VECTRA | SentinelOne

Vectra AI and SentinelOne: Autonomous Multi-Layered Detection and Response

Key Challenges

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. Traditional 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.

Solution Overview

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

Vectra AI's Network Detection and Response (NDR) technology and AI Platform take a risk-based approach to cyberattacks while reducing manual tasks, alert noise, and analyst burnout with AI-driven detections that map to the brains of attackers, AI-driven triage to know what is malicious, and AI-driven prioritization is so security teams can focus on urgent threats.

The SentinelOne Singularity™ Endpoint (EDR) technology and Singularity™ Platform provide 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.

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

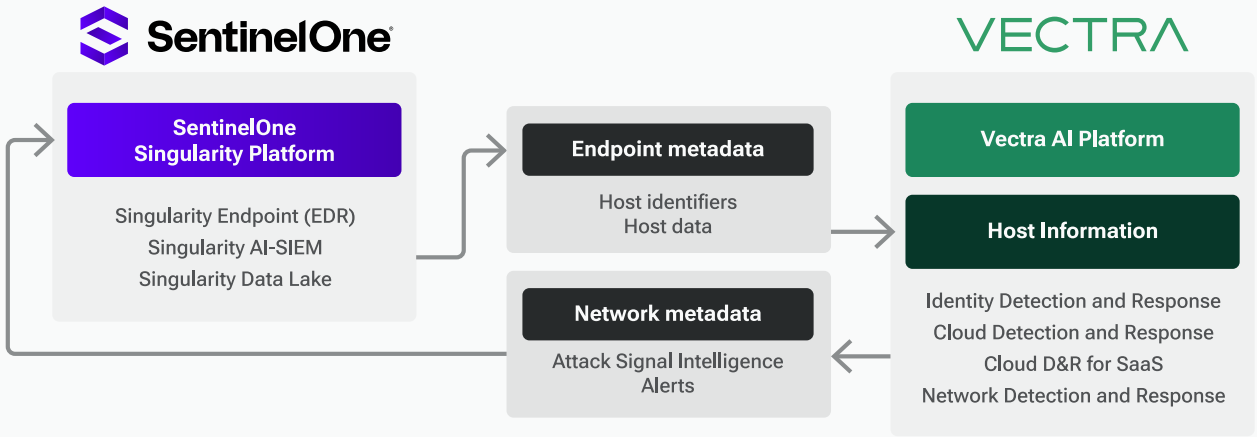
Solution Components:

- SentinelOne Singularity™ Endpoint (EDR)
- SentinelOne Singularity™ Platform
- Vectra AI NDR
- Vectra AI Platform

Key Benefits:

- Multi-layered detection and response that covers all attack surfaces from network to endpoint
- Maximized SOC efficiency and reduced alert fatigue with artificial intelligence that does not rely on signatures or daily and weekly updates
- Attack signal clarity through enriched detections with endpoint and network context to take immediate action and stop attacks
- Autonomous ability to trigger different response actions based on threat type, risk, and certainty
- Bi-directional technologies that communicate with each other seamlessly and in real-time

How it Works



1. When a potential threat is detected on either network or endpoint, Vectra AI and SentinelOne will provide security teams with instant access to detailed information for quick verification and investigation.

2. With a threat detected on an endpoint, SentinelOne Singularity™ Endpoint (EDR) will send host identifiers, host data, and endpoint metadata into the Vectra AI Platform to enrich detection information where it will be triaged and prioritized.

3. The same will happen on the flip side where Vectra NDR will send network metadata to the SentinelOne Singularity™ Platform when a potential network threat is detected.

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to 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 MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

About SentinelOne

SentinelOne® (NYSE: S) is a leading AI-powered cybersecurity platform. Built on the first unified Data Lake, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own. Leading organizations—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments – trust SentinelOne to Secure Tomorrow™. Learn more at sentinelone.com.

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