Vectra Platform

Getting Started Guide

Version: December 16, 2022

Table of Contents

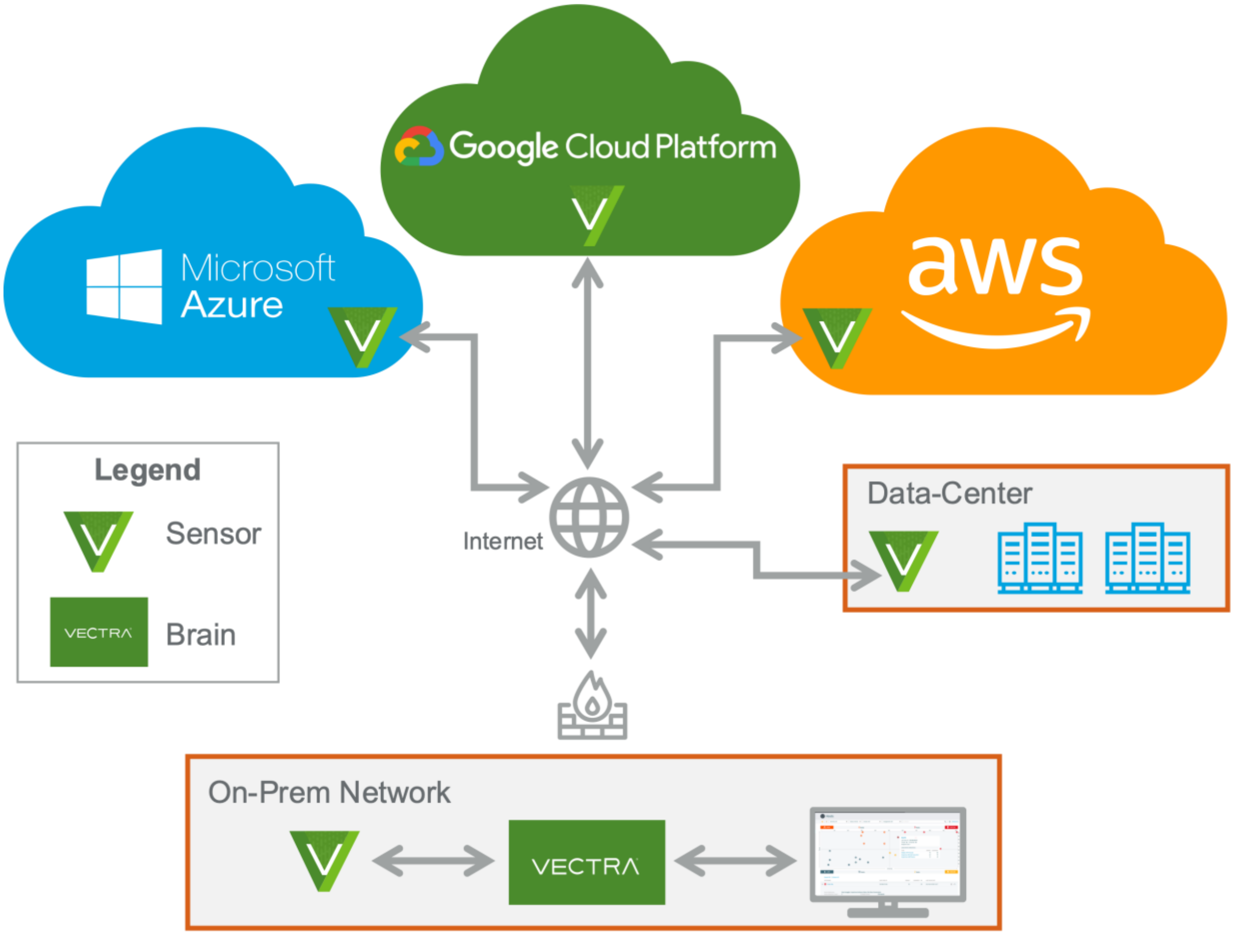
Introduction

This guide is intended to help customers or partners get started with the Vectra Platform. This will include an overview of the platform including components and Vectra terminology. It covers basic network connectivity requirements (firewall rules that may be needed in your environment), guidance for air-gapped deployments, initial settings, and recommended next steps. It is intended for use regardless of your deployment method (physical appliances, virtual appliances, cloud (IaaS), etc.

