Cognito® Platform Software Update

In February 2022, the Vectra® X-series appliances, B-series appliances, S-series sensors, Cloud Brain, and Cloud Sensors, will be updated to Cognito® software release Version 6.16.

The Version 6.16 release introduces Host and Account Scoring Improvements, FIPS mode support, new AD Coverage Metrics, and the ability to pull the Brain Registration Token via API.

Cognito® platform enhancements and bug fixes are also included in this release

Release Schedule

Starting with the 6.16 release, we are introducing a new process to deploy Cognito Detect for Network releases. Instead of releasing 6.16 to all customers at once, we will be rolling the release out based upon connectivity status in the following Sequence:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on 3/3/22. 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 3/7/22. 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 3/10/22.
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Host and Account Scoring Improvements — Cognito Detect Products

Improvements have been made to how Vectra maps detections to scoring and quadrant positioning of the respective Hosts and Accounts. This applies to Cognito Detect for Network, Cognito Detect for O365 and Cognito Detect for AWS and applies whether you consume those products via on-premises or SaaS delivery.

These changes are based on research by Vectra Security Research into recent attack campaigns and result in more effective prioritization of threats to the high and critical severity quadrants. These changes to scoring do not require any user action.

Note that a small number of hosts and accounts with detections prior to this update will receive new Account and Host threat and certainty scores. In cases where those scores increase past alerting thresholds, new alerts may trigger shortly after the update.

FIPS Mode Support — Cognito Detect for Network

In 6.16, the Cognito platform support FIPS mode for the Brain and Sensor. By default, FIPS mode is not enabled, but can be enabled by issuing the "set security-mode fips" on the Brain command line interface (SSH or Console) to enable FIPS mode. After a reboot, the Brain will be in FIPS mode, and will restart the connected Sensors to put them in FIPS mode as well. This can be disabled via the "set security-mode default" which will also trigger reboots to restore the platform to non-FIPS mode.

Windows Active Directory Coverage Metrics — Cognito Detect for Network

Starting in 6.16, Vectra will provide additional metrics on Active Directory deployments to provide the user with additional context on how many total accounts Cognito can observe based upon the AD Credential and Base DN provided, along with the total number of accounts observed on the network via Kerberos. This information is available under Settings -> External Connectors -> Active Directory and Lockdown. These metrics will be visible if the Active Directory integration has been configured.

Registration Token API Support

Cognito Detect for Network

A new endpoint is available in the Vectra API to provide the Registration Token via API for large scale deployment automation. This is available via the https://<headend_ip>/api/v2.2/sensor_token endpoint

Notices and EOL Announcements

Connection to New External Vectra Endpoint

Cognito Detect for O365

On February 1st, 2022 on-premises systems with Detect for O365 sensors must be able to connect externally to a new Vectra-managed endpoint to continue to receive Detect for O365 detection alerts to their system.

We ask that customers ensure their firewalls are configured to allow for their Vectra system to connect outbound to the Vectra endpoint in the region of the deployed O365 sensor. This additional endpoint is being added to ensure increased platform stability and enable continued feature development for the Detect for O365 product. To test ensure a successful roll-out of this functionality systems may attempt to contact the new endpoint to ensure there is connectivity before February.

Region	Vectra endpoint
United States	https://authgateway.uw2.public.app.prod.vectra-svc.ai/
European Union	https://authgateway.ew1.public.app.prod.vectra-svc.ai/
Canada	https://authgateway.cc1.public.app.prod.vectra-svc.ai/
Australia	https://authgateway.as2.public.app.prod.vectra-svc.ai/

Bug Fixes

CS-5748: Unable to save Crowdstrike EDR HTTP 500 Error

Fixes issue where an HTTP 500 error appears when invalid Crowdstrike credentials are provided. Now if invalid credentials are provided, an error message will properly reflect this.

CS-5675: Incorrect Host-ID when SentinelOne and Kerberos have conflicting information

Fixes issue where conflicting Host-ID artifacts between SentinelOne and Kerberos could result in incorrect Host-ID applied to a host.

CS-5736: Sensor to Brain Alerting Not Sending Notification

Fixes issue where when the connection between a Brain and Sensor is disrupted for more than 60 minutes, an alert was not sent (if configured.) This has been resolved.

CS-5776: Stage Loader Detection shows same host as Target/Attacker

Fixes issue where the same host is listed as the Target and the Attacker for the Stage Loader Detection.

CS-5731: Duplicate Host / IP with the same name

Fixes issue where duplicate Host-ID entries are created in some scenarios. This has been addressed.