Cloud Agent Platform

Chris Carlson
VP, Product Management, Qualys, Inc.
Digital Transformation is Driving IT Transformation for Organizations
... But creates new Challenges for Security

Don’t know how many assets you have

Don’t know when those assets are running

Credential issues / Authentication failures

Monthly / weekly scanning too slow [WannaCry]

Can’t scan remote users
Qualys Sensors
Scalable, self-updating & centrally managed

Physical
- Legacy data centers
- Corporate infrastructure
- Continuous security and compliance scanning

Virtual
- Private cloud infrastructure
- Virtualized Infrastructure
- Continuous security and compliance scanning

Cloud/Container
- Commercial IaaS & PaaS clouds
- Pre-certified in market place
- Fully automated with API orchestration
- Continuous security and compliance scanning

Cloud Agents
- Light weight, multi-platform
- On premise, elastic cloud & endpoints
- Real-time data collection
- Continuous evaluation on platform for security and compliance

Passive
- Passively sniff on network
- Real-time device discovery & identification
- Identification of APT network traffic
- Extract malware files from network for analysis

API
- Integration with Threat Intel feeds
- CMDB Integration
- Log connectors
Qualys Cloud Agent Platform

Lightweight Software Agent
(collects metadata only)

On-Premise Servers
Public Cloud
User Endpoints

Windows
Linux
Mac
AIX
Cloud Native

Delivers Multiple Security Functions in one Agent
Qualys Platform

Cloud Agent

<table>
<thead>
<tr>
<th>Central Management / API</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Qualys Suite of Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Efficient Network Usage (Delta Processing average)</th>
<th>50 - 350 KB / day</th>
</tr>
</thead>
</table>

| Lightweight Metadata Collection (tunable) | ~1-2% CPU |

| Windows, Linux, Mac, AIX | 3 MB application |

6
Qualys Cloud Agent

IT, Security, Compliance Apps

- Asset Inventory
- Vulnerability Management
- Policy Compliance
- Indication of Compromise Detection
- File Integrity Monitoring

Upcoming IT App  (Beta November 2018)

- Patch Management
Try and Manage Apps on One Cloud Agent

End the fight with IT to deploy security agents!

Remove point-solution agents from your endpoints

Consolidate security tools
Cloud Agent Extends Network Scanning

No scan windows needed – always collecting

Find vulnerabilities faster

Detect a fixed vulnerability faster

Many new Apps only available on Agent

Best for assets that can’t be scanned

Unable to get credentials / authentication failures

Remote systems in branch offices / NAT

Roaming user endpoints

Cloud / Elastic deployments
Cloud Agent Adoption

(Unit in millions)

Number of Cloud Agents Sold

- LTM Q4 2017: 6.0
- LTM Q1 2018: 7.3
- LTM Q2 2018: 8.1
- LTM Q3 2018: 13.9

(LTM = Last Twelve Months)
# Cloud Agent VM Usage and Growth Drivers

<table>
<thead>
<tr>
<th>Year</th>
<th>Events</th>
</tr>
</thead>
</table>
| 2016 | Deploy on servers to overcome customer limitations with their network scanning  
- Auth issues  
- Scan windows  
- More frequent VM assessments |
| 2017 | - Servers increasing  
- Initial end-users (WannaCry)  
- Early Cloud - AWS and Azure  
- Add Policy Compliance |
| 2018 | - Growth in endpoint deployments (50-300K)  
- Growth in public cloud  
- DevSecOps – Build CA into CI/CD/DevOps  
- Add Policy Compliance  
- Add FIM  
- Add IOC |
| 2019 | - Visibility - Asset Inventory  
- Increase endpoints  
- Increase in public cloud  
- Migration from on-premise servers to public cloud  
- Multiple Qualys Apps  
- Add Patch Management |
Cloud Agent CPU Tuning - Linux

VM: < 1.2% CPU peak usage for less than 15 mins

AWS EC2 not allowed to scan nano, micro, or small instances using network scanning

0.5% CPU when idle / heartbeat

AWS t2.micro instance running Cloud Agent
Cloud Agent CPU Tuning - Windows

Tunable CPU Limit
Example: 8% configured max on 1-core
(Effective: <2% on 4-core)
Cloud Native – Collect Provider Metadata