This guide is meant to be used in conjunction with other deployment guide that can be found on the Vectra support site. A good starting point for related documents is the Vectra Product Documentation Index. Here you will find quick start guides to get any physical appliances on your network, the physical appliance pairing guide, guides for vSensors deployed on hypervisors in your own infrastructure, guides for deploying the platform and Sensors in IaaS cloud infrastructures, and more.

Platform Overview

Any Vectra deployment will include some components of the overall Vectra platform. In its simplest form a deployment consists of a Brain which receives metadata from paired Sensors. Those Sensors can be physical, virtual, or cloud based. The Vectra Brain can also receive or pull data from a number of sources to enrich its learning or add context for analysts. It can also integrate with external tools to enact response.



The diagram above shows a conceptual high-level deployment with Sensors in IaaS clouds, an internet connected private data center, and an on-premise network that also houses the Brain. Deployments in the real world can span hundreds of sites and utilize both public internet and private connectivity. The simplest deployment is a single Vectra X-series appliance that is deployed in mixed mode and acts as both a Brain and Sensor.

The metadata that Vectra processes is valuable to customers for investigation, compliance, security posture assessment, and many other reasons. Metadata can be made available to customers via Stream and Recall.

Vectra Products

- **Detect for Network**
  - Always-learning behavioral models use AI to find hidden and unknown attackers, enable quick, decisive action, and provide a clear starting point for AI-assisted threat hunting.
- **Detect for Microsoft 365 and Azure Ad** – Available as SaaS or by deploying the Vectra platform.
  - Ingests activity logs from multiple services like O365, Azure AD, SharePoint/OneDrive, Teams, and Exchange. By analyzing events like logins, file creation/manipulation, DLP configuration, and mailbox routing configuration & automation changes, it accurately finds attacker behavior patterns.
- **Recall**
  - Cloud based SaaS solution that provides a comprehensive source of security-enriched network metadata and empowers security analysts and professional threat hunters to conduct conclusive incident investigations, compliance and security posture assessment.
- **Stream**
  - Translates Vectra's proprietary metadata into a Zeek compatible format and transfers it to a customer data lake. Like Recall, it provides a comprehensive source of security-enriched network metadata and empowers security analysts and professional threat hunters to conduct conclusive incident investigations, compliance and security posture assessment.
- **Detect for AWS** – Available as a SaaS offering
  - 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.

Appliance Modes

The 3 modes are Brain, Sensor, and Mixed. S series appliances and virtual Sensors can only function as Sensors. X series appliances can be configured as Brains or Sensors. The X29 appliance can also function in mixed mode.

Brain Mode

- Serves as the central point of management for the Vectra platform.
- Processes / deduplicates and optionally forwards metadata received from Sensors (when licensed for Recall or Stream).
- Runs Detect when licensed for it.

Sensor Mode

- Must be paired to Brain.
- Captures / deduplicates traffic.
- Forwards metadata to Brain.
- Houses rolling capture buffer to enable PCAP retrieval when requested from the Brain.

Mixed Mode

- Performs both Brain and Sensor functions.

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Basic Connectivity Requirements

The Vectra platform uses several TCP/UDP ports for different communication purposes. This document will detail basic requirements for initial setup and pairing. Many features and integrations are optional and not in scope for this document. For full detail on all possible firewall rules that might be required in your environment please see the following Vectra support portal article:

- Firewall requirements for Vectra appliances

Firewall/Proxy SSL Inspection

Please note that Vectra appliances validate SSL certificates for all HTTPS connections. For this reason, SSL/TLS inspection on firewall and proxy appliances must be disabled for these connections to work.

We have also identified that some firewall software transparently enables SSL inspection if certain filters (DNS hostname filtering) are enabled. This is not necessarily obvious to the administrator and should be investigated if connectivity issues are being observed.

Internet Access from Vectra Brain

The Vectra Brain requires connectivity to the automatic update service for normal operation. This connectivity is used for automatic (including security) updates and to synchronize keys for cryptographic authentication of Sensors.

The Brain requires Internet DNS resolution to obtain the IP addresses for these requests. The customer may choose public/Internet DNS servers or internal DNS servers; however, Internet DNS entries must be resolvable by the Brain. Please note that DNS is often considered to be a UDP-only protocol, however, TCP may be used depending on the type of DNS transaction. Both UDP and TCP use port 53 and should be permitted to all configured DNS servers.

