+

Vectra AI Platform – 9.0 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 9.0. The version 9.0 release includes dynamic group support of QUX, high performance GCP brains, proxy support for Suspect Protocol Activity and Match, added southside proxy IPs command, improved traffic validation report, S1 SFP+ interfaces supported for management or capture. The 9.0 release also includes a final reminder for an end-of-life notice for the X80 and S2 hardware platforms.

9.0 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after March 12th, 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 March 12th, 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 March 20th, 2025.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Introduction of Dynamic Groups on Quadrant UX — Network

Starting in 9.0, Vectra now supports Dynamic Groups on the Quadrant UX. Dynamic Groups is a feature on the Vectra AI Platform that allows customers to use Regex rules to define what hosts or accounts should belong to each triage group, resulting in entities being automatically sorted into groups as they are detected. This feature will reduce the amount of time customers spend managing and updating groups. Respond UX support for this feature was introduced in December 2024. For more information see: https://support.vectra.ai/s/article/KB-VS-1839

High Performance GCP Brains — Network

Vectra has created a new 64 core variant of the GCP Brain and validated the existing 96 core Brain to support higher overall throughput than previously published. Please see the GCP Brain Deployment Guide for details. As of 9.0, Vectra supports the following configurations for GCP Brains:

VM Type	CPU Cores	Memory	Disk	Interfaces	Throughput
n2-highmem-64	64	512 GB	1.2 TB	1 (MGT)	~ 50 Gbps
n2-highmem-96	96	768 GB	4 TB	1 (MGT)	~ 85 Gbps

Proxy Support for Suspect Protocol Activity and Match — Network

Starting in 9.0, Vectra added automatic proxy support for Match and SPA. While no user action is required, additional variables for Match are available. Please see the Match FAQ for more details: https://support.vectra.ai/s/article/KB-VS-1635

Southside Proxy IPs via CLI — Network

Starting in 9.0, Vectra added support to view the southside learned list proxy IPs via command line. Southside Proxies identify Proxies where Vectra sits between the Client and the Proxy. This differs from Northside proxies which are configured under Manage -> Proxies in the UI. Use “show proxy --southside" to display southside proxies that the system has learned from observing the network traffic.

Improved Traffic Validation Report — Network

Starting in 9.0, Vectra has added new fields to the Enhanced Network Traffic Validation report available on the Network Stats page. The new fields include statistics on NIC errors, packet truncation, and drops/holes in traffic. For more information see: https://support.vectra.ais/article/KB-VS-1648

S1 SFP+ Interfaces Supported for MGT1 or Capture Use — Network

Starting in 9.0, Vectra now supports the use of the S1’s two onboard SFP+ interfaces for capture or management. The command **“set management <default|sfp>”** will alter the interface configuration for the MGT1 port. The command **“set capture <default|sfp>”** will alter the interface assignment used for capture. This creates 4 total configurations for management or capture. All options with new interface assignment diagrams for each are detailed in the S1 Quick Start Guide. Please note: The rated throughput of the S1 appliance does not change when using SFP+ ports. This only changes the physical interface assignments. Care should be taken to only forward a supported amount of traffic to the S1.

X29/M29 Appliance – New syntax for using SFP+ for MGT — Network

The X29/M29 appliances have an option to configure one of their SFP+ interfaces to be used as the MGT1 management port. The command has changed in version 9.0 to be consistent with the command syntax that is used now for all appliances that offer options to change similar interface options. The old command was **“set management speed <1G|10G>”** and the new command is **“set management <default|sfp>”**. Please see the X29 Quick Start Guide or the M29 Quick Start Guide for details.

Detections

Enhancements to AWS Detections — AWS

Enhancements have been introduced to the following AWS detections to improve the fidelity associated with them. Introduction of these enhancements results in broader coverage of malicious behaviors and may be associated with minor increases in prioritized entities within customer environments.

- **AWS CloudTrail Logging Disabled:** This detection alerts on the defense evasion technique of turning off AWS logging. Enhancements have been introduced to the model to broaden the behavioral profile representing this malicious behavior.
- **AWS CloudTrail Logging Modified:** This detection alerts on the defense evasion technique of downgrading AWS logging. Enhancements have been introduced to the model to broaden the behavioral profile representing this malicious behavior.
- **AWS User Hijacking:** This detection alerts on persistence techniques surrounding creation of AWS access keys. Additional learning has been introduced in this model to account for repetitive occurrence of behaviors and subsequent impact on volume of alerts surfaced. This enhancement results in improved efficacy of alerting around this risky behavior.

Scoring Enhancements to M365 Detections M365/AAD

Enhancements have been introduced to the following Microsoft 365 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:

- **M365 Suspect Power Automate Activity:** This detection alerts on potential exfiltration or C2 behaviors using Power Automate 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 observed within this detection and similar detections (M365 Power Automate HTTP Flow Creation and M365 Suspicious Power Automate Flow Creation).

Bug Fixes

CS-9810: Members of Regex-Based Groups are not Persistent

Resolved an issue in which members of a group based on regex would disappear after a few minutes. This problem has been resolved.

CS-9799: Fix Detection Timestamps

Resolved an issue in which the detection UI did not display the true time a detection first occurred. This problem has been resolved.

CS-9797/CS-9595: Triage Filters Based on External Domain Groups are not Applied

Resolved an issue in which adding a domain to the group does not accurately triage the detection. This issue has been resolved.

CS-9792: Groups Cannot be Edited

Resolved an issue in which groups could not be edited by users. This issue is resolved.

TM-5131 & TM-5417: VMWare Version Compatibility

Clarified documentation for VMWare hardware. Vectra only supports version 11 and 15 of VMWare hardware. Vectra does not recommend upgrading either version after deployment. For more information see: https://support.vectra.ai/s/article/KB-VS-1075

Appendix:

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

No, a reboot is not required as part of the 9.0 update.