VECTRA
SECURITY THAT THINKS.®

PLATFORM OVERVIEW

Vectra Threat Detection and Response Platform:
See and Stop cyber-attacks before they become breaches

> “The organization’s rapid adoption of cloud is bypassing our defenses and burning out our team. In the end, we don’t know where we are exposed nor what has been compromised”

Vectra research found that 83% of security professionals say traditional approaches don’t work for modern threats. It’s time to move security forward with AI-driven threat detection and response designed for the hybrid and multi-cloud enterprise.

Harnessing the power of security-led AI, allow security analysts to think like an attacker, knowing what threats are critical while building upon their human intelligence when it comes to cyber attacker tools, techniques, and practices.

With the Vectra AI-driven Threat Detection and Response Platform:

- **You are covered**. Get threat coverage across 4 of your 5 attack surfaces—network, SaaS, cloud and identity
- **You are certain.** Map to 97% of ATT&CK techniques with patented MITRE D3FEND countermeasures
- **You are in control.** Integrate with your unique security stack for context, workflow, and response

As the leader in AI-driven threat detection and response for hybrid, multi-cloud environments, the Vectra platform arms security analysts and admins with visibility into malicious attacks in motion. With visibility and context, security teams are equipped to prevent attacks like ransomware from taking hold of the environment. Vectra’s Behavioral Security AI efficiently pinpoints attacker methods early so security analysts can easily prioritize and drive the right level of response immediately. Unlike traditional approaches rooted in IDPS and SIEM, with Vectra, your SOC is more efficient and effective, and your organization is more resilient.

83%

83% of security professionals say traditional approaches don’t work for modern threats.

Vectra transforms the SOC

- Native coverage for 4 of 5 attack surfaces – Datacenter, cloud, SaaS & identity
- Integrates with EDR tools for context, workflow and response
- Only alerts on real events and attacks not anomalies
- Connects the dots between threats across all environments
- Triages and prioritizes threats and attacks automatically
- Eliminates tuning to reduce mountains of false positives

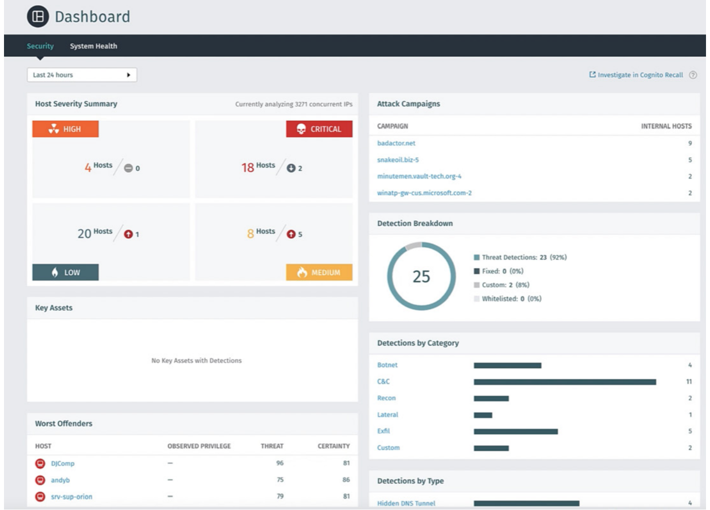
Transforming The SOC With Security AI

Recent Vectra data cites that 79% of security decision makers have bought tools that failed to live up to their promise. However, SOC modernization is a reality when using artificial intelligence and machine learning through a security-led approach.

- **The AI-driven SOC covers critical attack surfaces: network, SaaS, cloud, and identity**
- **The AI-driven SOC pinpoints attacker methods to prioritize attacks by severity**
- **The AI-driven SOC unifies disparate tools and processes to minimize analyst burnout**

Vectra helps security teams analyze massive amounts of data and telemetry against the MITRE D3FEND framework, so analysts know exactly what’s happening across all attack surfaces and can easily prioritize threats.