Internet Access to Vectra Appliances (Physical or Virtual)

As with all security infrastructure Vectra appliances should be blocked from Internet access and access should only be granted from trusted workstations and/or authenticated sources.

Guidance for Air-Gapped Deployments

Certain customers may have a requirement to run in an air-gap configuration with no connectivity to the outside world or Vectra. This is a supported configuration, but you should be aware that there are some impacts:

- *Suspect Domain Activity* Detections will be disabled
- *Vectra Threat Intelligence* Detections will be disabled

In fully air gapped environments it is possible to do manual updates. You must work with your Vectra account team or Vectra support to get enabled for offline updates.

Additional guidance for version updates and pairing will be provided later in this document.

Connectivity Requirements (Firewall Rules)

Source	Destination	Protocol/Port	Description
Admin Hosts	Brain / Sensors	TCP/22 (SSH)	CLI access to Brains and Sensors
Admin Hosts	Brain	TCP/443 (HTTPS)	Web GUI interface
Brain / Stream	update2.vectranetworks.com (54.200.156.238)	TCP/443 (HTTPS)	Automatic updates and pairing key retrieval for physical Sensors
Brain	api.vectranetworks.com (54.200.5.9)	TCP/443 (HTTPS)	Health monitoring, algorithm support, reverse lookups for external IPs, Vectra Threat Intelligence, additional Detection context.
Brain (Cloud)	rp.vectranetworks.com (54.200.156.238)	TCP/443 (HTTPS)	Used only for Brains deployed in IaaS clouds. Used for authentication and verification (integrity check of the file system).
Brain	DNS servers (as configured)	TCP/53 UDP/53	DNS resolution, see above note for details regarding using both TCP and UDP
Brain	NTP servers (as configured)	UDP/123	Time synchronization
Brain	SMTP servers (as configured)	TCP (as configured)	Email alerting (optional but suggested)
Brain	Sensors / Stream	TCP/22 (SSH)	Remote management and troubleshooting
Sensors / Stream	Brain	TCP/22 (SSH) TCP/443 (HTTPS)	Pairing, metadata transfer, and ongoing communication
Stream	Data lake (as configured)	TCP (as configured)	Metadata streaming to data lake
Brain	Recall collector	TCP/443 (HTTPS)	Destinations provisioned after enabled

Connectivity Requirements (Firewall Rules) - optional but highly recommended

Source	Destination	Protocol/Port	Description
Brain	vpn.vectranetworks.com (74.201.86.229)	TCP/443 and UDP/9970	Remote Support VPN for remote troubleshooting. OpenVPN type if using firewall with App ID rules
Brain	metadata.vectra.ai (Multiple IPs, see article below for current details)	TCP/443 (HTTPS)	Optional anonymized metadata sharing to contribute to future algorithm development

- For additional detail and complete list of potential rules see: Firewall requirements for Vectra appliances

Why is Metadata Sharing Important?

Metadata Sharing improves threat detection by contributing anonymized metadata sourced from Brain deployed in your organization. You are contributing directly to the efficacy and accuracy of Vectra's detection capabilities and the security of your network. Access to detection metadata improves Vectra's threat detection algorithms, enabling the Vectra software you use to be more effective in a constantly evolving threat landscape. For full details please see the following Vectra support portal article that details this including additional optional levels of sharing:

- Why is Metadata Sharing Important

Brain Initial Installation and Configuration

Requirements

To configure your Vectra Brain physical appliance, you will need both CLI (Command Line Interface) and web-browser GUI (Graphical User Interface) access. The initial configuration at the CLI is covered in the *Quick Start Guide* for your Brain appliance. Please refer to that guide to configure an IP address, network mask, and default gateway on the Brain. You may have already configured DNS following that guide. If not, this guide will cover configuration of DNS using the GUI. Vectra Brains can also be deployed in IaaS clouds. This will not require CLI access (but it is available). It is recommended to proceed through all the below sections before any other configuration.

