VECTRA SECURITY THAT THINKS® | SentinelOne™

SOLUTION BRIEF

# Vectra + Sentinel One: Detect and mitigate cyberattacks with behavior-based AI

Vectra and Sentinel One enables a complete and authoritative view of a cyberattack by combining the network and the endpoint. Vectra analyzes network and cloud traffic to automatically detect attack behaviors and prioritizes each one based on the risk they pose.

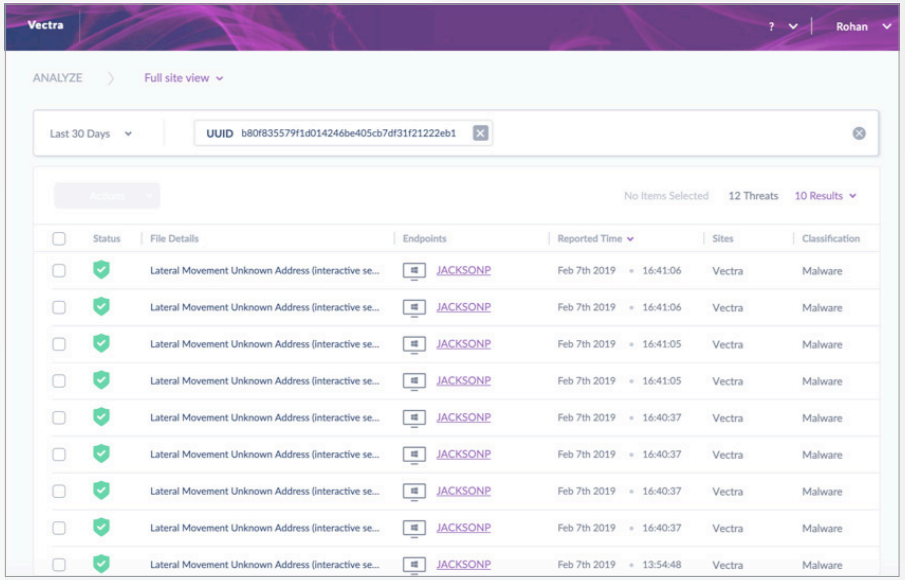
The Sentinel One Endpoint Protection Platform (EPP) provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint with full-context, real-time forensics.

As the scale and sophistication of network threats continues to increase, businesses need greater visibility into threats and the devices and accounts used in attacks against them. A modern security approach also has to be built on automated and actionable intelligence to reduce SOC workload and decrease the time an attacker is allowed to be active in your network.

Security teams that deploy NDR and EDR are empowered to answer a broader range of questions when responding to an incident or hunting for threats.

## KEY BENEFITS

- Autonomous multi-layered detection and response that covers all attack vectors, from the endpoint through the network to the cloud, even when offline.
- Enrich detections with endpoint context, and take immediate action to stop an attack.
- Reduce alert fatigue with machine learning technology that does not rely on signatures and does not require daily/weekly updates.
- Trigger different actions based on type of threat, risk and certainty.



Security teams that deploy NDR and EDR are empowered to answer a broader range of questions when responding to an incident or hunting for threats. For example, they can answer:

- Did another asset begin to behave strangely after communicating with the potentially compromised asset?
- What service and protocol were used?
- What other assets or accounts may be implicated?
- Has any other asset contacted the same external command-and-control IP address?
- Has the user account been used in unexpected ways on other devices?

