VECTRA
SECURITY THAT THINKS.®

COMPLIANCE BRIEF

Vectra Detect for Amazon Web Services

amazon web services™

Vectra Detect for Amazon Web Services (AWS) sees and stops attacks targeting an enterprise's AWS footprint in real-time.

Vectra ingests AWS CloudTrail management & data event logs from the entire AWS footprint into the Vectra secure cloud. It can then run security-led AI detection models on the data and publish threat detections to a Vectra-hosted, per-customer, web portal.

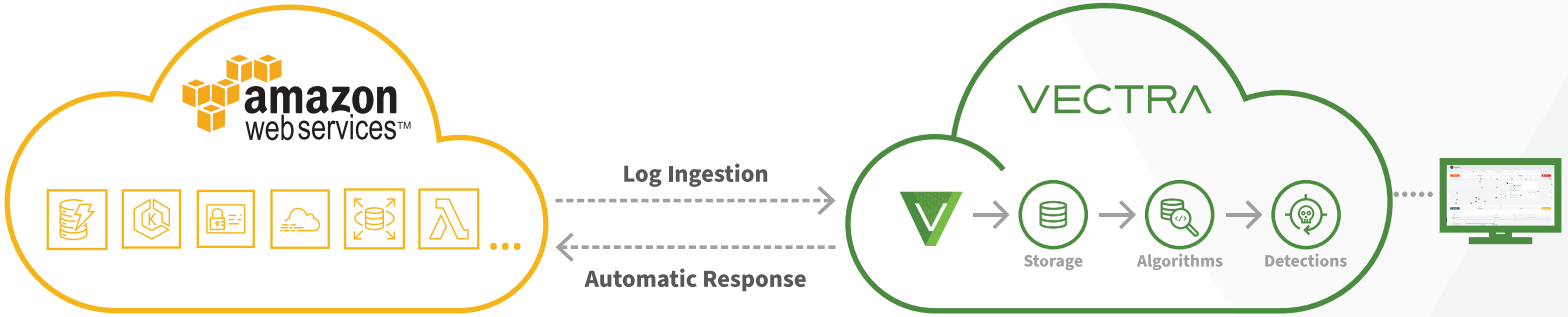
Vectra is a SOC2 Type 2 compliant organization with our Detect for Network product and is currently applying these controls for Detect for AWS.

Collecting only the required data to Secure your AWS Footprint

Vectra will only monitor the CloudTrail Logs, which the customer grants access to. At a minimum, this will include management events logged by CloudTrail, but we recommend including S3 Data events for better coverage. These logs do not contain any Personally Identifiable Information (PII) aside from user email addresses, and you retain complete control over the events sent to Vectra.

You can read about the specific permissions required and why they are required here: https://support.vectra.ai/s/article/KB-VS-1554

Using artificial intelligence, Vectra Detect sees and stops attacks targeting an enterprise's Amazon Web Service footprint in real-time.



Complete Control over Data Transfer

Logs are ingested from your AWS cloud over secure TLSv1.3-encrypted sessions through the AWS Role created for Vectra by your AWS admin. This consent can be revoked at any time by deleting this role or removing the role's permissions to access S3 data. Once authorization is revoked, log collection will stop immediately.

The AWS Role is secured by limiting read-only access from the specified AWS account and using an AWS External ID, which acts as a unique key where external accounts cannot assume the role in the customer environment without producing that External ID.

Vectra Detect for AWS will monitor any AWS CloudTrail logs stored in a specified S3 bucket. The cloud logs consist of Management Events, which represent management activity performed by users and services within your AWS environment, and Data Events, which represent operations performed against specific resources.

- You can read more about management events here: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-events-with-cloudtrail.html#logging-management-events
- You can read more about Data events here: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html#logging-data-events

Data at rest, Encrypted and Segregated

The data ingested by Vectra is received and stored separately per customer. Therefore, there are no direct interfaces to access the data for third parties, and only Vectra Detect applications are authorized to access this data.

As part of the feed, we only retrieve log event objects, as created by AWS CloudTrail and stored in your S3 bucket; we do not ingest company or user data.

Data at rest is encrypted leveraging Cryptographic Service Provider (CSP) techniques.

Information is only retained for up to 90 days.

Trusted Hosting Environment

Vectra cloud services are deployed within Amazon Web Services (AWS), whose facilities and services are certified to the highest standards. You can read more about AWS compliance programs here: https://aws.amazon.com/compliance/programs/

To comply with customers' data sovereignty mandates, Vectra deploys in multiple regions globally. For example, a customer in EMEA may choose to store and analyze data out of Vectra's EU cloud in Dublin only.

Only specific, authorized, Vectra employees have access to the production Vectra cloud for maintenance purposes.

Secure User Access for the Modern day Cloud

End users will only be able to access data through the Vectra cloud. Access is limited to registered users, and Multi-Factor Authentication is strictly enforced.

A secure direct link between the Vectra Web Portal and a customer's Vectra AWS log receivers (sensor) is maintained. This ensures that the Vectra Web Portal can only access detections from logs ingested by its paired sensors. Additionally, Vectra Detect connectivity is secured through TLSv1.3-encrypted sessions.

Authorized access to the Vectra Detect Web Portal is entirely under the customer's control. No user, including Vectra employees, will access the customer web portal or any data within it without explicitly being added as a user to the portal by the customer.

Maintaining Privacy & Protecting PII

Vectra acts as a data processor for PII on behalf of its customer – the data controller.

Vectra:

- Collects only the minimum PII required to discharge its cybersecurity obligations on behalf of the data controller – in this case, the user account name (email ID).
- Do not transfer any PII out of the EU or to any 3rd party organization.
- Retains detections and relevant evidence logs for six months, after which the data is permanently deleted.
- Makes all detections and relevant logs available through the product UI in the Vectra Web Portal.

Versions

v1.0 October 1, 2021

For more information please contact a service representative at privacy@vectra.ai.

Email info@vectra.ai vectra.ai