+

Vectra AI Platform – 8.9 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 8.9. The version 8.9 release includes the introduction of Vectra X3 system, troubleshooting enhancements, offline upgrade improvement, new GCP cloud sensors, air-gapped customers: Vectra Match curated ruleset download ability, backup/restore supports cloud connect migrations, additional Network / M365 / AAD detections, and various bug fixes. The 8.9 release also includes a reminder for an end-of-life notice for the X80 and S2 hardware platforms.

8.9 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after November 4th, 2024.
    - 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 November 13th, 2024.
    - 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 November 13th, 2024.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Introduction of Vectra X3 System — Network

Starting in 8.9, Vectra is introducing the new X3 system. Like other X-series systems, the X3 can be deployed as a Brain, Sensor, or in Mixed mode. It features all of the same features as the rest of the Vectra NDR product line, with performance ratings of

- Brain Mode 15Gbps
- Sensor Mode 9Gbps
- Mixed Mode 8Gbps

The hardware features 4x1Gbps Copper and 2 x 10Gbps SFP+. For more information about the appliance specs, please see our Datasheet at: https://content.vectra.ai/hubfs/downloadable-assets/Datasheet_Appliance-SensorSpecs.pdf

For the deployment guide see: https://support.vectra.ai/s/article/KB-VS-1814

Troubleshooting Enhancements — Network

Starting in 8.9, Vectra is improving the Troubleshooting facilities available in the platform. The following enhancements are introduced:

- “show pairing-status": Provides a new command to explore the pairing status of sensors to brains.

- “show interface all”: Provides more detailed output for the existing interfaces command, including all interfaces available in the system, which is particularly useful with Virtual and Cloud sensors which may have a different interface layout depending on the hypervisor.
- “show system-health": Provides additional monitoring for disk space consumption which is also provided for in a new syscheck.
- “show siem statistics”: Provides a new command which details statistics for the SIEM integration for DHCP stats.
- “status-report”: The status-report command has been enhanced to request status reports for hardware, including for RMA’s. This command can now be run from the Brain for sensors at the direction of Vectra support.
- ‘debug dns’: Provides a command to perform DNS troubleshooting to identify how DNS is being resolved from the viewpoint of Brain
- 'debug ntp’: Provides a command to perform NTP troubleshooting to identify how time is being resolved in NTP from the viewpoint of the Brain

Offline Upgrade Improvement — Network

Starting in 8.9, Vectra will provide a streamlined experience for Airgapped customers who perform offline upgrades. Rather than needing to perform upgrades sequentially one at a time, a bulk upgrade package can be prepared for the user so as little as a single file may need to be provided to the Vectra appliance to complete the upgrade process without additional intervention. For more information, please see: https://support.vectra.ai/s/article/KB-VS-1831

New GCP Cloud Sensors — Network

Starting in 8.9, Vectra is increasing the bandwidth capabilities of Sensors hosted in Google Cloud Platform, or GCP. The GCP Sensors are capable of handling 5Gb/s and 10Gb/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-1553

Air-Gapped Customers: Vectra Match Curated Ruleset Download Ability — Network

Vectra Match customers who are air-gapped can now download the Vectra Match Curated ruleset from the Vectra support portal: https://support.vectra.ai/s/login/ Prior to this improvement, only customers who were connected to Vectra would be able to download the ruleset within the platform; now air-gapped customers can receive it as well. For more information see our KB article: https://support.vectra.ai/s/article/KB-VS-1784

Backup/Restore Supports Cloud Connect Migrations — Network

Starting in 8.9, when using the “--replace” option when performing a restore will enable the Cloud connections to also be migrated to the new Brain which is important when running Respond UX and other cloud services. Prior to 8.9 Vectra support would need to assist. For more information please see https://support.vectra.ai/s/article/KB-VS-1782 under the restoring backups section.

Detections

New Hidden Tunnel Detection — Network

A new detection called Hidden Tunnel has been introduced for the Detect for Network platform. The Hidden Tunnel detection detects Command and Control channels over protocols that are not existing named detections (ICMP Tunnel, Hidden DNS Tunnel, Hidden HTTP Tunnel, Hidden HTTPS Tunnel.). For more information, please see the Understanding Vectra AI guide for details on all Vectra AI detections. https://support.vectra.ai/s/article/KB-VS-1285

Hidden HTTP Tunnel Update — Network

The Hidden HTTP tunnel detection has been enhanced to detect new and evasive forms of C2 tunnels over the HTTP protocol. A new tunnel sub-type has been introduced called beaconing-channel.

Hidden HTTPS Tunnel Update — Network

The Hidden HTTPS tunnel detection has been enhanced to detect new and evasive forms of C2 tunnels over the HTTPS protocol. A new tunnel sub-type has been introduced called beaconing-channel.

SQL Injection Update — Network

The SQL Injection detection has been enhanced to detect additional types of SQL injection. No changes to the UI or detection notes are present, but the underlying logic to the SQL Injection detection has been improved.

File Share Enumeration Scaling Improvement — Network

The File Share Enumeration detection has been improved to handle larger environments where a large volume of SMB data may have previously resulted in some File Share Enumeration detections to not published. There is no UI change or user action required.

SMB Account Scan Scaling Improvement — Network

The SMB Account Scan detection has been enhanced to handle larger environments where a large volume of SMB data may have previously resulted in some SMB Account Scan detections to not publish. In a very small number of customers, we are observing an uptick in SMB Account Scan detections as a result of the improved scale. Customers are encouraged to review the activity and create triage rules if the activity is benign. If additional assistance is required, please contact Vectra support. There is no UI change for this detection enhancement.

Azure AD Successful Brute Force – Failed Login — M365/AAD

New coverage has been released to provide deep coverage against sophisticated password spraying techniques. The new 'Azure AD Successful Brute Force - Failed Login' detection alerts when credentials associated with an Identity are validated but a login was not successful (reason indicated by an error code). Password brute force tools are known to use password spraying techniques that validate credentials without performing successful authentication allowing attackers to remain undetected. Techniques associated with this threat vector have been observed in activity by Russian state-sponsored hacking group Midnight Blizzard.

The new 'Azure AD Successful Brute Force - Failed Login' detection complements an existing Vectra AI detection 'Azure AD Successful Brute-Force' that surfaces instances where an attacker successfully logs into an environment.

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

PROD-1677: SQL-ES Deadlock Detection

Resolved an issue that caused SQL-ES to deadlock and pause service. This problem has been addressed by implementing a deadlock detection that forces a service restart to recover from a detected deadlock.

LUNA-690: Opening Hyperlink to Detections Shows 500 Page

Resolved an issue where a hyperlink to the detections page shows a 500 error page before moving on to the detections page. This issue has been addressed.

CS-9468: Hosts Sensor Filtering Not Listing All Sensors

Resolved an issue when trying to filter the Hosts page by sensors it does not show the recently deployed ones. This issue has been resolved.

CS-8842: Accounts Advanced Investigation LDAP Email Field Misnamed

Resolved an issue with of having two options in advanced search for account.ldap.email. One option resulted in nothing being returned while the other returned as expected. The faulty option was removed, and this resolves the issue.

CS-9125: Carbon Black EDR Integration Not Able to Retrieve Existing ‘Sensors’

Resolved an issue where hosts in the Brain UI portal accurately reported EDR: Carbon Black, but there is no panel for locking/unlocking the host. This problem 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 8.9 update.

If you skipped the 8.8 upgrade: The 8.9 release will upgrade the firmware on your system. Do not stop the 8.9 upgrade while in progress—doing so may render your system unstable.