Login and Change the "admin" password

Once an IP has been configured for the MGT1 interface of your Brain, you can access it using a modern browser such as Edge, Chrome, or Safari at https://configured_IP or the hostname if you have configured a hostname in your DNS for the Brain. The GUI can also be accessed via MGT2 (on physical appliances) at https://169.254.0.10. The default username is **"admin"** and the default password is **"changethispassword".**

Please note that by default, Vectra uses a self-signed certificate to secure the user interface. As a result, the certificate causes SSL warning in most web browsers. Instructions for how to replace this with a customer-provided signed certificate can be found in the following Vectra support portal article:

- SSL Certificate Installation

After logging in to the GUI, it is recommended to immediately change the "admin" password.

- Navigate to "My Profile" on the left-hand side of the screen
- Click on "Change Password" in the username/password area, fill in and save the form
- Password requirements - must be at least 8 characters long and contain at least
  - 1 digit (0-9), 1 upper case letter (A-Z), 1 lower case letter (a-z)
  - One symbol (~!@#$%^&*_-+=`| \ ( ){ }[ ]:;”’<>,.?/)

Settings > General > Brain

This area of the GUI displays various Brain settings and information and also has "Restart" and "Shut Down" links in blue. Click on the "Edit" link or pencil icon next to it to access the settings screen for this area.

- DNS Name
  - FQDN (Fully Qualified Domain Name) that can be used to pair Sensors and/or Stream to this Brain.
  - To use this value for pairing, change the pairing setting under General > Sensors to "DNS Name".
    - Additional guidance for pairing via IP or DNS will be given later in this document.

  - In general, it is recommended to configure your DNS with a proper hostname for the Brain.
- Management IP Address
  - This is not editable in the GUI but displays what the configured IP of the Brain is.
- Alias
  - The label for this brain within various areas within the Vectra platform.
- For linking in alerts/notifications (except AWS SecurityHub):
  - Choose either "DNS Name" or "Management IP Address".
  - This will determine the format of links in alerts/notifications.
  - Please also note that if you are configuring SAML based SSO to the Vectra UI, this setting will also control if the "SP ACS URL" and "SP Entity Provider" provided by Vectra during SAML setup for use at your IdP are hostname or IP based.
- Command Line Interface Password for Brain
  - This area allows you to change the CLI password for the Brain.
  - Setting this password can be done at the CLI using the "**set password**" command.

Settings > General > DNS Entries

These DNS settings apply to the Brain only. Sensor DNS is set individually at the CLI or via a configuration string when deploying vSensors using the command line.

- If you have not already configured DNS for the Brain at the CLI, please do so in this section.
- It is also highly recommended to enable Reverse DNS Lookup as well.
  - This is done under *Settings > External Connectors > Reverse DNS Lookup.*
  - Reverse DNS Lookup will utilize the DNS servers that are configured in *Settings > General > DNS Entries.*
  - Reverse DNS Lookup will help to contribute naming artifacts for automated Host Identification.

Settings > General > Internal IP Addresses (CIDR)

For proper algorithm operation and recognition of traffic directionality within Stream or Recall metadata it is important to accurately identify internal vs external IP space. By default, all RFC-1918 IP space is considered "internal".

- RFC-1918 IP space
  - https://tools.ietf.org/html/rfc1918
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- Internal IP Addresses (CIDR)
  - IP addresses or CIDR blocks entered here will be considered internal to your network.
  - Everything else will be considered external.
- Exclude a Subset of Internal IP Addresses (CIDR)
  - Use this area if you have a subset of internal IP addresses listed above you want to be considered external to your network.
- Drop IP Addresses (CIDR)
  - IP addresses or CIDR blocks entered here will be ignored.
  - Any traffic to or from these addresses will not be analyzed by your platform.
  - Ignoring traffic by VLAN is supported at the CLI using the **"set capture-vlan"** command.

Fox example, if you were going to simulate Command and Control behavior from an internal lab, you should configure the lab IP space as external (excluded in the middle section). This lets Detect models properly identify the behavior.

Settings > General > NTP Entries

Vectra provides some defaults here but please set your preferred sources here.

Settings > General > PCAP Generation

PCAPS provide great value to analysts in a number of scenarios. PCAPs are assembled from the Sensor's rolling capture buffer upon request from the Brain during the publishing of Detection alerts. In some circumstances, customers may not want to have PCAPs generated at all or from certain Sensors that may be deployed in areas with stricter privacy controls that don't allow for PCAP.

