



## Qualys Cloud Suite 2.16

We're excited to tell you about new features coming with Qualys Cloud Suite 2.16.



We've added these features to AssetView and ThreatPROTECT

- Easily Refresh Dashboard in One Go
- Customize Display of your Dashboard Widgets
- Support for DNS hostnames in Asset Group Tags
- Configure Number of Threats in Your Live Feed Widget



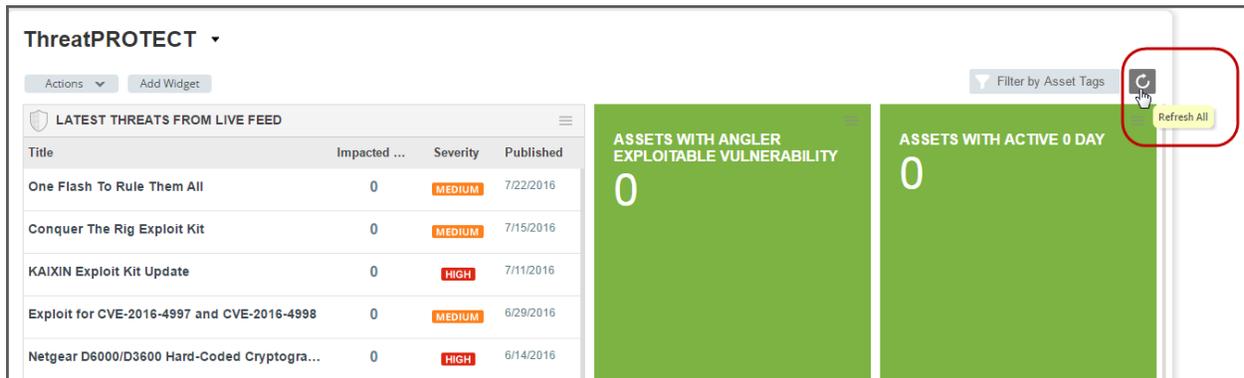
We've added this feature to Cloud Agent

- Bulk Activation of Agents



## Easily Refresh Dashboard in One Go

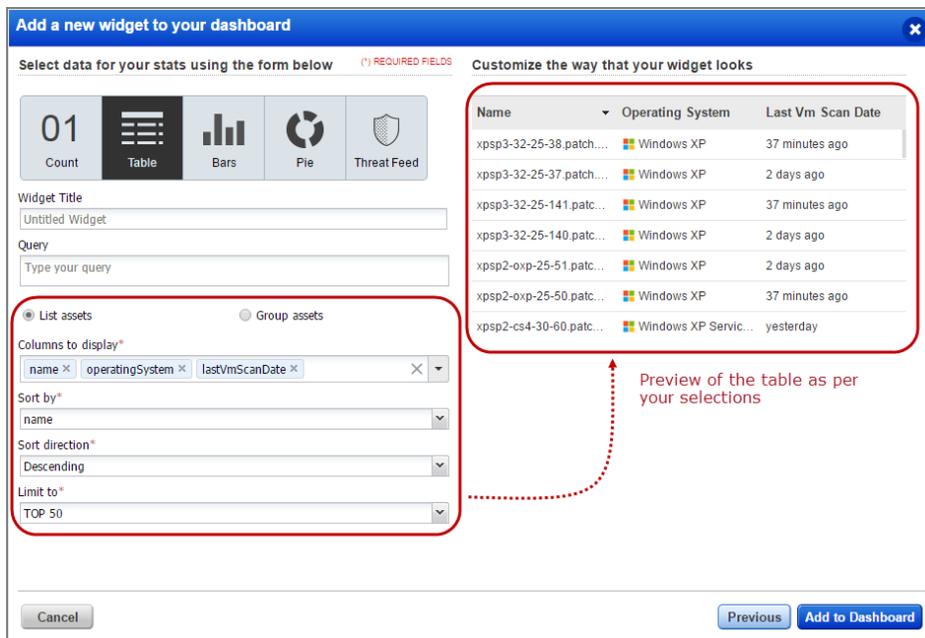
Now you can quickly refresh all the widgets displayed in the dashboard with the click of a single button. Just hit Refresh All on the Dashboard and all your widgets will be refreshed.



