VECTRA
SECURITY THAT THINKS.®

COMPLIANCE BRIEF

Vectra Detect for Azure AD and M365

Security, Privacy, and Compliance

Overview

Vectra Detect for Azure AD and M365 lets you see and stop threats to your SaaS apps, Azure AD backend, and M365 data. Vectra achieves this by securely collecting Azure AD and M365 logs from the customer's tenant into Vectra's secure cloud, running detection models on those logs in Vectra's cloud, and publishing detections events and context into the customer's Vectra UI located on a customer-managed brain (on-premises or a virtual) or in Vectra's SaaS UI.

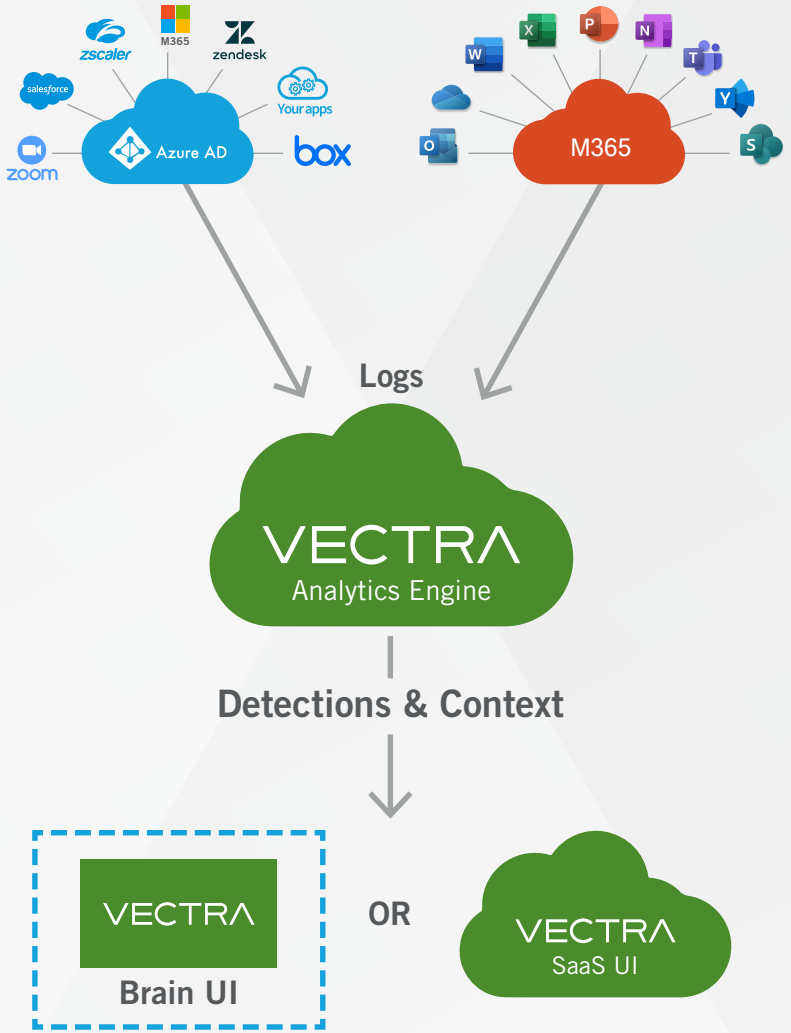
Data Ingested

Recognizing the sensitive nature of Azure AD and M365 usage and the information in the resulting logs, Vectra ingests logs on a strictly need-to-know basis. Only the subset of logs required for the analytics are ingested into the Vectra cloud.

Vectra collects the necessary data using a secure OAuth application that runs in the customer's Azure AD tenant. The application is authorized by the customer's Global Admin and uses the following read-only permissions:

- ActivityFeed.Read (Office Management API)
- ActivityFeed.ReadDLP (Office Management API)
- Directory.Read.ALL (Graph API for Azure AD logs)
- AuditLog.Read.All (Graph API for Azure AD logs)
- User.Read (Added by default by Microsoft – this is not actually requested)

The OAuth application can be removed at any time by the customer. Once removed, log collection will stop immediately.



How is the ingested data secured?

Logs are ingested from the Microsoft cloud over secure TLSv1.3-encrypted sessions pursuant to the authorization of the Vectra app by the customer's Global Admin.

The data ingested from each customer tenant is received and stored separately per customer. There are no direct interfaces to access this data.

- Only Vectra applications are authorized to access this data.
- Only log event objects created by Azure AD and M365 are retrieved.
- Data at rest is encrypted leveraging Cryptographic Service Provider (CSP) techniques.
- Information is only retained for up to 90 days.

Logs collected

Log events related to Azure AD access and setting changes and M365 activities in applications like Exchange, SharePoint, OneDrive, eDiscovery, Power Automate, and Teams are collected.