- **Upskill SOC & heighten knowledge to “understand” cybersecurity threats and risk**
- **Automate efforts to identify, validate, prioritize & triage incidents & discern attribution**
- **Expose relationships between events and surface attacks fast**
- **Identify relevant events & attacks without noise so detections can be consumed efficiently**



Host Severity Summary

Currently analyzing 3271 concurrent IPs

HIGH 4 Hosts / 0

CRITICAL 18 Hosts / 2

LOW 20 Hosts / 1

MEDIUM 8 Hosts / 5

Key Assets

No Key Assets with Detections

Worst Offenders

HOST	OBSERVED PRIVILEGE	THREAT	CERTAINTY
DJComp	–	96	81
andyb	–	75	86
srv-sup-orion	–	79	81

Attack Campaigns

CAMPAIGN	INTERNAL HOSTS
badactor.net	9
snakeoil.biz-5	5
minutemen.vault-tech.org-4	2
winatp-gw-cus.microsoft.com-2	2

Detection Breakdown

25

- Threat Detections: 23 (92%)
- Fixed: 0 (0%)
- Custom: 2 (8%)
- Whitelisted: 0 (0%)

Detections by Category

Botnet	4
C&C	11
Recon	2
Lateral	1
Exfil	5
Custom	2

Detections by Type

Hidden DNS Tunnel	4

Vectra uses machine learning models rooted in deep science along with algorithms that think just like an attacker. By doing so, evolving attacks and threats are accurately detected and prioritized for security teams. This patented approach yields rich metadata and context containing actionable insights that enhance dashboard reporting and alerts, to inform and educate SOC analysts and increase automation.

Whether under-resourced or fully staffed—security teams gain the level of resiliency necessary when operating across today’s threat landscape. This includes everyday tasks around forensic investigations and threat hunting to detecting dynamic attack tactics that can lead to supply-chain attacks, lateral movement, C2 establishment, malicious hacks, or identity takeovers. Together with Vectra, organizations can truly optimize operations, providing fast, high-quality attack insight with understanding, increasing automation that augments limited security functions, and reduces human oversight and opportunities for error where it matters most.

Increase security efficacy of existing toolsets

splunk>

bring real-time, correlated attack detections to the operational intelligence of the Splunk platform

CROWDSTRIKE

Expanding visibility into attacker methods to drive complete protection

vmware Carbon Black

Automate detection of hidden cyberattacks and unify network & endpoint threat context

paloalto NETWORKS
SentinelOne

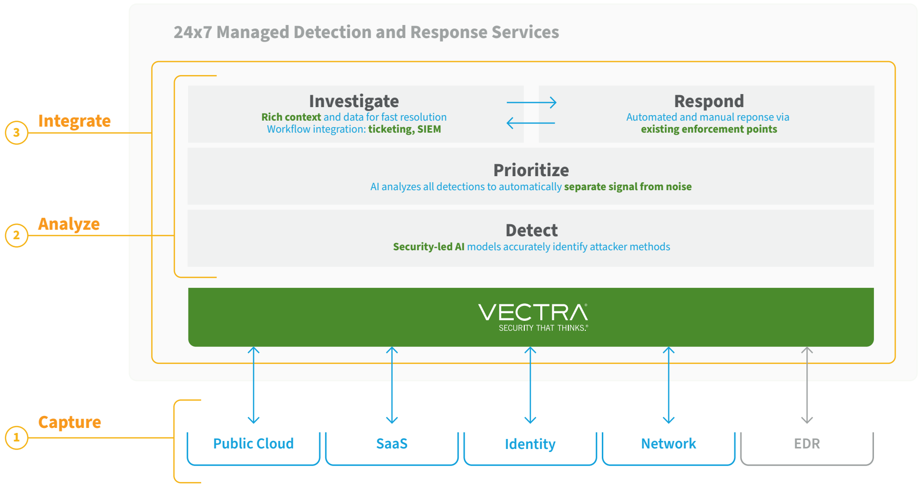
Boost detections with network-based behavioral analytics to ensure no data is lost

Click here to see the complete list of Vectra technology partners and gain insight into the value of integrating security-led AI with your existing security toolset.

