+

Vectra AI Platform – 9.1 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 9.1. The version 9.1 release includes the introduction of the X47 system, SSL key handling improvements, altering group type on Quadrant UX, Vectra Match Suricata version upgrade, and Quadrant UX API version upgrade.

9.1 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after May 7th, 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 May 15th, 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 May 15th, 2025.
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Introduction of Vectra X47/M47 System — Network

Starting in 9.1, Vectra is introducing the new X47 and M47 systems. Like other X-series systems, the X47 can be deployed as a Brain, Sensor, or in Mixed mode. The M47 supports Vectra Stream at up to 75 Gbps rates. The M47/X47 performance is in the below chart:

Brain Mode	Sensor Mode	Mixed Mode	Sensor (Match) Mode	Mixed (Match) Mode	M47 Stream Mode
30 Gbps	20 Gbps	15 Gbps	13 Gbps	6 Gbps	75 Gbps

The hardware features 4x1Gbps Copper and 2 x 10/25 Gbps SFP28. For more information about the appliance specs, please see the Appliance and Sensor Specifications.

- For the deployment guides please see the X47 Quick Start Guide or M47 Quick Start Guide.

Altering Group Type on Quadrant UX — Network

Starting in 9.1, Vectra supports conversion between static and dynamic group types for QUX deployments. Existing triage filters that reference a static group, will continue to function without requiring any change after the group is redefined using a regex in the dynamic group configuration. This should allow for greater flexibility and ease of implementation as customers move to dynamic groups. For more information on dynamic groups see the Dynamic Groups FAQ

SSL Key Handling Improvements Network

Starting in 9.1, Vectra now supports Elliptic Curve Cryptography (ECC) certificates. Customers can upload their own certificate via the existing commands

Additionally, the commands supporting Certificate Signing Request (CSR) have been updated. Use

- `` `certificate replace-key` `` to generate a new key and self-signed cert for the HTTPS server to use, essentially resetting it to default but allowing the customer to customize the key length.
- `` `certificate info` `` to print some information on the current HTTPS certificate for the user to see.

For full certificate installation details, please see: SSL Certificate Installation (Quadrant UX only)

Vectra Match Suricata Version Upgrade Network

Vectra has upgraded the Suricata to support new features in the Suricata engine including JA4 and we have enabled protocol parsing for OT protocols. The suricata.yaml base configuration has also been upgraded to reflect the

latest Suricata features. For details on Vectra's Suricata configuration please see: Vectra Match Suricata Configuration.

Oauth2 Support Added for v2.x. QUX APIs Network

Vectra has updated the QUX v2.x APIs to include support for OAuh2 authentication. Now, both the existing Personal Access Token (PAT) and Oauth2 flow are supported in v2.x. The Oauth2 access token will be valid for 6 hours after which it will expire, and a new token will need to be requested using the API client credentials. API client creation must be done in the Vectra UI only. Accessing v2.x APIs older than v2.5 works the same way it does for v2.5. The public postman collection has been updated for all v2.x versions.

For more information see: REST API Quick Start Guide for Postman v2.5 using OAuth2 (QUX)

Detections

Hidden Tunnel Detection Improvement Network

The Hidden Tunnel detection has been improved to identify new beaconless connections which are contacting external systems. This enhancement provides new coverage for hidden tunnel command line based beaconless attack tools. For more information about the Hidden Tunnel detection in general, please see Understanding Vectra AI Detections.

RDP Recon Detection Enhancement Network

The RDP Recon detection has been enhanced to detect RDP Password Spray attacks which an attacker can attempt to test a small number of passwords against a large number of accounts. The previous version of RDP Recon focused on an attacker attempting to try a large number of passwords against an account, this enhancement extends the RDP Recon to cover scenarios where a very shallow brute force attack is conducted across many accounts.

AWS Detection Enhancements 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 Cryptomining:** This detection alerts on behaviors around multiple high powered compute instances being started. It has been expanded to surface a broader range of cyptomining activity attributed to both human and non-human principals. Customers may observe a small increase in volume of detections.
- **AWS Attack Tools:** This detection alerts on known attack tools in an AWS environment. It has been improved for fidelity and a lower false positive rate.

Signal Enhancements M365/AAD

Significantly reduced benign prioritization alerts through improvements to Vectra's AI prioritization algorithm and detection updates. In some cases, customers may see up to 50% fewer prioritized host and account alerts—without sacrificing coverage for real threats.

- **Azure AD & M365:** Prioritization alerts for accounts with specific detections have been refined, reducing benign alerts while maintaining detection of modern attacks. Affected detections include M365 DLL Hijacking Activity, Azure AD Suspicious Access from Cloud Provider, and Azure AD Suspicious Sign-on.
- **Network:** Prioritization alerts for hosts with specific detections have been refined, reducing benign alerts while maintaining detection of modern attacks. Affected detections include exhibiting patterns such as Suspicious Admin activity and co-occurrences of Port Scanning, Darknet Scanning, and Port Sweeps.

Online Improvements

The following improvements have been made to algorithms since the last software release cycle. Customers that are connected to Vectra's Update service with Remote Support enabled have received these improvements. All other customers will be receiving the following improvements as part of 9.1:

- NDR-96: This release introduces an improvement to our RDP Recon algorithm, expanding coverage of RDP Sweep attacks where evasions are in place to limit the quantity of passwords attempted per account.
- NDR-106: Improves our C2 detections against techniques used by Mythic C2.
- NDR-104: This release introduces attack coverage for the Apache Camel Case exploit: CVE-2025–27636.
- NDR-73: This release introduces an attack signal improvement for External Remote Access to decrease benign true positive detections to popular destinations.
- NDR-108: This release introduces an improvement to increase the scale and health of Beacon Detector when under heavy load, by limiting beacon metadata for popular benign destinations in the environment.

Bug Fixes

CS-9964: Triage Filter Not Filtering Against Custom Model

Resolved an issue in which custom models were not filtering correctly, due to a bug in the triage detection processing. This issue has been addressed.

CS-9954: SMTP Configuration using O365 Doesn’t Allow for Sign-In

Resolved an issue during SMTP configuration that caused the O365 connector to show an error while attempting to sign-in with a Microsoft account. This problem has been fixed.

CS-9830: Network Stats Page Error

Resolved an issue during SMTP configuration that caused the O365 connector to show an error while attempting to sign-in with a Microsoft account. This problem has been fixed.

CS-9787: Cannot Delete Syslog Configuration

Resolved an issue when trying to delete one of the syslog configurations from the notifications page post adding an entry for SSL protocol. This issue has been addressed.

CS-9760: UI - Notification Checkbox Selecting Two Fields at Once

Resolved a bug that automatically selected both "Data exfil SQL" and "Data exfiltration towards internet" when only one detection was selected for Email Alert Notifications. This issue has been resolved.

CS-9731: Issues Editing the LDAP Profile Used for External Authentication

Resolved an issue when creating/editing LDAP profiles. The issues involved the use of special characters in the password of the profile. This problem has been resolved.

Appendix:

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

No, a reboot is not required as part of the 9.1 update.