to invest more cycles in active threat hunting. The solution also enables remediation either via automated enforcement or through integration with existing workflows leveraged by the enterprise.

Today, deployments are hybrid consisting of connected surfaces such as on-premises data centers, identity providers, SaaS offerings and public clouds. Sophisticated attackers aim to compromise one exposed surface and then move laterally to connected surfaces in service of their goals. These attacks manifest in various forms such credential theft, compromise of hosts in on-prem networks or identity-based threats that eventually pivot to key resources in public cloud environments. Modern SOC teams are on a mission to eliminate data breaches, disruption of services, and damage to an organization's reputation from attacks targeting these hybrid cloud deployments.

Once in the cloud, identification of these behaviors can be challenging and the longer an attacker can move undetected across the connected hybrid footprint, the greater the potential damage. With the Vectra AI Platform for AWS, SOC teams have broad visibility into threats across connected surfaces in a single pane of glass with a deep focus on identifying advanced lateral movement techniques in cloud environments. Vectra AI monitors behaviors across users and services in the cloud leveraging its Attack Signal Intelligence™ to prioritize threats and mitigate the risk of impact on an organization's footprint.

Learn more about the Vectra AI Platform

Schedule a Demo

About Vectra AI

Vectra AI is the leader in AI security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit www.vectra.ai.

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