VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Detect for AWS

The problem

The need for speed and agility in today's always-on, always-connected digital business has led IT teams to transform the traditional on-premises infrastructure to cloud-native architectures, but often at the cost of security.

The rise of DevOps and the use of Platform as a Service (PaaS) & Infrastructure as a Service (IaaS) have been foundational to this change and are now the norm. But where as security traditionally fell on dedicated teams, it now often falls on the developers themselves, and as a result, when speed and agility increase, so does the risk of introducing security issues. Public cloud environments have grown incredibly complex and are in constant change; deploying a cloud application in a secure manner is at this point impossible.

> Through 2025, 99% of cloud security failures will fall on customers.[1]

According to Gartner, 99% of cloud security failures that occur through 2025 will be the customer's own fault. Cloud providers are responsible for the availability and infrastructure, not the user, application, and data security. And even the organizations that have dedicated security teams quickly find that legacy operations and the traditional security practices don't translate well to the public cloud, and the gap is growing as the cloud surface area that needs to be protected and audited is constantly changing.

[1] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

71% aws

71% of AWS customers use four or more AWS Services.

HIGHLIGHTS

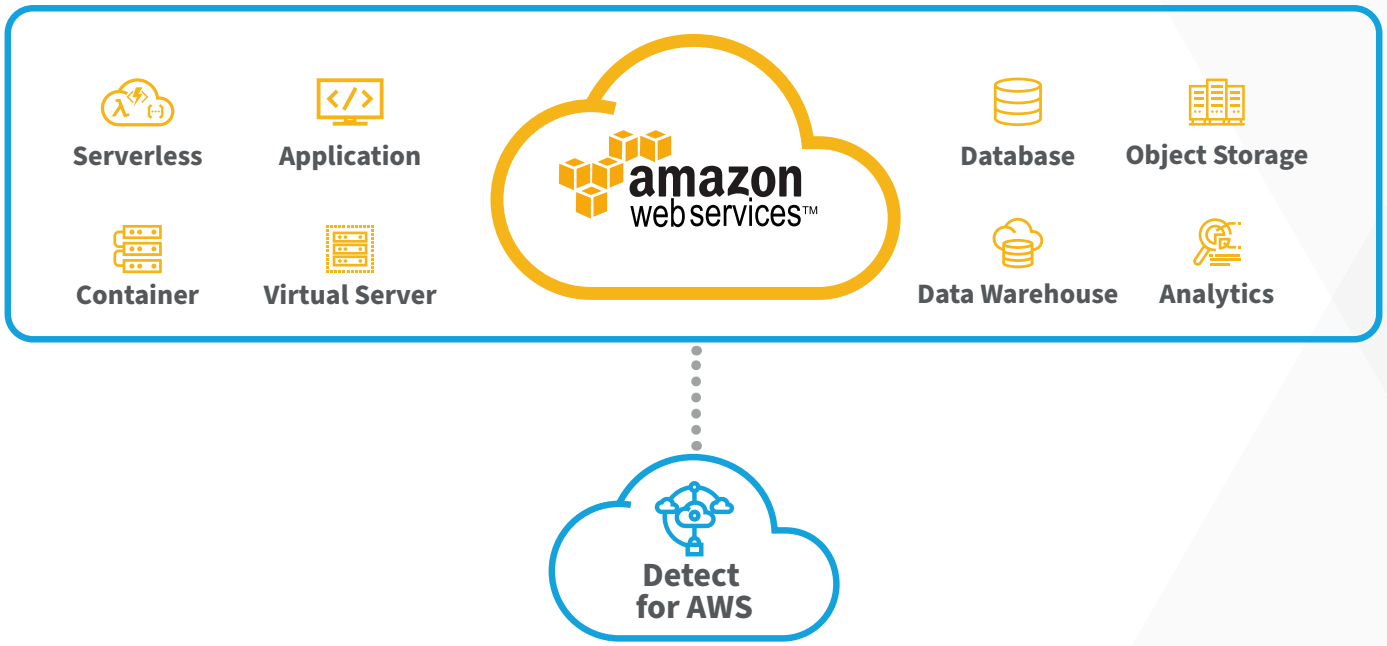
Rapidly detect threats against enterprise applications and data running on AWS IaaS, and PaaS using the first behavioral AI that detects and prioritizes threats.

Deploy in minutes with agentless coverage that does not rely on signatures, virtual taps, or static policy.