## Customize Display of your Dashboard Widgets

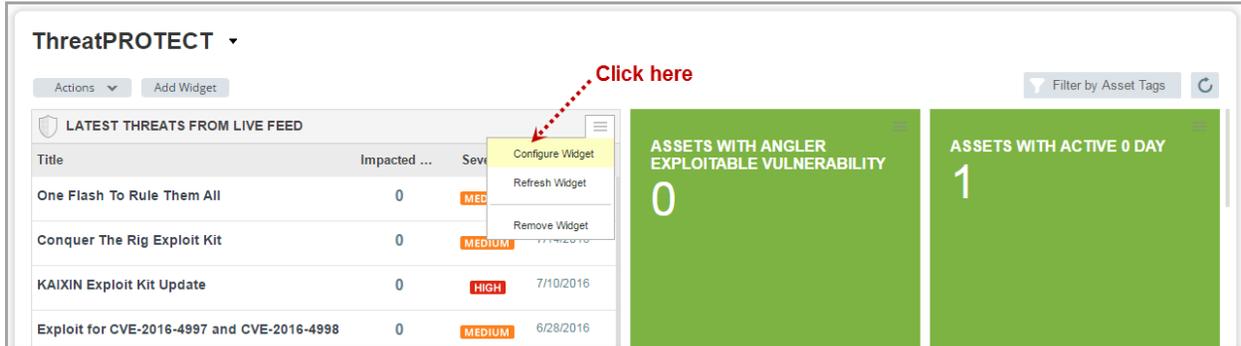
You now have multiple ways to configure a table in widget to help you visualize assets in your environment and their security. Create tables with multiple columns, sort by any column you like and set the sort order (ascending or descending).

On the Dashboard, simply go to Add Widget > Custom table. Here customize the table as per your liking and click Add to Dashboard.



## Configure Number of Threats in Your Live Feed Widget

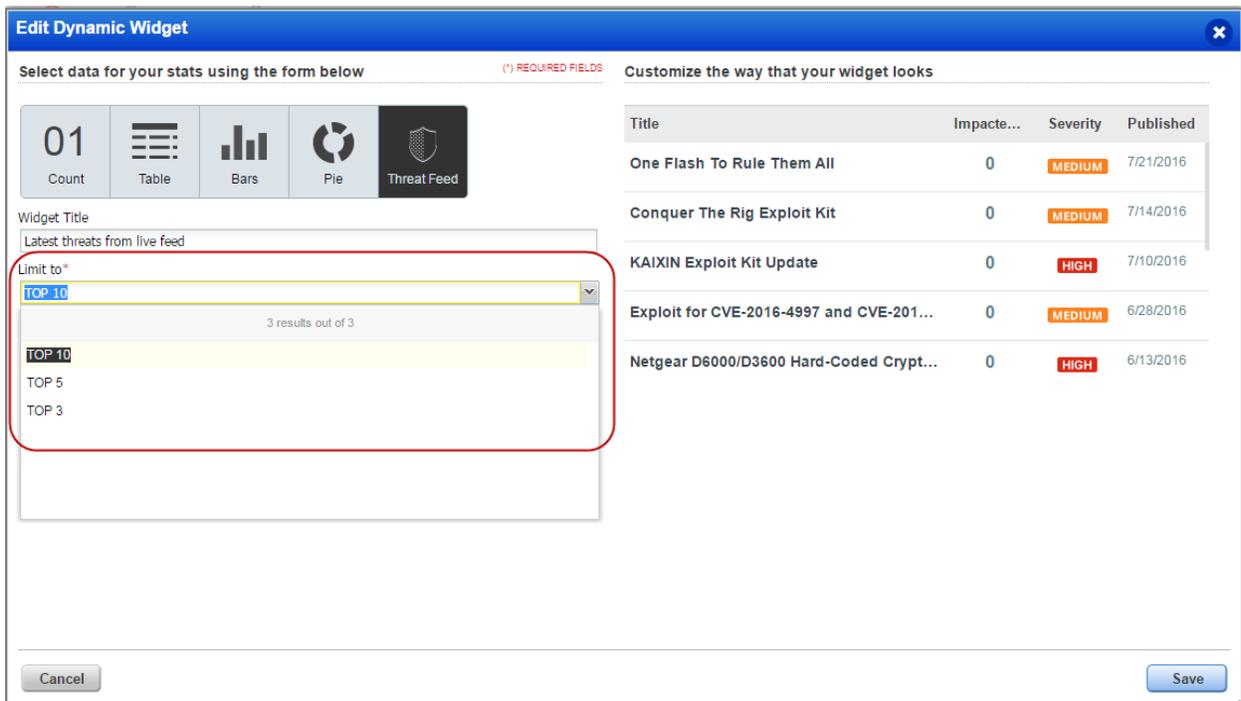
You can easily configure the number of threats shown on your ThreatPROTECT dashboard in the Latest Threats widget.



The screenshot shows the ThreatPROTECT dashboard. On the left, there is a table titled "LATEST THREATS FROM LIVE FEED". The table has columns for Title, Impacted, Severity, and Published. The table contains four rows of threat information. To the right of the table are two green summary cards: "ASSETS WITH ANGLER EXPLOITABLE VULNERABILITY" showing 0, and "ASSETS WITH ACTIVE 0 DAY" showing 1. A red arrow points to the "Configure Widget" button in the menu of the "LATEST THREATS FROM LIVE FEED" widget.