<table>
<thead>
<tr>
<th>AWS EC2</th>
<th>Microsoft Azure</th>
<th>Google Compute Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountld</td>
<td>dnsservers</td>
<td>hostname</td>
</tr>
<tr>
<td>amiId</td>
<td>ipv6</td>
<td>instanceId</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>location</td>
<td>macAddress</td>
</tr>
<tr>
<td>hostname</td>
<td>macAddress</td>
<td>name</td>
</tr>
<tr>
<td>hostnamePublic</td>
<td>name</td>
<td>offer</td>
</tr>
<tr>
<td>instanceId</td>
<td>osType</td>
<td>publisher</td>
</tr>
<tr>
<td>kernelId</td>
<td>privateIpAddress</td>
<td>resourceGroupName</td>
</tr>
<tr>
<td>macAddress</td>
<td>publicIpAddress</td>
<td>tags</td>
</tr>
<tr>
<td>privateIpAddress</td>
<td>publisher</td>
<td>subnet</td>
</tr>
<tr>
<td>publicIpAddress</td>
<td>resourceGroupName</td>
<td>subscriptionId</td>
</tr>
<tr>
<td>region</td>
<td>securityGroupIds</td>
<td>version</td>
</tr>
<tr>
<td>reservationId</td>
<td>securityGroups</td>
<td>vmId</td>
</tr>
<tr>
<td>securityGroupIds</td>
<td>subnet</td>
<td>vmSize</td>
</tr>
<tr>
<td>securityGroups</td>
<td>tags</td>
<td></td>
</tr>
<tr>
<td>subnetId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPCId</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agent collects metadata locally
Cloud Provider Metadata (AWS EC2 example)

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountId</td>
<td>383031258652</td>
</tr>
<tr>
<td>ami-id</td>
<td>ami-d874e0a0</td>
</tr>
<tr>
<td>ami-launch-index</td>
<td>2</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>us-west-2a</td>
</tr>
<tr>
<td>hostname</td>
<td>ip-172-31-36-214.us-west-2.compute.internal</td>
</tr>
<tr>
<td>imageId</td>
<td>ami-d874e0a0</td>
</tr>
<tr>
<td>instance-id</td>
<td>i-03e86d77745bb2bba</td>
</tr>
<tr>
<td>instanceType</td>
<td>t2.micro</td>
</tr>
<tr>
<td>local-hostname</td>
<td>ip-172-31-36-214.us-west-2.compute.internal</td>
</tr>
<tr>
<td>local-ipv4</td>
<td>172.31.36.214</td>
</tr>
<tr>
<td>mac</td>
<td>06:26:0c:74:c5:9a</td>
</tr>
<tr>
<td>privateIp</td>
<td>172.31.36.214</td>
</tr>
<tr>
<td>profile</td>
<td>default-hvm</td>
</tr>
<tr>
<td>public-hostname</td>
<td>ec2-18-236-81-63.us-west-2.compute.amazonaws.com</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>18.236.81.63</td>
</tr>
<tr>
<td>region</td>
<td>us-west-2</td>
</tr>
<tr>
<td>reservation-id</td>
<td>r-06e5580c2918a00ba</td>
</tr>
<tr>
<td>security-groups</td>
<td>launch-wizard-2</td>
</tr>
</tbody>
</table>
Cloud Instance Metadata Merge and Agent Dynamic License Management

**EC2 Connector – Available now**

- `aws.ec2.accountId`
- `aws.ec2.availabilityZone`
- `aws.ec2.hostname`
- `aws.ec2.hostnamePublic`
- `aws.ec2.imageld`
- `aws.ec2.instanceId`
- `aws.ec2.instanceState`
- `aws.ec2.instanceType`
- `aws.ec2.kernelId`
- `aws.ec2.privateDNS`
- `aws.ec2.privateIPAddress`
- `aws.ec2.publicDNS`
- `aws.ec2.publicIPAddress`
- `aws.ec2.region.code`
- `aws.ec2.region.name`
- `aws.ec2.spotInstance`
- `aws.ec2.subnetId`
- `aws.ec2.VPCId`

**Cloud Agent – Available now**

- `aws.ec2.accountId`
- `aws.ec2.availabilityZone`
- `aws.ec2.hostname`
- `aws.ec2.imageld`
- `aws.ec2.instanceId`
- `aws.ec2.instanceState`
- `aws.ec2.instanceType`
- `aws.ec2.kernelId`
- `aws.ec2.privateDNS`
- `aws.ec2.privateIPAddress`
- `aws.ec2.publicDNS`
- `aws.ec2.publicIPAddress`
- `aws.ec2.region.code`
- `aws.ec2.region.name`
- `aws.ec2.spotInstance`
- `aws.ec2.subnetId`
- `aws.ec2.VPCId`

