SentinelOne

SOLUTION BRIEF

Detect and Mitigate Threats with Behavioral AI

SentinelOne & Vectra Joint Solution Brief

VECTRA

Market Challenges

As the scale and sophistication of network threats continue 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 a tightly integrated EDR and NDR solution are empowered to respond to, and answer a broader range of questions when investigating an incident or hunting for threats.

Joint Solution

With this joint solution, Vectra and SentinelOne have created a new class of defense. By combining data science and machine learning, Vectra provides inside-the-network threat detection as the next layer of defense in today's security infrastructure. And with sophisticated behavioral AI detection on the endpoint, SentinelOne enables automated response that provides a foundation that secures against the broadest spectrum of threats.

How It Works

When a threat is detected, SentinelOne and Vectra provide security teams with instant access to additional information for verification and investigation. Endpoint identifiers and telemetry from SentinelOne are shown automatically in the Vectra Cognito UI to enrich Vectra's network detection.

SentinelOne 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. Leveraging the SentinelOne API, policy-driven response capabilities are automated to eliminate the threats rapidly.

Use Cases

Security teams that deploy SentinelOne and Vectra NDR 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?

JOINT SOLUTION HIGHLIGHTS

+ Autonomous multi-layered prevention covers all attack vectors, even when offline.
+ Complete visibility from endpoint to the network, both in the enterprise andt cloud.
+ Reduce alert fatigue and false positives with signature-less machine learning
+ Trigger different automated response actions based on threat type, risk, and certainty.

INTEGRATION BENEFITS

- **Reduce Risk**
- **Increase SOC Efficiency**
- **Rapidly Respond**

- 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 rapid and well-coordinated automated responses across all resources, enhance the efficiency of security operations and reduce the dwell times that ultimately drive risk for the business.

Conclusion/Summary

By combining data science and machine learning, Vectra provides cloud and network threat detection as the next layer of defense in today's security infrastructure. With sophisticated behavioral AI, 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. Together, our platforms combine network and endpoint intelligence to provide early automated threat detection and response.

JOINT SOLUTION BENEFITS

Reduce Risk

of breach using AI to detect attacks that have bypassed preventative security controls

Increase SOC Efficiency

with prioritized high fidelity detections with endpoint and network context for rapid and conclusive investigations

Rapidly Respond

with automation and integrated workflows

READY FOR A DEMO?

Visit the SentinelOne website for more details.

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice™

97% Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97% Customer Satisfaction (CSAT)

FedRAMP · ISO 27001 CERTIFIED by schellman · EU GDPR COMPLIANT · TEVORA PCI DSS Attestation HIPAA Attestation · Gartner peerinsights 4.9

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

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 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.

sentinelone.com
sales@sentinelone.com
+ 1 855 868 3733