Pinpoint Attacker Methods Across An Entire Enterprise

Enterprise Datacenter	Cloud Environments	SaaS Services
Counter attacks hijacking the network and services to move laterally across the data center—without decrypting traffic.	Stop threat actors targeting IaaS infrastructure, workloads, cloud-native services, APIs, networks, and those misusing Azure AD to impact federated services	Identify risk and prevent abuse of native M365 applications and capabilities like Microsoft Teams, SharePoint and Power Automate

How the Vectra platform works


24x7 Managed Detection and Response Services
3 Integrate
2 Analyze
1 Capture
Investigate
Rich context and data for fast resolution
Workflow integration: ticketing, SIEM
Respond
Automated and manual reponse via existing enforcement points
Prioritize
AI analyzes all detections to automatically separate signal from noise
Detect
Security-led AI models accurately identify attacker methods
VECTRA SECURITY THAT THINKS.
Public Cloud
SaaS
Identity
Network
EDR

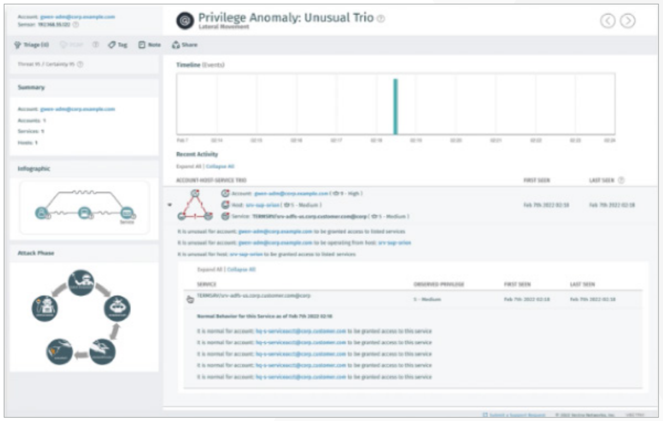
1) Extracts telemetry and data from logs, traffic sensors, and API calls
2) Captures are analyzed using applied security-led AI, advanced ML algorithms and deep learning with neural networks to hierarchical clustering.
3) Attacks detected are attributed to relevant accounts or hosts to prioritize the entities
4) Dashboard is updated to provide a unified view of attacks across hybrid and multi-cloud environments.

Dashboard Visibility and Threat Knowledge

Vectra ensures visibility across all attack surfaces—data center, cloud, identity or SaaS environments like M365—unifying detection of attempts on data and overcoming blind spots present in other solutions. Upon activation, organizations can confidently observe the full set of actions performed by threat actors in real-time with rich meaningful details indicating the nature of the attack, including attribution and priority levels.

Visibility that Simplifies Analyst Effort

- See correlated threat behaviors on a host or account prioritized by severity with a threat-certainty score.
- Prioritize threats and active attacks across hybrid and multi-cloud network accounts, host machines, and IAM users.
- Gather key information to understand root cause, triggers, and business impact in one click without writing queries or jumping to another tool.
- Stop attacks automatically by disabling an offending network host or use integrations with existing security investments.
- Generate reports on specific attacks that highlight attack trends and summarize security posture and compliance.



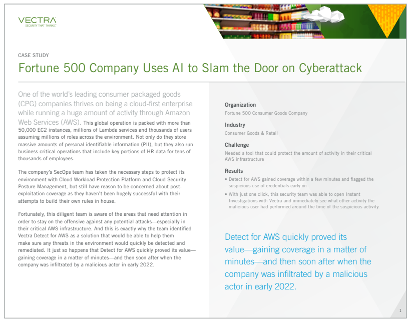
Stop 90% of Mitre ATT&CK methods targeting business-critical services

Network	AWS, Azure, GCP	M365 & Azure AD
• C&C Activity • Malware deposits • Botnet attacks • Recon scanning & sweeping • Lateral Movement • Web injection attacks	• Root and Tor activity • EC2 & S3 Enumeration • Credential access & escalation • Reconnaissance • Lateral movement setup/activity • User, ECR & Lambda hijacking	• Suspicious Access • Sus. Mail, SharePoint, Teams activity • O365 Misuse, exploitation & hijacking • Unusual Azure AD activity & script use • Exfiltration with Power Automate, eDiscovery

[Click to learn more about MITRE coverage]

Solving Real-World Problems

Leading consumer packaged goods company set out to strengthen existing CWPP and CSPM capabilities to address a high level of activity within their critical AWS infrastructure. 50,000 EC2 instances, millions of Lambda services and tens of thousands of users assuming millions of roles across the environment. **Immediately upon activation, they observed suspicious use of credentials and 'Secrets' interactions on S3 storage coming from a novel IP space. Existing tools had yet to detect these events.** Other activity performed around the time of the suspicious event were also visible in the Vectra dashboard.