**Automatically merge on Instance ID (Nov 2018)**

**Automated Rules (Dec 2018)**

“When `instanceState` = TERMINATED, then remove Cloud Agent license”
Integrate Cloud Agent into DevOps

**Use Cases for DevOps**

- Build Cloud Agent into gold image or auto-deploy with CI/CD - self-service results from Qualys API/UI & integrations
- Get vulnerability and configuration posture of OS and application along the DevOps pipeline
- Fix/verify security issues before going into production

**Use Cases for Security**

- End-to-end lifecycle tracking - development, deployment, production, decommission
- Same Cloud Agent across cloud, on-premise, endpoint, hybrid
- Single platform as DevOps tools evolve - Qualys Container Security, Jenkins integration, API automation, more
Cloud Agent – Microsoft Azure Integration
**RESOURCE GROUP**
HS_RESOURCEGROUP

**SUBSCRIPTION**
Visual Studio Premium with MSDN

**VIRTUAL IP**

**OPERATING SYSTEM**
Windows

**VERSION**
Compute

**STATUS**
Deallocated

**MONITORING STATE**
Monitored by Azure Security Center

**PREVENTION STATUS**
High severity

**Security Solutions**

**SYSTEM UPDATES**
Microsoft (Last scan time - 10/3/2016 1:22 PM)

**OS VULNERABILITIES**
Microsoft (Last scan time - 10/3/2016 1:22 PM)

**VULNERABILITY SCANNER - PREVIEW**
Qualys (Last scan time - 10/3/2016 11:56 PM)

**Recommendations**

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>RESOURCE</th>
<th>STATE</th>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Endpoint Protection</td>
<td>harivm2</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Remediate vulnerabilities (by Qualys)</td>
<td>harivm2</td>
<td>Open</td>
<td>High</td>
</tr>
</tbody>
</table>

**Vulnerability Table**

<table>
<thead>
<tr>
<th>VULNERABILITY NAME</th>
<th>VENDOR</th>
<th>AFFECT...</th>
<th>STATE</th>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled DCOM</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Allowed Null Session</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Enabled Cached Logon Cred...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Machine Information Disclosure</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Microsoft Windows Explorer Autopla...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Windows Explorer Autopla...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Access to File Share is Enab...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>ActiveX Controls Enumerated</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Antivirus Product Not Dete...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Disabled Clear Page File</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Enabled Caching of Dial-up...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Enabled Display Last Use...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>File Access Permissions for ...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>File Access Permissions for ...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Host Scan Time</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Hyper-V Host Information ...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Installed Applications Enu...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Internet Protocol version 6 ...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>IPSEC Policy Agent Service ...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Message For Users Attempt...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>VULNERABILITY NAME</td>
<td>VENDOR</td>
<td>AFFECT...</td>
<td>STATE</td>
<td>SEVERITY</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------</td>
<td>-----------</td>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Enabled DCOM</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Allowed Null Session</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Enabled Cached Logon Credential</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Machine Information Disclosure</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Microsoft Windows Explorer</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Windows Explorer Autoplay</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Access to File Share is Enabled</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>ActiveX Controls Enumerated</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Antivirus Product Not Detected</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>Disabled Clear Page File</td>
<td>Qualys</td>
<td>harvim2</td>
<td>Open</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Enabled DCOM**

**High**

The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.

Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.
Vulnerability Spread at Speed of DevOps

Red Hat 7.4 Marketplace Image
Auto-Deploy Qualys Cloud Agent
Vulnerability Results
Threat Protection Exploitability ☹️
Cloud Agent Roadmap

Agent Releases
• Mac 1.7.2 – released Aug 29
• Windows 2.1.1 – released Oct 22
• Linux 2.3 – Dec rollout for Policy Compliance UDCs
• https://www.qualys.com/documentation/release-notes/

Features
• Cloud Provider Metadata (AWS, Azure, GCP) – available
• EC2 Connector / Cloud Agent merge – available
• Nov – Windows agent to support Patch Management Beta
• Dec - Policy Compliance UDCs (Windows / Linux / AIX )
• Dec – Agent Lifecycle Management
  (Public cloud State-based w/ Connector / Any asset using Time-based)
Thank You

