Vectra Integrates with SentinelOne®, Providing Best of Breed Ecosystem Security

The adoption of hybrid cloud has led to an increased attack surface, making it easier for attackers to bypass prevention controls, infiltrate, compromise credentials, gain privileged access, move laterally and exfiltrate sensitive corporate data while going undetected.

To mitigate these challenges, Vectra and SentinelOne uncover the complete cyberattack narrative by combining coverage across the network and endpoint.

- **Vectra's Security AI-driven Attack Signal Intelligence™** takes a risk-based approach to cyberattacks while reducing manual tasks, alert noise, and analyst burnout with: AI-driven detections that think like an attacker, AI-driven triage to know what malicious, and AI-driven prioritization is so security teams can focus on urgent threats.
- **The SentinelOne Endpoint Protection Platform (EPP)** provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint with full-context and real-time forensics.

Key challenges addressed:

- Complete attack surfaces coverage
- Attack signal clarity
- Maximize SOC (Security Operations Centre) efficiency
- Security tool consolidation
- Reducing analyst workload

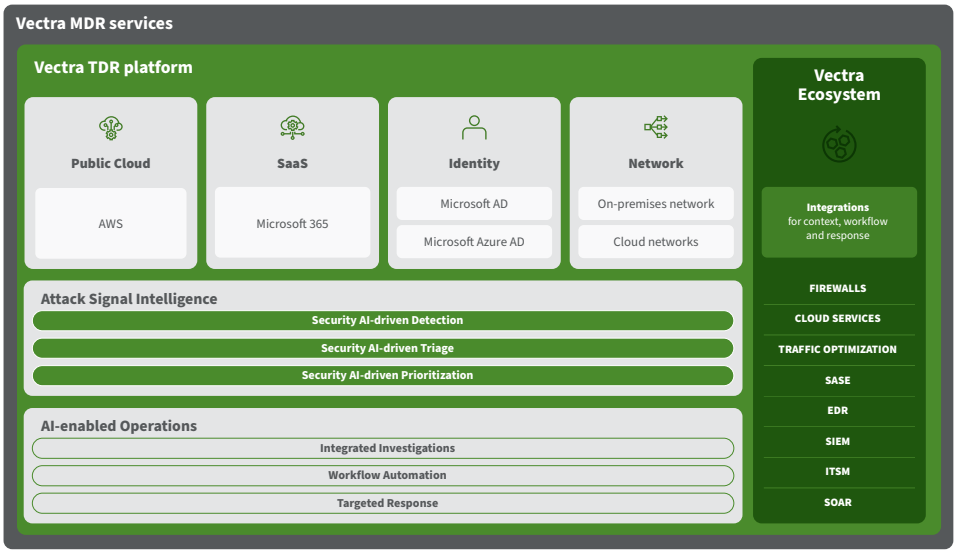
A security ecosystem that erases unknown threats

Defending against modern cyber attackers comes down to arming defenders with the right **coverage**, **clarity**, and **control**.

Attack surface coverage across all five attack surfaces: network (both on-premises and cloud-based), public cloud, SaaS (software as a service), identity and endpoint detection and response (EDR) via SentinelOne

Signal Clarity with Vectra's Security AI-driven Attack Signal Intelligence™: automate threat detection, triage, and prioritization across the cyber kill chain from execution, persistence and reconnaissance to command and control, evasion, access, escalation, lateral movement, and exfiltration.

Intelligent Control with AI-enabled operations: an intuitive user interface that puts answers at analysts' fingertips. Including automated workflows that reduce complexity and cost by automating manual tasks, while targeted response puts analysts in control with flexible response actions triggered automatically or manually.



When a threat is detected, Vectra and SentinelOne provide security teams with instant access to detailed information for quick verification and investigation. Host identifiers and host data from SentinelOne are shown automatically in the Vectra platform UI (User Interface). This enriches detection information from the network and cloud perspective and allows analysts to respond with urgency and stop any attacks.

A complete integration to get ahead of attackers

Traditional endpoint security tools are riddled with issues such as blind spots, easily circumvented signature-based detections and often require constant updates or scheduled run-cycles — making them unable to see and stop advanced threats. SentinelOne continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to detect and prevent advanced threats as they happen.

Vectra's Security AI-driven Attack Signal Intelligence empowers analysts to:

Think like an attacker

AI-driven Detections go beyond signatures and anomalies to understand attacker behavior and expose the complete narrative of an attack.

Focus on the malicious

AI-driven Triage reduces alert noise by distinguishing malicious from benign threat activity to expose malicious true positives while logging the benign.

Know what threats matter

AI-driven Prioritization reduces noise, automates alert triage and is 85% more effective at prioritizing the threats that matter most to the business.

What it means for your security team

Vectra and SentinelOne provide a powerful, simple, integrated solution to meet the needs of the modern SOC.

Security teams can leverage the power of integrated Vectra and SentinelOne solutions to deliver enhanced SOC effectiveness and efficiencies. Automation helps reduce the workload security teams face and enables them to erase unknown threats with faster response and threat resolution.

SOC teams experience:

- Autonomous multi-layered detection and response that covers all attack vectors, from the endpoint through the network to the cloud — even when offline.
- Enriched detections with endpoint context to take immediate action to stop attacks.
- Reduced alert fatigue with Security AI that does not rely on signatures or daily and even weekly updates.
- The ability to trigger different actions based on threat type, risk, and certainty.

Modern attackers are clever and continue to evolve with advanced tactics. Organizations need to ensure that security gaps are identified and secured. Vectra and SentinelOne help organizations deliver the attack surface coverage, signal clarity and intelligent control to ensure a compromise does not turn into a breach.

Resources to Learn More

About Vectra

Vectra® is the leader in Security AI-driven cyber threat detection and response for hybrid cloud. 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 (Managed Detection & Response) services to stay ahead of modern cyber-attacks. Visit www.vectra.ai

About SentinelOne

SentinelOne delivers autonomous endpoint protection through a single agent that successfully prevents, detects, and responds to attacks across all major vectors. Designed for extreme ease of use, the S1 platform saves customers time by applying AI to automatically eliminate threats in real time for both on premise and cloud environments and is the only solution to provide full visibility across networks directly from the endpoint.

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