- Edit in this area to turn off PCAP generation entirely.
- To turn off PCAP generation on an individual Sensor go to *Manage > Sensors*, select the Sensor you wish to edit, click the edit pencil, and then deselect the "Capture PCAPs for this Sensor" checkbox.

Settings > General > Sensors

In this area you can configure a number of options related to Sensor pairing and change the password for paired devices (Sensors or Stream).

- Sensor Registration Token
    - This is used to validate devices attempting to register to this Brain and resets every 24 hours.
    - It is used in the Registration Token field in the Sensor deployment template for cloud Sensors.
    - While the Sensor Registration Token (SRT) is required for cloud Sensor deployment, it is optional for physical Sensors and virtual Sensors.
    - Use of the SRT will allow you to pair a Sensor with any Brain in your organization. This can be useful for disaster recovery scenarios where a device may have been paired to another Brain previously.
    - After a Sensor registers with this Brain, it will appear in the Sensor list in *Manage > Sensors* where its pairing can be managed.
    - Stream devices will show paring status in *Settings > Cognito Stream > Pairing Status.*
    - Additional detail on pairing procedures will be shared later in this document and in the deployment guides for virtual Sensors.
- Pair using the Vectra Brain
    - This allows you to choose to pair via DNS name or Management IP (MGT1).
    - Pairing via the Brain DNS Name makes Brain replacement or IP Address change events easier to manage.
    - Customers may configure the DNS name of the Brain under *Settings > General > Brain.*
    - If you have not configured a hostname then you will only be able to pair by IP.
    - This setting affects future pairing operations only.
    - Any previously paired devices will remain paired regardless of how they were paired.
    - Should you choose to change the pairing method for previously paired devices, you will need to unpair the previously paired devices and re-pair them.
- Virtual Sensor Automatic Pairing
    - This setting allows you to choose if you want to automatically pair with virtual Sensors when they announce their availability.
    - It is recommended to allow auto pairing during initial setup or during large virtual Sensor rollouts.
    - When you are done deploying virtual Sensors, you may turn this off to enhance security posture.
- CLI Password for Paired Devices
    - In this area you can change the password for all paired Sensor or Stream appliances and easily keep passwords in sync.
    - If you require separate passwords for each Sensor or Stream appliance, the password for the

"vectra" user may be changed individually using the CLI **"set password"** command

Settings > General > Static IP Addresses (CIDR)

In many customer environments, Vectra's automated Host Identification (Host ID) is all that is required for customers to have all the pertinent hosts in their environment named and tracked. Generic hosts (IP-x.x.x.x) will inevitably be seen when a host comes into the environment, but not enough artifacts have been observed to create a stable named host or attribute its traffic to a previously created host. This can commonly happen when a user plugs in a laptop for the day, but the host is not recognized immediately. Vectra manages this on its own and will attribute traffic for this generic host to the real named host once it is recognized.

Many customers also have statically assigned hosts and may not even have hostnames in the customer DNS. Additionally, Vectra may not directly observe enough artifacts of other types to name the host. If a stable host never gets created, learning for several models cannot be anchored to generic hosts. This means that some Detections cannot fire and features such as the Host Role cannot function on these generic hosts.

- Enter IP addresses or CIDR blocks representing the statically assigned hosts in your environment in this area.
- Hosts on these IPs or ranges will show as STATIC-x.x.x.x in the Vectra UI and will no longer be generic hosts.
- These hosts will have full support for learning and all Detections and features.
- Statically defined hosts will not change name based on observed artifacts - they will remain static until they are no longer configured as such.
    - You are free to rename statically assigned hosts as you wish.

Settings > General > Timezone

Use this area to configure the timezone that you wish all Vectra platform data to use. This affects timestamps in logs, etc. The timezone defaults to UTC.