- Two specific APIs are used:
  The Management API is used to collect 'Audit.AzureActiveDirectory', 'Audit.Exchange', 'Audit.SharePoint', 'Audit.General', and 'DLP.All' logs.
  > Additional details about the data collected can be found here:

    https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema

- The Microsoft Graph API is used to collect 'directoryAudits' and 'signIns' logs.
  > Additional details about the data collected can be found here:

    https://docs.microsoft.com/en-us/graph/api/signin-list?view=graph-rest-1.0&tabs=http

    https://docs.microsoft.com/en-us/graph/api/directoryaudit-list?view=graph-rest-1.0&tabs=http

Select sensitive data fields, like file names and email or calendar subjects, can be anonymized such that values are not persisted in Vectra's cloud infrastructure. The customer may choose not to use anonymization while still assuring that the data is only available to select analysts who are granted access to the Vectra UI.

How is user access secured?

There is a 1:1 mapping between a customer's Azure AD and M365 tenant, their Vectra data collector, and their associated Vectra User Interface (UI). This ensures a customer's Vectra UI can only access detections from logs ingested by its paired connector.

Authorized access to the Vectra Brain UI (on-premises or virtual) is entirely under the customer's control. Vectra enables secure authentication using standard enterprise methods like RADIUS, TACACS+, and LDAP, together with granular role-based access control. SAML 2.0-based SSO to Vectra's Detect UI is available as a secure authentication standard.

Authorized access to the Vectra SaaS UI 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 SaaS UI by the customer. Access is limited to registered users, and Multi-Factor Authentication is strictly enforced.

Compliance

Vectra cloud services are deployed in the most widely used public cloud providers – namely Microsoft Azure and Amazon Web Services (AWS), whose facilities and services are certified to the high standards documented below:

- AWS
- Azure

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

Only specific, authorized Vectra personnel have access to the production Vectra cloud for management purposes.

Vectra is a SOC2 Type 2 compliant organization with our Detect for Network product and is currently applying these controls to Detect for Azure AD and M365.

Privacy

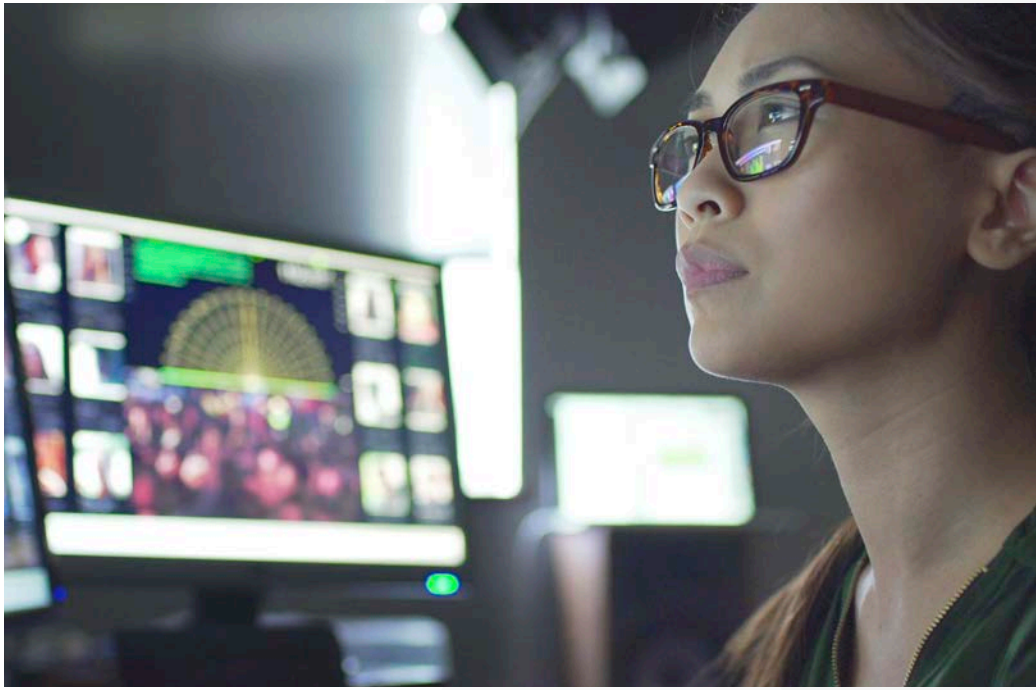
Vectra acts as a data processor for PII on behalf of its customer – the data controller.

Vectra:

- Collects only the minimum PII required to discharge its cyber-security obligations on behalf of the data controller – in this case, the user account name (email ID).
- Does 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 Vectra UI

Versions

v1.1



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

Email info@vectra.ai vectra.ai

Version: **041822**