Cognito® Platform Software Update

In July 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.9.

The Version 6.9 release introduces the renaming of the Executive Report to Asset Inventory Report, new identification for Cognito Recall, and improvements to StreamPlus. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

Executive Report renamed to Asset Inventory Report   Cognito Detect for Network

Release 6.9 renames the Executive Report to Asset Inventory Report. This change was to better reflect what the report covers. The actual content of the report remains unchanged as does the way to generate the report.

Added SNMP, Syslog, and FTP as Traffic Types in Recall   Cognito Recall

Previously SNMP, Syslog, and FTP would not be named as traffic types within the ISession stream of data. Now, port-based identification of SNMP and Syslog and port-based and traffic inspection identification of FTP protocols can be used as search filters in Recall to see if the traffic is on your network, and identify which machines are involved.

Minimizer for StreamPlus   Cognito StreamPlus

In 6.9 we have added an internal option to tokenize/minimize the syslog output that will be consumed by StreamPlus eliminating the need of a separate device to do the tokenization/minimization. This process will replace field names with shorter ones in the output streams and reduce the amount of data ingested/indexed.

Bug Fixes

CS-4904: Recall health failure queue being too long.

Fixes issue where the max limit was small for Recall health failure queue.

CS-4947: Large numbers of triage filters cause very slow UI.

Fixes issue where a large amount of triage filters causes the UI to be slow.

CS-4862: Microsoft Defender ATP connector UI breaks when remote end is not reachable.

Fixes issue where the Microsoft Defender ATP connector would break in the UI when the remote end was not reachable.