Settings > General > Version

This area displays version information for the platform. Editing the settings in this area allows you to set a preferred update window for automatic updates from Vectra. Automatic updates require a connection to updates2.vectranetworks.com. This area will have additional functionality if you have been enabled for offline updates. Please note the following for air gap scenarios:

- Offline updates must be enabled for your deployment by contacting your Vectra account team or Vectra Support.
- Once enabled for offline updates a "Manually update" link will appear in this area.
- For additional information about performing manual (offline) updates, please see the following Vectra support portal article here:
    - Offline Updates

Settings > Notifications > SMTP

This area enables you to configure the settings for an SMTP connector to send alerts from your Vectra platform deployment. This must be setup before you are able to configure Alert Emails. Select the “Edit” or pencil link to edit the settings and then:

- Fill in the IP or hostname and port for your STMP server.
- Select a protocol of (SMTP, STARTTLS, or ESMTPS).
- Fill in the Sender name.
- Fill in the STMP Username.
- Fill in the password.
- Once you have saved your STMP settings, a “Test” link will appear under the edit button. Click this to see if the settings work and also check your email folder. If you do not get an error on the Vectra side and still do not receive your email, check you spam folder and adjust your spam filter settings to allow the message.

Settings > Notifications > Alert Emails

Alert emails can be sent to email addresses or aliases. Enter the desired recipients in the top box. Alert types:

- Send campaign alerts
    - Attack Campaigns are formed when there is at least one active advanced command & control Detection, and several other hosts are observed to be communicating with the same domain or IP address.
    - These alerts are sent when a Campaign is created or closed.
- Send host alerts
    - These alerts are sent when a host crosses the scoring threshold that is configured.
    - Alerts are also sent when there is a Detection on a Host that is marked as a “Key Asset”. This alert does not rely on a threshold, only that the host is a “Key Asset” and has a new Detection.
    - The Threat and Certainty thresholds are configurable.
    - You may also choose to require that thresholds both be crossed or either crossed by clicking on blue pill between the thresholds thus selecting the “and” or “or” option.
- Send account alerts
    - These alerts are sent when an account crosses the scoring threshold that is configured.
    - Alerts are also sent when there is a Detection on an account that involves a Host that is marked as a “Key Asset”. This alert does not rely on a threshold, only that a host in the Detection details of the Account based Detection is a “Key Asset” and has a new Detection.
    - The Threat and Certainty thresholds are configurable.
    - You may also choose to require that thresholds both be crossed or either crossed by clicking on blue pill between the thresholds thus selecting the “and” or “or” option.
- Send detection alerts
    - These alerts are sent when any selected Detection scores above the configured certainty threshold.
    - For many customers, Host or Account scoring will drive prioritization for investigation by analysts.
    - Some customers may want Detection alerts for specific Detections that they consider critical, such as *Ransomware*, regardless of the current Host or Account score.
- Send system alerts
    - Alerts related to system operations are sent.
    - Examples are when there is a change in Sensor connectivity, capture interface health, or disk health.
- Send vCenter alerts
    - Alert related to changes in vCenter, such as new physical hosts being spun up that do not have vSensor coverage.
    - This requires vCenter integration to be setup.

Vectra Cloud Connectivity

All communications with the Vectra Cloud occur over a TLS encrypted channel. Appliance devices (physical, virtual, cloud) authenticate using keys. Unique public/private keys are generated when a device is provisioned by Vectra. The corresponding public key is copied to the Vectra Cloud. Every device connecting to the Vectra Cloud authenticates using its own private key.

The Vectra Cloud houses a number of services and products:

- update2.vectranetworks.com
  - Used for delivering updates to the Vectra software as they are released (per the update window selection made previously).
  - Offline updates as supported as previously described.
- api.vectranetworks.com
  - Used for health monitoring of the Vecvtra platform and for delivering additional context certain Detections may need.
  - Queries to external information sources to provide context, such a Virustotal lookup, are proxied through this connection.
  - If required, customers can block the platform from reporting health monitoring by blocking outbound connections on their firewall to api.vectranetworks.com.
- rp.vectranetworks.com
  - Used only for Brains deployed in IaaS clouds. Used for authentication and verification (integrity check of the file system).
- metadata.vectra.ai
  - As discussed earlier, metadata sharing improves threat detection by contributing anonymized metadata sourced from Brain deployed in your organization.
  - Additional detail is available below.
- Remote support VPN
  - This enables remote troubleshooting from authorized Vectra employees.
  - Additional detail is available below.
- SaaS product offerings such as Recall

Settings > Services > Proxy Config & Connection Status

Vectra Cloud connectivity to update2.vectranetworks.com and api.vectranetworks.com supports connecting through a customer proxy. If a proxy connection is required, click on the edit button in the “Proxy Config & Connection Status” section of the Services page and configure the settings for your proxy.