Investigate attacks to find the roles and accounts involved with historical security data that allows teams to trace an attack progression through all roles and accounts back to where it started and stop it there, without causing widespread outages.

Automate response to attacks on applications running on AWS using native capabilities in AWS or deep integrations with other security solutions allowing teams to mitigate threats without relying on agents or disruption to operations.

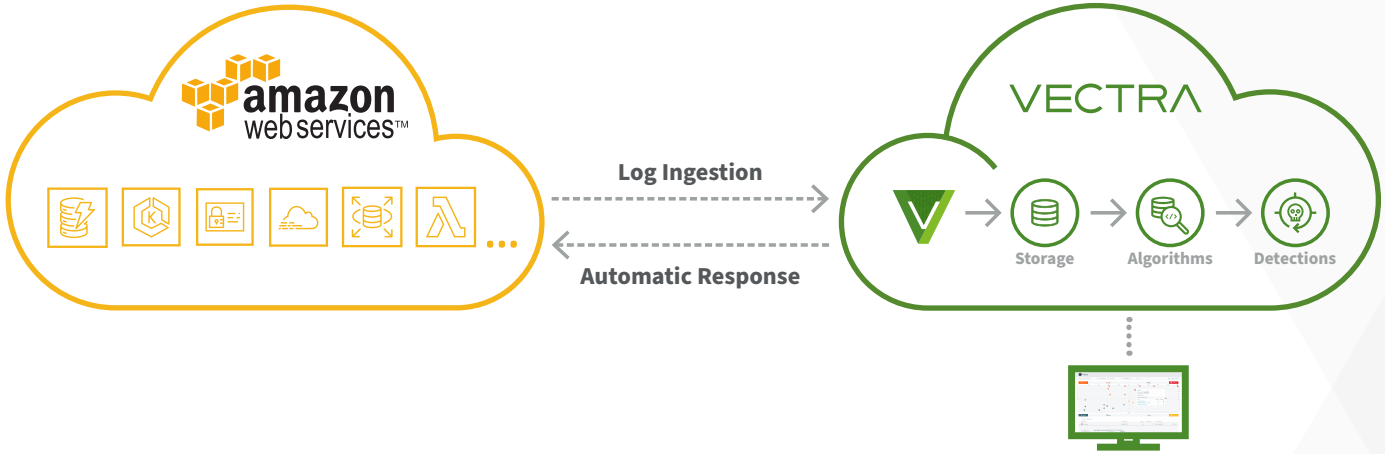
Vectra closes the security gap.



The cloud-native Vectra Detect for AWS SaaS offering bridges this gap. By observing and understanding attacker behavior, cloud identities, roles, access policies, and deployment configurations for workloads including storage, containers, and serverless, Detect for AWS finds and stops attacks without disrupting operations.

As the first threat detection solution that uses behavioral AI without relying on signatures, static policy, or the operational impact of agents, it allows organizations to confidently migrate, develop, and deploy more applications at scale while minimizing the risk of breaches from security issues introduced at deployment.

Detect for AWS is the only AI-driven solution that uses behavioral models to find and stop attacks without disrupting operations.