Title	Impacted ...	Seve	Published
One Flash To Rule Them All	0	MED	
Conquer The Rig Exploit Kit	0	MEDIUM	
KAIXIN Exploit Kit Update	0	HIGH	7/10/2016
Exploit for CVE-2016-4997 and CVE-2016-4998	0	MEDIUM	6/28/2016

The new **Limit to** option lets you set the number of threats to display - choose Top 10, Top 5 or Top 3. That's it!



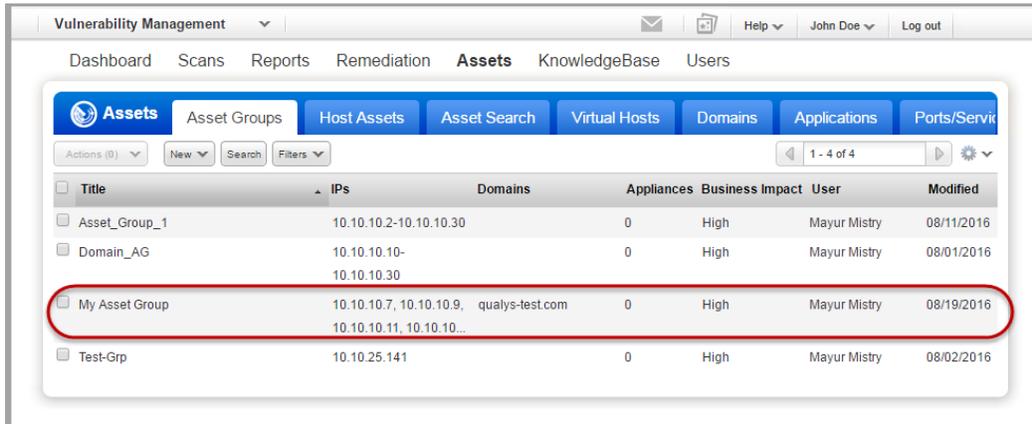
The screenshot shows the "Edit Dynamic Widget" dialog box. On the left, there are icons for different widget types: Count, Table, Bars, Pie, and Threat Feed. The "Threat Feed" icon is selected. Below the icons, the "Widget Title" is "Latest threats from live feed". The "Limit to" dropdown menu is open, showing options for TOP 10, TOP 5, and TOP 3. The "Limit to" field is highlighted with a red box. On the right, there is a table titled "Customize the way that your widget looks" with columns for Title, Impacte..., Severity, and Published. The table contains five rows of threat information. At the bottom of the dialog box, there are "Cancel" and "Save" buttons.

Title	Impacte...	Severity	Published
One Flash To Rule Them All	0	MEDIUM	7/21/2016
Conquer The Rig Exploit Kit	0	MEDIUM	7/14/2016
KAIXIN Exploit Kit Update	0	HIGH	7/10/2016
Exploit for CVE-2016-4997 and CVE-201...	0	MEDIUM	6/28/2016
Netgear D6000/D3600 Hard-Coded Crypt...	0	HIGH	6/13/2016

