Upgrading to the Vectra AI Platform with Respond UX

The Vectra AI platform is our latest and best experience for consuming Vectra AI's Attack Signal Intelligence using a unified set of interfaces and tooling to deliver:

- Best-in-class signal clarity
- Expedited access to relevant information
- Faster investigation workflow

The Vectra AI Platform is cloud-delivered, enabling:

- Best-in-class experiences and protection
- Cloud performance and scale
- Native support for remote and hybrid SOC teams

Customers not yet using the new Vectra AI Platform UX are consuming Vectra through the Appliance Platform where the UI is hosted on their Vectra Brain. This document outlines the process by which your data and configuration is migrated to the Vectra AI Platform. The migration process involves uploading a copy of the configuration, detections, hosts, detection state to the cloud and keeping that in-sync going forward (Please note that any Recall metadata is NOT migrated). Post-migration, customers…

- Continue to leverage their existing fleet of sensors and brains for the collection and analysis of network traffic.
- Fulfill all workflows (UI, API, etc) through cloud endpoints as opposed to endpoints hosted on the Vectra Appliance platform.
- Benefit from cloud-powered AI-driven prioritization, and cloud-powered AI-triage to help you focus on the things that really matter within your environment.

Customers not yet using the new Vectra AI Platform with Respond UX are consuming Vectra through the Vectra Appliance platform where the UI (Quadrant UX) is hosted on your Vectra Brain. This document outlines the process by which your data and configuration is migrated to the Vectra AI Platform.

Key Information

	From: Vectra Appliance platform	To: Vectra AI Platform
UI	Served from Vectra Brain	Served from Vectra Cloud
Signal	Partitioned experience, with quadrants, Threat and Certainty	Unified experience with single Urgency Score
Investigation	Using Recall or Stream for network only.	Using integrated Instant and Advanced Investigation for all attack surfaces
Network coverage	Using existing Brain and sensor deployment	Using existing Brain and sensor deployment

Frequently Asked Questions

Question	Answer
Will I lose active detections and history?	No, all detections and history are preserved (Recall Metadata is not migrated)
Do I have to do anything?	Yes, but not much! See "Preparing for the migration section" below
How long will it take?	Typical customers will take between 30 and 60 minutes to migrate
Is there any cost to migrate?	Depends on your deployment. Please talk to your Vectra account team to understand

Process for migrating to the Vectra AI Platform with Respond UX

1. Preparing for the migration

a. A planning meeting where your Vectra account team will discuss with you to understand exactly what will happen and when.

b. Adjust your firewall rules (if necessary) to enable access from the Vectra brain to the Vectra Cloud. Please see Respond UX deployment guide (here) or the firewall rules KB for the list of firewall rules required.

   i. In addition, during the migration only, Vectra will need connectivity from the existing brain to a specific AWS S3 bucket. This is required to enable the upload of the brain's backup to Vectra Cloud. The AWS S3 bucket names are below:

AWS Region	Connectivity required to this AWS S3 bucket
us-west-2 (US)	prd-vuibackup-artifacts-580786928539-uswt2.s3.us-west-2.amazonaws.com
eu-west-1 (Ireland)	prd-vuibackup-artifacts-580786928539-euwt1.s3.eu-west-1.amazonaws.com
eu-central-2 (Switzerland)	prd-vuibackup-artifacts-580786928539-eucl2.s3.eu-central-2.amazonaws.com
ca-central-1 (Canada)	prd-vuibackup-artifacts-580786928539-cacl1.s3.ca-central-1.amazonaws.com
ap-southeast-2 (Australia)	prd-vuibackup-artifacts-580786928539-apse2.s3.ap-southeast-2.amazonaws.com

   ii. These need to be opened for HTTPS use over TCP/443.

   iii. Access is only required to the one region where your Vecrta AI Platform tenant will be deployed, and it is only required during the migration.

c. Validate that you have adequate egress bandwidth to accommodate the transfer of network metadata to the new Instant and Advanced Investigation experiences. This is estimated to be between 0.5% and deployed of the traffic observed from the brain. If you have Recall, this is instead of Recall, not in addition to Recall. Please see 2. Migration g iii below for more details.

d. Align with your Vectra account team on the date and time for the migration.

e. List out any custom API based integration you may have built.

f. Please see topic 3.c in the Post-Migration below for details on authentication changes for RUX deployments.

