+

Vectra AI Platform – 8.10 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 8.10. The version 8.10 release includes backup downtime enhancements, a new VMWare vSensor, additional Network / M365 / AAD detections, and various bug fixes. The 8.10 release also includes a final reminder for an end-of-life notice for the X80 and S2 hardware platforms.

8.10 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after January 28th, 2025.
    - You can check if you have remote support enabled under Settings > General with Remote Support set to Enabled.
    - If you plan to enable or disable Remote Support in the near future, please reach out to Support to confirm if you will receive or skip the upgrade.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on or after January 28th, 2025.
    - You can check if you are connected to Updater under Data Source > Brain-Setup > Proxy & Status 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 February 6th, 2025.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Backup Downtime Enhancements Network

Starting in 8.10, Vectra has improved the Backup downtime to take less than ten minutes to complete. The usability of the backup function remains the same, this solution introduces a drastically reduced completion time for backups.

New VMWare vSensor Network

Starting in 8.10, Vectra is increasing the bandwidth capabilities of VMWare vSensors. The VMWare Sensors are capable of handling 20Gb/s of traffic and support all the same features as other Cloud/Virtual/Hardware Sensors. For more information, please see our deployment guide: https://support.vectra.ai/s/article/KB-VS-1075

Detections

Hidden DNS Tunnel NoReply Enhancement Network

As part of the 8.10 release, Vectra has improved our Hidden DNS Tunnel detection to detect scenarios where an attacker may attempt to exfiltrate data over DNS using techniques where the server does not respond (thus the tunnel is only a one sided tunnel where the attacker streams the data from In to Out.).

Scoring Enhancements to Azure AD and M365 Detections M365/AAD

Enhancements have been introduced to the following Microsoft 365 and Azure AD detections to better account for the risk of the underlying behaviors and surface them promptly for review. Introduction of these enhancements may result in changes to the number of entities prioritized within the Vectra platform:

- **Azure AD/Entra ID**
  - **Azure AD Domain Settings Modified**: This detection alerts when a new unverified or verified domain is suspiciously added to the environment.
  - **Azure AD Cross-Tenant Access Change:** This detection alerts when a partner's cross tenant access settings are added or updated.
  - **Azure AD New Certification Authority Registered:** This detection alerts when a new Certification Authority is registered to the tenant.
  - **Azure AD Privilege Operation Anomaly:** This detection alerts on potential privilege escalation or account takeover behaviors within the environment. The enhancements made to this detection result in significant improvements in the fidelity of this detection and reduction in the rate of false positives.
- **Microsoft 365**
  - **M365 Phishing Simulation Configuration Change:** This detection alerts when the configuration associated with a Phishing account is changed.
  - **M365 SecOps Mailbox Change:** This detection alerts when the configuration associated with a SecOps account is changed.

Additional details on these detections can be found in the 'Understanding Vectra AI Detections' guide available on the Vectra support portal.

Reminder: X80 and S2 Platform End-of-Life

The X80 and S2 hardware platforms are now EOL as of January 7th, 2025.

Please contact your Vectra account team to discuss options.

Bug Fixes

CS-9615: Host Group Not Reflected on Host Page

Resolved an issue in which a Host’s group is not indicated in the UI on the Host page. This problem has been addressed.

CS-9627: Host Group Members Disappeared

Resolved an issue in which adding new Hosts to a Group cleared the Group’s initial contents. This problem has been addressed.

GS-9762: Sensu Customer Syslogs Aren’t Sending Proper Source Serial & IP

Resolved an issue in which Sensu syslogs misreported that errors originated from the brain, when they were health alerts coming from the paired sensor. This problem has been resolved.

CS-9573: Manage User Does Not Show the "Login Type"

Resolved an issue in which in the Manage -> Users page, the ‘login type’ showed as empty, while the API query returned a value. This disconnect has been resolved.

CS-9362: Advanced Investigations Does Not Show the Correct Signature ID in the UI

Resolved an issue in RUX, where the Advanced Investigations page displayed the incorrect signature ID. The API endpoint showed the correct signature IDs. The UI has been corrected.

CS-9609: Automatic Mapping of Azure Domains to On Prem Disables Unexpectedly

Fixed an issue causing automatic Azure AD to AD account linking to be reset to manual. Customers who previously configured automatic linking will have it re-enabled.

Appendix:

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

FIPS Customers: Yes, customers abiding by the Federal Information Processing Standard will have their systems automatically rebooted as part of the 8.10 update.

Non-FIPS Customers: FIPS is off by default, and thus no reboot is required for any customer not running FIPS in 8.10

Determining Mode:

You can run the “show security-mode" command on the CLI of the Brain to determine if it is in FIPS mode or Default (non-FIPS). FIPS is off by default.