VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

Reduce your SIEM cost and stop attacks faster

With the increasing number of cyber threats your SOC team faces, ask yourself one question: can we keep pace by relying exclusively on our SIEM to detect and respond to attacks?

There's no doubt your security information and event monitoring (SIEM) solution must do more to aggregate, index, enrich, and analyze volumes of data from a growing number of data sources in order to effectively and efficiently detect and stop attacks faster.

All too often, security operations teams experience incomplete, marginal, SIEM implementations that fail to deliver on a variety of promises, including visibility into cyber threats, speed prioritization, simplifying investigations, and response to attacks at speed and scale.

Advanced, modern SIEM technology that delivers behavior profiling, ML, analytics, and automation require significant manual resources to process data, maintain detection use cases, and triage and investigate alerts—giving time and advantage to attackers.

How Vectra adds value to your SIEM deployment

The Vectra Threat Detection and Response Platform integrates with SIEM tools to help increase SOC efficiency with powerful security-led AI models and rich analytics that correlate data and prioritize detections across multiple domains. Vectra provides the automation, clarity, context, and controls for efficient investigation and response. Whether you currently use a SIEM solution, are defining SIEM use cases, are in the process of a SIEM rollout, or looking to replace your SIEM, Vectra can help you streamline your security operations and effectively meet SLAs.

BOOST SECURITY OPERATION

- Easily correlate data across multiple domains, including AWS, AZURE, and M365
- Improve alert accuracy, reduce false positives, and ensure rapid response
- Streamline MTTD with analytics-lead investigations and predictive analysis
- Automate efforts to connect, score, and prioritize events, and map detections to MITRE ATT&CK tactics

- **Simplify SIEM implementations across use cases** to reduce deployment costs and management overhead. With AI-driven threat detection and response in the Vectra Platform, 97% of malicious tactics and techniques in the MITRE ATT&CK enterprise frameworks are surfaced immediately without tuning or custom unique configurations, allowing you to focus on refining a smaller set of SIEM-based use cases that support the business.
- **Gain rapid, focused highly actionable insights** into attacker behavior faster using AI and machine learning in the cloud and through the network with the precision that reduces noise and mountains of false positives that often plague SIEM users and require timely analysis.
- **Reduce mean time to detection** by accelerating the time it typically takes a SIEM to collect and aggregate data against SIEM policy rules, index findings, while translating results against known factors so you can respond to events faster.
- **Maximize your budget by sending enriched data to your SIEM**. Vectra extracts more value from log data without paying a premium to store it in the SIEM. This approach follows Gartner's guidance of adopting an "output-driven SIEM model where nothing enters the SIEM tool unless there is clear knowledge of how it would be used." It also can lower annual maintenance and log-retention costs by up to 50 percent.
- **Accelerate time to value** while integrating SIEM uses cases at your own pace. As a detection and response platform, Vectra provides immediate value and helps you to refine SIEM/SOAR/EDR operational flows using prebuilt integration modules that speed deployment and activation.

SIEM savings experienced with Vectra

	Before Vectra	After Vectra
SIEM use case development costs	• Splunk $6,000/use case • QRadar $12,500/use case	• 50-68% of SIEM use cases covered by Vectra • Reduction of use case development cost
Yearly use case maintenance cost	• $2,500/use case/year	• Reduced costs with fewer use cases
Log volume		• Up to 50% log volume reduction in SIEM • 37.5% on average
SIEM use case reduction		• 50-63% reduction of # of use cases in SIEM
SOC Level-1 work		• 34x workload reduction in SOC Level-1
IDPS consolidation		• Reduced need of classic IDPS • Includes cloud apps & environments
IR response time		• Accelerated IR response • Increased investigation confidence

Vectra expands SIEM capabilities and attack surface coverage

The complexity and cost of buying and managing SIEM solutions, and the emergence of other security analytics technologies, have fueled interest in alternative approaches to collecting and analyzing event data to identify and respond to attacks. Organizations looking to maintain a steadfast, cost-effective security practice with SIEM are encouraged by experts to seek solutions with increased capabilities that include support for AI-driven behavior analysis that fill critical gaps in detections. With the increasing adoption of hybrid and multi-cloud services, solutions must also facilitate monitoring across IaaS environments and workloads and SaaS applications whether natively or through integrations with third-party technologies.

OPTIMIZE YOUR SIEM STRATEGY WITH VECTRA.

- Increase efficacy using analytics-led detection vs. analysis led SIEM approach
- Pinpoint affected assets correlating telemetry from the cloud, threat intelligence, and other sources combined with the high-fidelity metadata collected from the network.
- Extract more value from log data without shifting work to the humans and paying premium to store it in the SIEM

*CWPP has wide coverage, but only where agents can be deployed, which is lacking in cloud

The Vectra Platform increases coverage, prioritizes threats and provides focused investigation using AI-driven behavioral models and machine learning that expands detection coverage. Vectra combines log telemetry from the cloud, threat intelligence, and other sources with high-fidelity metadata available from collected packets to pinpoint affected assets. Unlike SIEM-based solutions, it moves across environments with the attack, feeding analysts actionable security intelligence based on real-time cloud and network behaviors. These capabilities make Vectra perfectly suited to achieve many of the same use cases (plus a significant number of new ones) previously envisioned for the SIEM, with greater efficacy, and at lower costs.

With the Security AI-driven Vectra Platform and the Sidekick managed detection and response services, SOC teams can effectively mitigate zero-day exploits at the first encounter. The Vectra Platform and MDR services identify tactics and techniques other solutions cannot without manual rule maintenance and tuning. Vectra ensures SOC efficiency and effectiveness without adding complexity for security architects, analysts, and incident response teams.

Deploy Vectra Platform Today

The Vectra Platform can be up and running in days. It's agentless, device agnostic and doesn't require in-line deployment. Vectra also delivers rapid ROI self-funded through lower SIEM costs, tool consolidation and greater SOC efficiency. We help SOC teams see and stop attacks with less work, less tools and in less time.

Accelerate your SOC transformation

SOC 1.0	SOC 2.0
Data source = Logs Coverage depends on log coverage	Data source = Logs + endpoints + network Cover all attack surfaces (on-prem, cloud & SaaS
Detect the "known bad" (threat intel)	Detect unknown & lateral movement attacks
Detection based on rules and thresholds	ML automates attacker behavior detection
Centered on the smart SOC analysts	AI automates Tier-1 analyst workflow
Slow to deploy – custom use cases, log ingestion, alert fatigue, false positives	Works out-of-the box, self-learning
SLA focused on processing events	SLA focused on stopping breaches

Learn more

- Click here to read more about the Vectra Platform and see it in action.
- Download the Case Study
- Contact your service representative for a demo.

Email info@vectra.ai vectra.ai