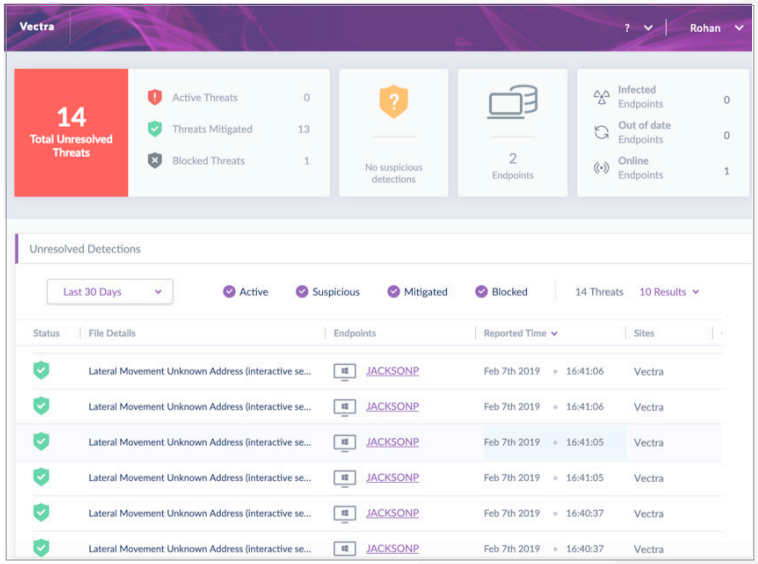
Together, they lead to fast and well-coordinated responses across all resources, enhance the efficiency of security operations and reduce the dwell times that ultimately drive risk for the business.

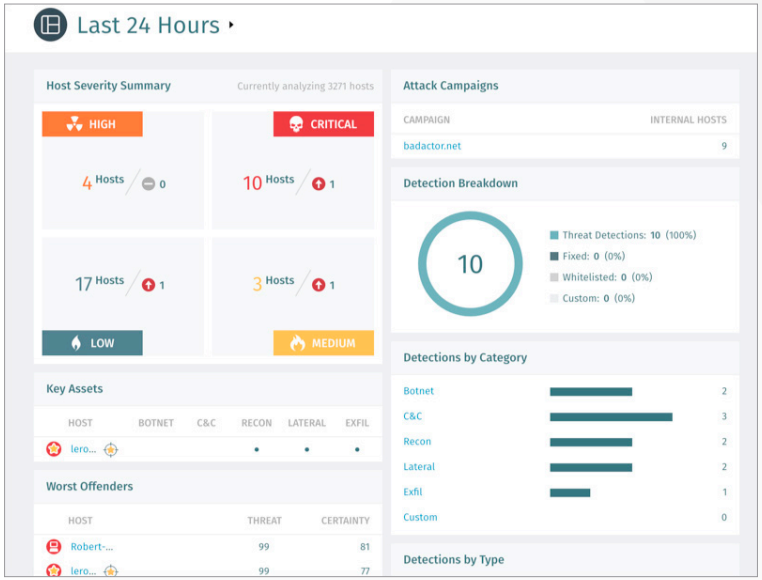
## Sentinel One technology and product

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. The Sentinel One 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.

## Easily integrate network and endpoint context

When a threat is detected, Vectra and Sentinel One provide security teams with instant access to additional information for verification and investigation. Host identifiers and other host data from Sentinel One are shown automatically in the Vectra Cognito UI to enrich Vectra's detection information from the network and cloud perspective, and allows analysts to stop the attack, right from the Vectra Cognito UI.



Sentinel One ingests detections and risk scoring from Vectra and can combine the data with internal behavioral detections to reveal traits and behaviors of a threat that are only visible inside the host, to leverage automated, policy-driven response capabilities to rapidly eliminate the threats.

With this joint solution, Vectra and Sentinel One have created a new class of defense. By combining data science and machine learning, Vectra provides inside-the-network threat detection as a next layer of defense in today's security infrastructure. And with sophisticated behavioral AI, automation with response on the endpoint, Sentinel One enables instant automated response to limit an infected device to stop communication with a C&C server, providing a foundation that secures against the broadest spectrum of threats.

When a threat is detected, Vectra and Sentinel One provide security teams with instant access to additional information for verification and investigation.

## About Vectra

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

## 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 a service representative at info@vectra.ai.**

Email info@vectra.ai vectra.ai