AI-driven Security Stops Hybrid and Multicloud Threats

Raise your SOC efficiency by 85% and SecOps productivity by >2X.

The adoption of hybrid cloud means an easier path for attackers to bypass prevention controls, move laterally and exfiltrate data while going undetected. As workloads have shifted from the data center to IaaS, PaaS and SaaS services, attackers now target user credentials to access cloud resources. In fact:

- 83% of organizations saw multiple breaches in 2021
- 45% were cloud-based
- Average response time: 9 to 10 months

Key challenges addressed:

- Compromised credentials
- Cloud threat detection
- Securing SaaS, IaaS and PaaS
- Ever expanding attack surface
- Unknown threats

Attack surface expansion opens the door to unknown threats

Network expansion has created a new, hybrid and multicloud environment that cannot be protected by legacy network security focused on signatures and anomaly detection.

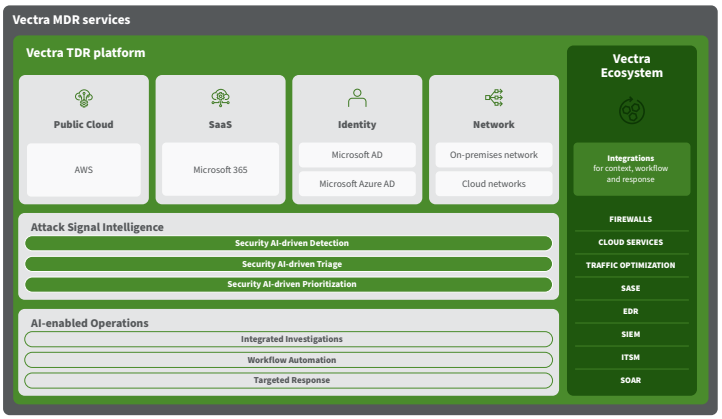
- **Securing identity, users and roles:** Attacks using compromised user credentials are hard for security solutions like cloud access security brokers (CASB) and web application firewalls (WAFs) to detect, as they look like legitimate user actions. If an external attacker is hard to detect, the threat posed by malicious insiders is even more challenging.
- **Securing SaaS applications and data**: Trying to implement virtual firewalls or CASB solutions to filter access to SaaS and cloud-native applications is cumbersome to maintain, disruptive to your employees and is easily circumvented by attackers. Cloud workload protection (CWPP) requires agents, while cloud security posture management (CSPM) requires constant tuning — both with limited visibility.
- **Securing IaaS and PaaS**: Infrastructure as a service (IaaS) and platform as a service (PaaS) are ever changing. As a result, you cannot confidently deploy a cloud application in your IaaS or PaaS environment in a secure manner. In fact, through 2025, Gartner states that 99% of cloud security failures will be the fault of the customer.

Vectra Threat Detection and Response platform and services

Our approach is simple. Defending against modern cyber attackers comes down to arming defenders with the right coverage, clarity and control. By harnessing Vectra's Security AI-driven Attack Signal Intelligence™, the Vectra platform empowers security teams with AI-driven detection, triage and prioritization to expose the complete attack narrative across the entire cyber kill chain.

Only Vectra provides:

- **Attack Coverage across 4 of your 5 attack surfaces**: cloud (IaaS and PaaS), SaaS, identity and networks — monitoring for attacker TTPs throughout the entire cyber kill chain and across hybrid and multicloud attack vectors.
- **Signal Clarity with Attack Signal Intelligence**: patented AI-driven technology automates threat detection, triage and prioritization, empowering security analysts to focus on the most urgent threats to the organization.
- **Intelligent Control with AI-enabled operations**: integrated investigations, automated workflows and targeted response actions optimize security investments in tools, processes and playbooks to boost SOC efficiency and effectiveness.



Vectra provides the hybrid cloud building blocks to future proof your cyber defense as your attack surface expands:

- Vectra Network Detection and Response (NDR)
- Vectra Cloud Detection and Response (CDR) for AWS
- Vectra Cloud Detection and Response (CDR) for M365
- Vectra Identity Detection and Response (IDR) for Azure AD
- Vectra Recall to query, investigate, hunt for threats
- Vectra Stream for security-enriched metadata lake
- Vectra Managed Detection and Response (MDR)

Security Outcomes

The Vectra platform enables your SOC to become more resilient, efficient and effective at detecting and stopping modern hybrid and multicloud attacks before a breach occurs.

Resiliency: Future-proof your expanding attack surface across 4 of 5 attack surfaces — cloud (IaaS and PaaS), SaaS, identity and networks.

- Deploys in hours, not weeks.
- Respond to attacks in minutes, not months.
- Reinforce SOC with Vectra MDR at the ready.

Efficiency: Cut time, cost and complexity and gain 85% more SOC efficiency.

- Unified threat visibility and context lowers SIEM costs and maintenance.
- Security AI-driven detection, triage and prioritization automates manual tasks.
- Native ecosystem integrations optimize existing EDR, SOAR and ITSM investments.

Efficacy: Arm human intelligence to be more effective boosting SOC analyst productivity 2x.

- Lower alert noise by 80% and reduce alert fatigue and analyst burnout.
- Provide context at analyst's fingertips to streamline workstreams and increase analyst throughput.
- Partner with Vectra MDR analysts to enhance skills and expertise defending against modern cloud-based attacks.

Only the Vectra platform harnessing Security AI-driven Attack Signal Intelligence breaks the spiral of security complexity with unrivaled signal clarity and automated threat detection, triage and prioritization. Transform your cloud security strategy with the intelligent signal that empowers security analysts to take intelligent action — move away from complexity, gain signal clarity and resolve urgent threats in minutes.

Schedule A Demo

Learn more about Vectra's platform

About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

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