+

Vectra AI Platform – 8.7 Release Notes

The Vectra® X-series appliances, B-series appliances, S-series sensors, VM and Cloud Brain, VM and Cloud Sensors, are scheduled to be updated to Vectra Network software release version 8.7. The version 8.7 release includes the introduction of a GCP Brain, improved Suricata detection functionality, and additional Azure AD / M365 detections. The 8.7 release also includes a reminder for an end-of-life notice for the X80 and S2 hardware platforms.

8.7 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after August 27th, 2024
  - You can check if you have remote support enabled under Settings -> Services with Remote Support set to Enabled.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on or after September 3rd, 2024
  - You can check if you are connected to Updater under Settings -> Services and see that Updater Destination shows as connected, while Remote Support shows disabled.
- **All Other Customers***: Will be able to download the update on or after September 3rd, 2024
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Introduction of GCP Brain — Network

Starting in 8.7, Vectra is introducing support for a new Brain hosted in Google Cloud Platform, or GCP. The GCP Brain is capable of handling 50Gb/s of traffic and supports all of the same features as other Cloud/Virtual/Hardware Brains. For more information, please see our deployment guide: https://support.vectra.ai/s/article/KB-VS-1803

Suspect Protocol Activity Detections — Network

Starting in 8.7, Vectra is introducing a new set of dynamic detections called Suspect Protocol Activity detections. These detections are currently for Command and Control and supported on HTTP, HTTPS, DNS, and TCP protocols, and enable Vectra to publish new detections much more quickly than traditional detections. This feature is off by default but can be customer enabled and is included as part of the standard Detect product line. For more information, please see https://support.vectra.ai/s/article/KB-VS-1793

Selective PCAP Support in Respond UX — Network

Starting in 8.7, Selective PCAP support has been added to Respond UX. Selective PCAP is already available in Quadrant UX, but support has been added in Respond UX to enable diagnostic troubleshooting of packets arriving on sensor interfaces. The feature works exactly the same as it does in Quadrant UX, for more information see: https://support.vectra.ai/s/article/KB-VS-1579

Detections

New Detection – M365 Suspicious Copilot for M365 Access — M365/AAD

Copilot is OpenAI's ChatGPT embedded into M365 enabling the use of Large Language Models (LLMs) on an organization's data. New Vectra coverage has been released to surface reconnaissance behaviors related to the use of Copilot in an M365 environment. The new Suspicious Copilot for M365 Access detection alerts when a Copilot for M365 session is initiated by a user originating an unusual location. An attacker may be using the Copilot for M365 functionality to simplify their ability to discover knowledge documented within your environment that can help them enable their next steps in their attack (i.e. IT policies and procedures, documented static passwords/accounts, etc.)

New Detection – Azure AD Login from Suspicious Location M365/AAD

New coverage has been released to surface command & control behaviors of logins from suspicious locations. The new Azure AD Login from Suspicious Location alerts when a successful login is observed from a country that is unusual for this tenant. An attacker may sign into the account they compromised from their true location or from a random proxy system that does not consider the valid user's normal expected location.

New AWS Region Ingestion Support AWS

Vectra has enabled support for new AWS regions to ensure customers can leverage AWS CDR regardless of their region. The new regions supported are:

il-central-1	Israel (Tel Aviv)
me-south-1	Middle East (Bahrain)
me-central-1	Middle East (UAE)

Reminder: X80 and S2 Platform End-of-Life Notice

The X80 and S2 hardware platforms will be EOL on January 7th, 2025.

After the 7th of January 2025, Vectra will no longer support:

- Software upgrades for X80 and S2 appliances.
- Software upgrades for brain appliances where an S2 sensor is paired.
- Hardware replacements for X80 or S2 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X80 or S2 hardware prior to the 7th of January 2025.

Bug Fixes

DATA-7020: DNS Metadata Updated to Support Non-UTF-8 Characters

DNS metadata has been updated to support non-UTF characters. If non-UTF characters are present in the query or response fields, Vectra will encode them into Base64 so they can appear in the metadata properly. For more information, please see https://support.vectra.ai/s/article/KB-VS-1245

CS-9233: Multi-domain AD Integration Issue

Resolved an intermittent issue where users would not be displayed all of their AD integrations when more than 1 was first connected. This issue has now been addressed.

CS-9178: Data Source Page Returned Error

Resolved an intermittent issue where users would receive an error upon navigating to the Data Source settings page in GUI. This issue has now been addressed.

CS-9242: Internal Nameserver Issue

Resolved an intermittent issue where in certain scenarios some internal nameservers were not returned accurately which resulted in slight impact to DNS Tunnel detections. This issue has now been addressed.

CS-8921: Virtual Infrastructure Page Displays Incorrectly

Resolved an issue where connectivity issues from the brain to vCenter were not displayed in the health dashboard. This issue has now been addressed.

CS-8684: Stream Metadata Stats Download

Resolved an intermittent issue where certain customers encountered an error upon downloading Stream metadata stats from the GUI. This issue has now been addressed.

PROD-1389: Improved Advanced Search

Starting in 8.7, the database replication performance has increased allowing Advanced Search to be available at higher observed traffic levels. This issue has been addressed.

Appendix:

Will this upgrade perform a reboot of the Brain or Sensors?

No, a reboot is not required as part of the 8.7 update.