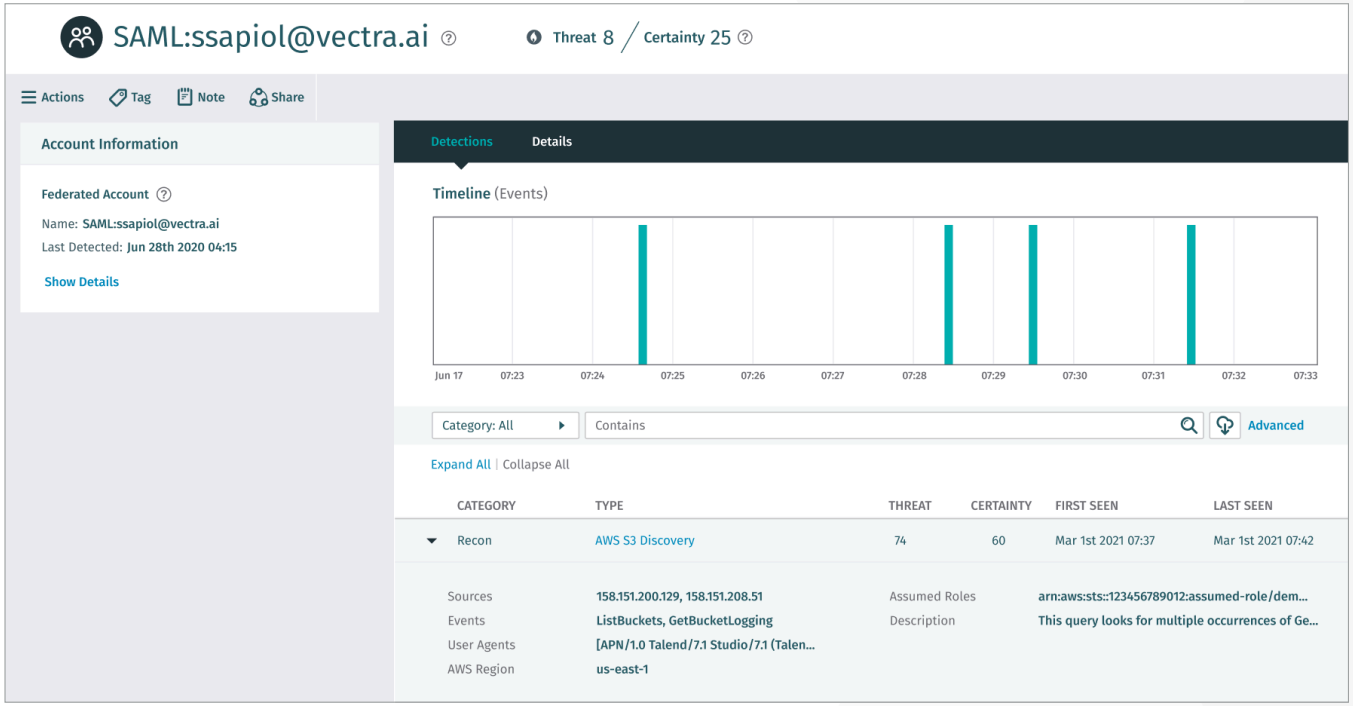


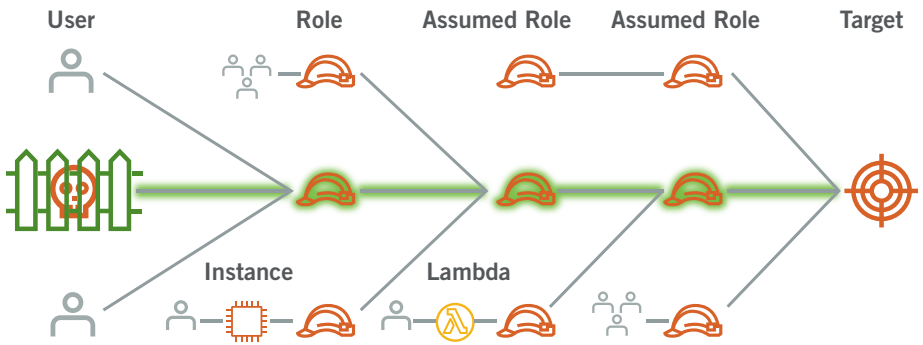
Full coverage across the MITRE ATT&CK framework

MITRE ATT&CK mapping

- Native AWS integration monitors the interaction of users and resources with AWS services, such as creating or deleting EC2 instances or exposing S3 buckets to the public.
- Agentless setup in minutes enables Vectra to analyze activity and start protecting your AWS organization with patented AI-driven attacker behavioral models.
- Converged security view across multiple regions, offering a unified view of your worldwide activity.
- Instant one-click investigations will accelerate investigations by providing intelligent queries and historic logs.
- Usage is licensed per GB of activity logs analyzed.

Vectra uses artificial intelligence to track down malicious actors through chains of assumed roles, whether local or federated, on both the same AWS account or cross-accounts. The industry first KingPin technology will clearly show what principal originated the attack in every alert you receive, giving you clear next steps to investigate and remediate.





Every alert you receive will clearly show what principal originated the attack, and you will have clear next steps to investigate and remediate.

Coverage for AWS Attacks

Tactic	Example attacks
Initial Access	Suspicious Credential Usage, access from TOR, Root activity
Persistence	Hijacking existing users & services, Granting external access
Privilege Escalation	Adding permissions to users, Pivoting to full console control
Evasion	Disabling security tools, Disabling Logging, bypassing security controls
Cred Access	Harvesting credentials from services
Discovery	Discovering User permissions, Organization details and services
Gathering	Search for S3 Buckets and data stores
Impact	Excrypting files for Ransom, Cryptomining
Exfil	Downloading from S3 buckets, Exposing instance data to Public

Example Target Services

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

Email info@vectra.ai vectra.ai

Version: **061021**