2. Migration

a. On the day before the migration, Vectra will request authorization to proceed with the migration. If authorization is not received, the migration will be postponed. This is to ensure that we don't migrate when key people are out of office, or when there's an active and ongoing incident.

b. [Optional] Should you desire an active call bridge during the migration, this will be provided. Vectra will create this bridge 15 minutes before the migration is due to start and will ensure you are present before the migration starts. The Vectra account team will be able to provide updates on progress during the migration.

c. On the day of the migration, the CSM/SE will send you an email confirming that the migration will start at the designated date and time.

d. During the migration, you will not have any access to the Brain UI. The Vectra services running on the Vectra Brain will be suspended for the duration of the migration.

e. Migrations that take longer than 40 minutes to complete will result in a detection coverage gap from the start of the migration window to the start of the "last 40 minute" window. I.e. if the migration takes 60 minutes, there will be a detection coverage gap from the start of the migration window to 20 minutes into the migration window.

f. During the migration, data flowing to Recall and Stream will be stopped. The data flow to Stream will resume automatically when the migration completes successfully and attempt to catch up on any queued data. A gap in data in Stream may exist from the migration window.

2. Migration continued

g. Once the migration is completed:

i. All data and configuration from the Brain has been sent to the Vectra AI platform in the cloud.

ii. All new configuration, metadata, hosts, accounts, detections will start flowing into the Vectra AI platform and visible in the new UI.

iii. If you are a Recall customer, forwarding to Recall will stop since metadata is integrated into the Vectra AI platform and accessible directly from the UI. Your Recall instance will be deprovisioned once the metadata retention period you previously had with Recall has elapsed. Please note that Recall metadata is NOT migrated to your new RUX deployment. If you wish to retain access to Recall before your existing Recall metadata has aged out, please let your migration team know and credentials to directly access your Recall Kibana URL can be provided.

iv. You will receive an email from Vectra with details on how to log into the new Vectra AI platform. This initial login to the UI will require the setup of MFA (Multi-Factor Authentication) once authenticated.

v. The CSM/Support contact will send you an email to confirm that the migration has been completed, and to ensure that you are able to access the UI.

vi. The UI on the Brain will no longer be accessible. All access must be through the new UI.

Please note once the migration is complete, you cannot revert back to the appliance platform UI for that deployment. ’

3. Post-migration

a. Login to the Vectra AI platform UI using the link and credentials provided in the email.

b. You will need to re-create any standalone users to enable access to the Respond UX for your team.

c. If you use SAML, you will need to register a new SAML profile to enable Single-Sign On (SSO) access to the Respond UX. The setup for SAML requires claims in a different format for a RUX deployment vs any existing QUX SAML deployment. Please see Setup SAML SSO with any IdP (Respond UX) for details.
   a. Please note that RUX deployments do not support legacy authentication options such as LDAP, RADIUS, and TACACS+ that were available in QUX deployments. Local authentication, which uses accounts defined in the Vectra UI, is still available in RUX deployments.

d. Setup your SIEM, SOAR integrations.
   a. Please note that the Respond UX does not support direct syslog output but if your integration requires syslog, an intermediary can be used to pull the required data via API calls, and then forward it using syslog. Please see SIEM Connector for the Vectra AI Platform (Respond UX) for details.
   b. It is recommended to directly use the API with the Respond UX. Several integrations using the API have already been published such as Splunk, Qradar, Sentinel, Splunk SOAR, PAN XSOAR, ServiceNow SIR, and ServiceNow ITSM.

e. If you use the Vectra API, the v2.x API endpoints that were used on your QUX deployment will no longer work. You will need to use v3.x API endpoints that are designed for your new RUX deployment. You will need to create new authentication tokens (using OAUTH) for any API clients. Please note that while the API is largely backwards-compatible, the API authentication is not. Any custom integrations that use the API will have to be updated. Please work with your Vectra account team if you wish for Vectra to assist with migration of custom API scripts. Please see the following KB articles for v3.x API details:
   a. Vectra Platform API Guide v3.4 (RUX)
   b. Vectra Platform API Quick Start Tutorial (RUX)