- Note that Remote Support VPN does not support proxy configuration by default. If this is the only option, please contact Vectra support to configure Remote Support to manually to use a proxy.

Lightweight Health Monitoring

The lightweight health monitoring includes the following statistics, only aggregate statistics are collected, no details are collected

- System Health Metrics
  - Installed packages, running processes, system interface information, system usage, database usage, system error stats
- Environment Metrics

    - Host counts, traffic counts, Brain configuration, VPN status, notification status, metadata status
- Detection Metrics
    - Detection counts, PCAP stats, Triage stats

Remote Support VPN

This is optional and allows Vectra Support access to the UI and shell for remote support, debugging, address potential performance problems, verify software updates, and perform troubleshooting.

- Utilizes Open VPN on TCP:443 and UDP:9970.
- Access to the shell is two factor secured, requires a support ticket to be logged, and is audited.
- Please note that this can be toggled on and off as required if you would prefer to not leave it enabled.
- In situations where direct access will not be allowed due to policy, Vectra Support can also do screen sharing sessions with a customer observer but some diagnostics will not be possible due to product security needs.

Metadata Sharing

- Metadata Sharing Improves Threat Detection
    - By contributing anonymized metadata sourced from the X-series platform deployed in your organization, you are contributing directly to the efficacy and accuracy of the Vectra software and the security of your network.
    - Access to Detection metadata improves Vectra's threat detection algorithms, enabling the Vectra software you use to be more effective in a constantly evolving threat landscape.
    - Data is collected daily and includes:
        - Anonymized information about Detections that are triggered in your network.
        - Anonymized information about algorithms in the research and development phase (and not yet visible in the UI) that are triggered in your network.
        - Anonymized attribution of Detections to Hosts.
        - Anonymized information related to host identification efficacy.
- Vectra Secures and Limits Access to Metadata
    - Any metadata you contribute is anonymized by removing personal and network-specific information before it is sent to metadata.vectranetworks.com via an encrypted connection.
    - Vectra treats this metadata as highly confidential and only allows authorized research personnel to access the metadata.
    - Any metadata collected is securely deleted after a six-month period.
- Contact Vectra support if non-anonymized Full Metadata Sharing is desired
    - Algorithm development using non-anonymized metadata helps to ensure that new models function as efficiently as possible in your environment.

Recommended Next Steps

Configure and pair any physical, virtual (including IaaS cloud based) Sensors required for your deployment.

Vectra offers a variety of deployment services and consulting options for customers that need more help or expert analyst assistance. Please work with your Vectra account team for additional details.

This guide covered initial configuration of basic settings. There are a number of other settings and options that you should consider examining and implementing:

- Work on traffic engineering and getting traffic flowing to your Sensors or mixed mode Brain.
- Add virtual or cloud Sensors.
- Integrations that help with HostID such as:
  - vCenter integration if you have a VMware environment.
  - DHCP and Windows Event Log ingestion.
  - EDR integration.
  - AWS Resource Manager integration.
- Integrations that bring additional context to analysts.
  - The integrations listed above to help with HostID also bring additional context.
  - AD integration.
- Integrations to enable taking action.
  - AD and EDR integration bring host and account Lockdown capability.
  - Scripts to enable taking action in other tools such as SentinelOne, PAN FWs, etc.
- Enabling Recall or Stream.
- Enabling syslog or Kafka output to SIEMs or CLM servers.
- Setting up SSO or external authentication sources.
  - Enabling differing roles for different types of users (admins, analysts, view only, etc).
- Setting up automated backup.
- Installing a signed certificate for the GUI.
- Building groups and triage rules to suppress detection for authorized behaviors.

Please note the following best practices:

- Change default passwords for the “admin” (GUI) and “vectra” (CLI and IPMI/iDRAC) users to strong versions.
- Limit exposure to admin interfaces through firewall rules that permit communication only from appropriate nodes/networks (including Vectra required endpoints as well).
- IPMI / iDRAC interfaces should be on their own isolated networks when possible.

Worldwide Support Contact Information

- Support portal: https://support.vectra.ai
- Email: support@vectra.ai (preferred contact method)
- Additional information: https://www.vectra.ai/support