Building an Always Up-to-Date, Real-Time View of Your Global IT Assets in the Hybrid IT Environment

Chris Carlson
VP, Product Management, Qualys, Inc.
Starting Point...

Knowing what’s on your Global Hybrid IT environment is fundamental to security.
Not an Easy Problem to Solve

CISO: How many windows hosts do we have?
AV Guy: 7864
Desktop Management: 6321
EDR Team: 6722
CMDB Team: 4848
SIEM Team: 9342
5:55 AM - 8 Feb 2018

494 Retweets 920 Likes
Asset Inventory Catalog

Software Models
420K+

IBM 58,949
HP 24,707
CA 21,510
Oracle 42,543
SAP 8,917
Microsoft 14,466
Symantec 17,072
Adobe 9,555
BMC 17,912

Hardware Models
140K+

Lenovo Group 224,731
IBM 129,254
HP 86,538
Sony 5,485
Panasonic 2,307
Toshiba 6,279
ASUSTeK 3,291
Dell 2,537
Gateway 1,236
Acer 2,362
<table>
<thead>
<tr>
<th>Hardware</th>
<th>Operating System</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Data</td>
<td>Dell R510</td>
<td>Base OS Runtime AIX: 06.01.0009.0300 EE</td>
</tr>
<tr>
<td>QID</td>
<td>Title</td>
<td>CVE IDs</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>91470</td>
<td>Microsoft Windows FragmentSmack Denial of Service Vul...</td>
<td>CVE-2018-5391</td>
</tr>
<tr>
<td>100131</td>
<td>Microsoft Internet Explorer Mouse Tracking Events Design ...</td>
<td></td>
</tr>
</tbody>
</table>

The search query highlighted is: `Asset ▼ X operatingSystem.category:Server and software:(category:Database)`. This query is searching for vulnerabilities associated with servers and software categories in the database.
Auto-Tagging using Catalog Attributes

Asset Inventory catalog attributes are extended to the tagging rule engine

Auto-Tagging rules uses QQL syntax (no groovy!)

Use catalog auto-tags to solve the “OR” reporting problem
Eliminate Asset Blind Spots for your Security Program

Passive Sensor (included in VMDR) discovers assets in real time and provides context of how these devices communicate.

Immediate visibility of unknown unmanaged devices between VM scan windows.

VMDR adds new workflows:
- auto-tag unmanaged assets
- activate for VM scanning
- trigger 3rd party install of Cloud Agent

Eliminate Asset Blind Spots for your Security Program.
Introducing Cloud Agent for Android and Apple iOS mobile devices included in VMDR.
DEMO

Asset Inventory

Software Normalization + Catalog
VM Dashboard and Searching
Enhance VMDR with additional Asset Inventory add-on capabilities
Hardware and Software Lifecycle (EOL/EOS)

Current and Future EOL and EOS

Make remediation decisions based on current and future EOL status

Sunset vs. Patching
Asset Inventory
CMDB Sync

Use Qualys VMDR sensors for asset discovery (scanner, agent, cloud, container, mobile device, more)

Continuous sync for enriched asset data into ServiceNow CMDB (certified for 3 last releases)

Assets are automatically mapped to Configuration Item (CI) Classes
New: Software Usage for Patching... or Uninstall

<table>
<thead>
<tr>
<th>Application</th>
<th>Category</th>
<th>License Category</th>
<th>Edition</th>
<th>Update</th>
<th>Release</th>
<th>Installed On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox</td>
<td>Storage / Backup and Restore</td>
<td>Commercial</td>
<td>-</td>
<td>84.4.170</td>
<td>3.1.0.101</td>
<td>-</td>
</tr>
</tbody>
</table>

- **Last Use Date:** Nov 10, 2019
- **Lifecycle Stage:** EOL (Extended Support)
  - **GA:** Oct 30, 2019
  - **EOL (Estimated):** Nov 14, 2019
  - **EOS (Estimated):** Nov 14, 2019

- Other software included in the list:
  - Internet Explorer
  - Adobe Reader
  - Microsoft Office 365
  - Windows Defender File Protection
  - Internet Explorer 11.0.14393.2007
  - Adobe Reader 84.4.170
  - Microsoft Office 365 1.2.3
  - Windows Defender File Protection 4.10.14393.2999
  - Internet Explorer 8.110.14393.2906
  - Adobe Reader 5.6.7
  - Microsoft Office 365 8.110.14393.2906
  - Windows Defender File Protection 4.10.14393.2999
Summary and Take-Aways

Great Security Programs start with Great Asset Inventory

Use the included Qualys VMDR sensors for asset discovery across all asset types for your hybrid IT environment

Always up-to-date normalized view with catalog attributes gives asset context to VM programs

Enhance VMDR with additional Asset Inventory capabilities: EOL/EOS Lifecycle, CMDB Sync, Software Usage
Thank You

Chris Carlson
ccarlson@qualys.com