VECTRA
SECURITY THAT THINKS.

CASE STUDY

Fortune 500 Company Uses AI to Slam the Door on Cyberattack

One of the world's leading consumer packaged goods (CPG) companies thrives on being a cloud-first enterprise while running a huge amount of activity through Amazon Web Services (AWS). This global operation is packed with more than 50,000 EC2 instances, millions of Lambda services and thousands of users assuming millions of roles across the environment. Not only do they store massive amounts of personal identifiable information (PII), but they also run business-critical operations that include key portions of HR data for tens of thousands of employees.

The company's SecOps team has taken the necessary steps to protect its environment with Cloud Workload Protection Platform and Cloud Security Posture Management, but still have reason to be concerned about post-exploitation coverage as they haven't been hugely successful with their attempts to build their own rules in house.

Fortunately, this diligent team is aware of the areas that need attention in order to stay on the offensive against any potential attacks—especially in their critical AWS infrastructure. And this is exactly why the team identified Vectra Detect for AWS as a solution that would be able to help them make sure any threats in the environment would quickly be detected and remediated. It just so happens that Detect for AWS quickly proved its value—gaining coverage in a matter of minutes—and then soon after when the company was infiltrated by a malicious actor in early 2022.

Organization
Fortune 500 Consumer Goods Company

Industry
Consumer Goods & Retail

Challenge
Needed a tool that could protect the amount of activity in their critical AWS infrastructure

Results

- Detect for AWS gained coverage within a few minutes and flagged the suspicious use of credentials early on
- With just one click, this security team was able to open Instant Investigations with Vectra and immediately see what other activity the malicious user had performed around the time of the suspicious activity.

Detect for AWS quickly proved its value—gaining coverage in a matter of minutes—and then soon after when the company was infiltrated by a malicious actor in early 2022.

1

Click here to read the case study

> "Vectra quickly proved its value—gaining coverage in a matter of minutes— providing security confidence when the company was infiltrated by a malicious actor in early 2022"

Most Common Use cases

- Prioritize and triage threats and incidents
- Streamline efforts to understand relationships between events
- Identify active threats in the network, cloud and M365
- Strengthen Zero-trust practices

For more information please contact us at info@vectra.ai.

Email info@vectra.ai   vectra.ai

Experience the benefit of an AI-driven SOC with Vectra

- Hybrid cloud monitoring from the data center to the cloud
- Detect attacker movement between public and private cloud
- Respond and stop cloud attacks automatically using native integrations with current security stacks
- Disable specific hosts, user accounts and cloud workloads automatically or in a customizable fashion

VECTRA PLATFORM STANDS OUT

Vectra Platform	NDR	EDR/XDR
Security-lead AI that combines security research and AI mapping to MITRE D3FEND to catch attacks based on attack methods used across the enterprise and in the cloud	Identifies everything "different' without context	Most lack sufficient network coverage and use simple anomaly-based detection
Depth in coverage for attacker behavior in SaaS, Identity & cloud	Significant cloud coverage gaps with anomaly detection and lack of understanding of attack vectors in the cloud, for example eDiscovery and Power Automate misuse	No coverage
AI-drive attack prioritization out-of-the-box to surface only relevant threats to security teams	Requires constant manual tuning	Requires constant tuning to increase the efficacy
Provides rich attack narrative and context for security teams to investigate	Lacks attack understanding and insight into what's behind the priority	Context is limited to endpoint; lacks network context
Comprehensive view into the M365 / AzureAD attack surface configuration and compliance reporting (Kevin/Aaron	Lacking any support	Separate integrations
24X7 MDR service to augment security teams	No MDR offering	MDR limited to end point