# Vectra Detect Platform Software Update

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 8.5. The version 8.5 release includes a Vectra Match curated ruleset, Respond UX support for Vectra Match, IPv6 management support, additional configuration options for backup restore, and various detection enhancements. The 8.5 release also includes a reminder for an end-of-life notice for the X80 and S2 hardware platforms.

## Release Schedule

8.5 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after July 1st, 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 July 10th, 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 July 10th, 2024
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

## Platform

### Vectra Match – Curated Ruleset

Network

Starting in 8.5, Vectra has introduced a downloadable link that allows users to retrieve the curated ruleset for Vectra Match. A new link will appear in the UI on the Vectra Match page for updated daily content, as well as consumable via API.  Please see Vectra Match Curated Ruleset for more details.

### Vectra Match – Respond UX Support

Network

Starting in 8.5, Vectra Match is supported in Respond UX. Respond UX support brings all the WebUI and API support delivered in Quadrant UX, and adds Instant and Advanced Investigation support for Match alerts.  Please see the Match Deployment Guide for additional details.

### IPv6 Management Support

Network

Starting in 8.5, Vectra has added IPv6 Management support for Brain and Sensors.  This means that you can administer Brain's and Sensor's via IPv6 addresses (in addition to IPv4), and the Brains and Sensors can use IPv6 to communicate.  Note that this does not introduce IPv6 support for AI detections, however IPv6 is already supported by Match, Stream, and Recall.  For more information, please see IPv6 Management Support for Vectra Appliances for more details.

### Backup Restore Configuration Options Network

Starting in 8.5, Vectra has introduced the ability for customers performing backup restore via CLI to configure multiple external targets. In version 8.5 and higher of Vectra Brain software, backup and restore functionality has been updated to be more consistent in how the commands work for the various different options available in backup/restore. As a result, new backup jobs must use the new syntax. Please see Backup and Restore for Vectra Brain Appliances (v8.5+) for more details.

### Multi-AD Profile Limit Network

Starting in 8.5, customers will be presented with a tooltip when multi-AD profiles are nearing the profile limit (e.g., 20) for what Vectra can handle. This will notify users through a tooltip on the integration page and warning message on the “Add Active Directory” modal that upon saving the next AD profile, users will reach the maximum amount of AD profiles.

## Detections

### ICMP Tunnel – AI-Triage Support Network

Vectra has added the ICMP C2, Exfil, Lateral Client and Lateral Server detections to AI-Triage so now AI-Triage will be able to triage out benign true positive detections. No user action is required.

### Hidden DNS Tunnel (C2 and Exfil) Detection Improvement Network

Vectra has made significant improvements to the Hidden DNS Tunnel C2 and Exfil detections to detect more exotic forms of DNS tunneling, as well as reducing benign scenarios where the model may have previously triggered. No user action is required.

### Scoring and Prioritization Enhancement Network

Starting in 8.5, Vectra has improved the Scoring and Prioritization for the family of Privilege Access Analytics (PAA) and Suspicious Admin detections such that a single PAA or Suspicious Admin detection will no longer result in a host / account going to the high quadrant.

### Deeper Identity Coverage for tactics observed in Midnight Blizzard M365/AAD

Enhancements have been made to our Azure AD Successful Brute-Force detection and Azure AD Suspicious OAuth Application detection to provide deeper coverage against compromises associated with the Russian state-sponsored actor Midnight Blizzard (aka NOBELIUM, APT29). These enhancements enable improved visibility into advanced password spraying techniques and abuse of OAuth applications aimed at establishing persistence.

### New Detection - Azure AD New Partner Added to Organization M365/AAD

New identity-centric coverage has been released to surface behaviors around creation of redundant privileged access. The Azure AD New Partner Added to Organization detection alerts when new persistent access is established to the environment via the addition of a new AAD Partner. Partners can be leveraged to take privileged actions within the environment.

### New Detection - Azure AD New Certification Authority Registered M365/AAD

New coverage has been released to surface behaviors around abuse of elevated privileges. The Azure AD New Certification Authority Registered detection alerts on backdoors leveraging password-less authentication for persistence. Attackers could register their own certification authority to create backdoor access into the environment.

### New Detection – M365 Link Sent by External Teams User M365/AAD

New coverage has been released to surface behaviors around spearphishing campaigns. The M365 Link Sent by External Teams User detection alerts when an external Teams user sends URLs or attachments to internal users. External users are not directly part of the organization (for example, contractors). This behavior could be indicative of spearphishing/whaling campaigns or an attempt to infect target accounts with malware.

### Improved M365 and AAD detection reporting times M365/AAD

Significant enhancements have been released to Vectra's real-time cloud detection engine. These enhancements improve M365/AAD detection reporting times **by over 17X in cases**, enabling defenders to stop identity-centric attackers before they can do damage. Jetstream is now able to deliver true AI-driven M365 and AAD detections at far superior velocity to counter the speed of fast-moving attackers.

## 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

### CS-8965 / VULNS-1576: Deletion of Groups

Resolves an issue where users can delete groups marked as undeletable if created by other users. This has now been addressed.

### GS-9428: Multi-AD UI Enhancement

Resolves an intermittent issue where users are presented with the overview panel for Multi-AD after saving the first AD profile or deleting the last AD profile, instead of remaining on the edit panel. This has now been addressed.

### BRIDGE-549: Group Search Filter on Accounts Page

Resolves an intermittent issue where "Groups” search filter is not fully functional on the All-Accounts Page and certain search parameters were not taken into account. This has now been addressed.

### CS-9170: Host Page Icons Displaying Incorrectly

Resolves an issue, where in certain situations, the icons representing hosts on the Host page are not showing colors (e.g., icons are all greyed out). This has now been addressed.

## Appendix:

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

No, a reboot is not required as part of the 8.5 update.