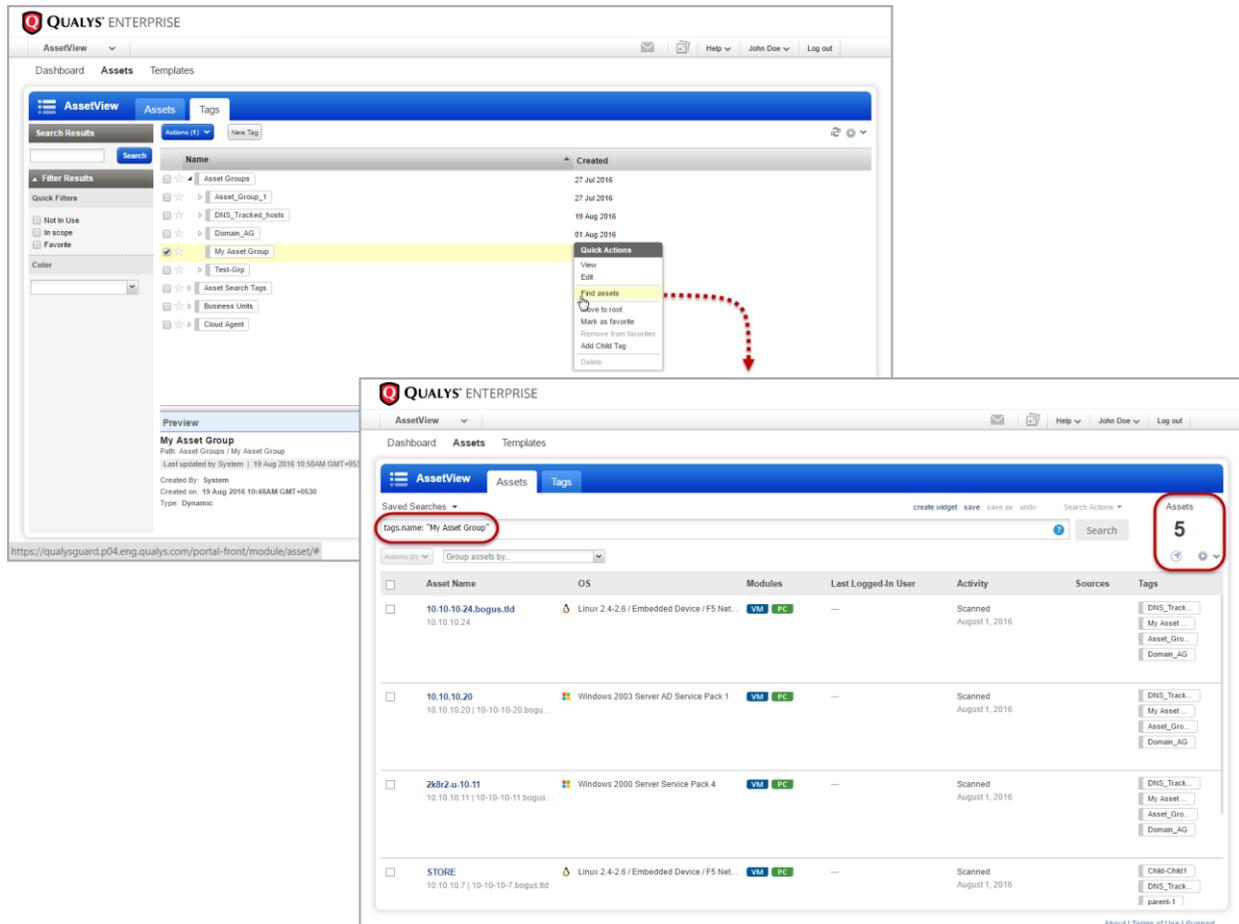
## Support for DNS hostnames in Asset Group Tags

In this release, the DNS hostnames in new asset groups will be assigned asset group tags. You'll see these DNS hostnames tagged with their asset group tag in the AssetView (AV) module.

For example, if you add DNS hostname qualys-test.com to My Asset Group (asset group) in the Vulnerability Management (VM) module, then qualys-test.com will be assigned the tag My Asset Group.



The AssetView (AV) module displays the My Asset Group tag with the DNS host assets.





## Bulk Activation of Cloud Agents

We now provide a new option to activate all the cloud agents listed in the search result or all cloud agents in your account. For example, search for cloud agents that are not activated on any of the modules and click Activate Multiple Agents.

The screenshot shows the Qualys Enterprise Agent Management interface. At the top, there's a navigation bar with 'Cloud Agent' selected. Below it, the 'Agent Management' section is active, with sub-tabs for 'Agents', 'Activation Keys', and 'Configuration Profiles'. The 'Agents' tab is selected, and the search criteria are set to 'Activated For: PC'. The 'Agent Overview' section shows 'Total Agents: 4' and a breakdown of 'VM Agents: 3/1,000' and 'PC Agents: 3/1,000'. A donut chart displays the 'Top 4 Operating Systems': Ubuntu Linux 14.04.1 (1), Mac OS X 10.11.2 (1), Microsoft Windows 7 Professional 6.1.7601 Ser... (1), and Debian Linux 8.4 (1). The 'Actions' menu includes 'Install New Agent' and 'Activate Multiple Agents', which is circled in red. A table below lists three agents: 'qualys-virtual-machine', 'AmoIC-Mac', and 'deb8-4-0'. Each agent has checkboxes for 'VM' and 'PC' modules, which are also circled in red. A red arrow points from the text 'Specify the Cloud Agent search criteria' to the search filter, and another red arrow points from 'Click to activate all Cloud Agents in the search result' to the 'Activate Multiple Agents' button.

Select the module(s) you want to activate, and click Activate. All the agents listed in the search result will get activated.

The screenshot shows the 'Activate Multiple Agents (100)' dialog box. It has a title bar with a close button. The main content area contains the following text: 'Bulk Activate 100 cloud agents for the modules selected below.' and 'The cloud agent platform will start to continuously perform host assessments and report security threats using these agents. A license, if available, will be consumed for each agent activated.' Below this, there are two sections for module selection: 'VM Vulnerability Management' and 'PC Policy Compliance'. Each section has a green checkmark and a '100' in a box, indicating that all agents meeting the search criteria will be activated for that module. Below each section, it says '901 available of 1001 total licenses'. At the bottom of the dialog, there are 'Cancel' and 'Activate' buttons, with the 'Activate' button circled in red.