Chris Carlson
ccarlson@qualys.com
Qualys Indication of Compromise

Bringing IOC to the Next Level

Chris Carlson
VP, Product Management, Qualys, Inc.
Adversary TTPs are Changing

Early 2010s
Zero-day Vulnerabilities
(Nation State, Industrial Espionage, Black Market)

Today
Rapidly weaponizing newly-disclosed vulnerabilities
(Good, Fast, Cheap - Pick 3)
Known Critical Vulnerabilities are Increasing

6-7K vulnerabilities are disclosed each year*

30-40% are ranked as “High” or “Critical” severity

“Mean Time to Weaponize” (MTTW) is rapidly decreasing year-over-year
Announcing: CVE-2018-12238

Multiple Symantec Products CVE-2018-12238 Local Security Bypass Vulnerability

Bugtraq ID: 105917
CVE: CVE-2018-12238
Remote: No    Local: Yes
Published: Nov 28 2018 12:00AM
Credit: Qualys Malware Research Lab

Vulnerable:
Symantec Norton AntiVirus 22.7
Symantec Norton AntiVirus 21.0
Symantec Norton AntiVirus 17.6.0.32
Symantec Endpoint Protection Cloud 12.1.6
Symantec Endpoint Protection Cloud 14
Symantec Endpoint Protection 12.1.6 MP4
Symantec Endpoint Protection 12.1.6
+ 95 other products
Vulnerability Management Lifecycle

- Asset Inventory
- Patch Management
- Vulnerability Management
- Threat Risk and Prioritization
- Report & Research
- Remediate / Patch
- Discover at Scale
Get Proactive – Reduce the Attack Surface

Immediately Identify Vulnerabilities in Production
Notify IT Asset Owner to Patch/Stop the Instance
Control Network Access / Cloud Security Groups
Change Configuration to Limit Access (Compliance)

Add Detection and Response – Endpoint & Network
Proactively Hunt, Detect, and Respond

Indication of Compromise
Detect IOCs, IOAs, and verify Threat Intel

Passive Network Sensor
What new devices are on the network? Are there new/different traffic patterns?

Monitor the Network
Monitor System Indicators
Organizations Struggle to Answer Basic Questions

Are these hashes on/running in my network?
Are these mutexes / processes / registry keys?

Did any endpoints connect to these IPs / Domains?
Are there any connections to TOR exit nodes?

What system is the first impacted? “Patient Zero”
Did this spread to others systems? When?
Qualys IOC Use Cases –
Visibility Beyond Anti-Virus

**Threat Intel Verification**
Threat Intel Feeds / Mandated to Verify
"Is this hash, registry, process, mutex on my network?"

**“Look Back” Investigation after a known breach**
Go back over months of stored events and find the first occurrence of a breach

**Hunting / Find Suspicious Activity**
Indicator of Activity hunting with pre-built and user-defined queries for Fileless attacks

**Detect Known/Unknown Malware Family Variants**
Using Qualys Malware Labs behavior models and Threat Feeds (OEM, customer)
Threat Intel Verification

1. Threat Intelligence lists attack information ...

2. Search for the file hash here...

3. Find the object there.
Malware Hides with Stolen Code-Signing Certificates

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign

IOC 2.0 Release (Dec 2018)

Responses - Alerting and Actions
Send alerts via Email, Slack, PagerDuty for any Hunting (QQL) searches

UI Updates
Event Relationship Tree / Trending Widgets / Event Group By Asset

Threat Feed (find malware that legacy AV may have missed)
Known Bad – 1B hashes
CVE-to-Malware hashes (shared with Threat Protection)

New Scoring Model
Prioritization for Investigation and Response (confirmed vs. suspicious)
Integration with Alerting / Actions

IOC API
Integrate with any 3rd party SIEM / TIP
Splunk TA + Dashboards – Jan 2019
New IOC CVE - File Reputation Threat Feed

Find Vulnerabilities
Verify that vulnerabilities have been remediated

Real-Time Indicators for which vulnerabilities have known / POC exploits
Prioritize vulnerability remediation on likelihood of attack

Threat Feed of malware hashes used in real-world vulnerability exploits
Prioritize vulnerability remediation based on successful attacks in your network
Indication of Compromise

Threat Intel Verification
Hunting
Alerting
Create Emergency Patch Job from CVE Exploitation

18fc1b9b29a2d281ec9310f9f226ad77e3cb9c558f696c37390bbac72baa8ba8
168.63.129.16
Thank You

Chris Carlson
ccarlson@qualys.com