Cloud Agent Platform Overview

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 Built-in Security Functions in one Agent
Qualys Cloud Agent

IT, Security, and Compliance Apps

Delivered by a single agent

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

Cloud Agent

Central Management / API

Qualys Suite of Applications

Efficient Network Usage
*Delta Processing average*

6 – 50 KB / day

Lightweight Metadata Collection *(tunable)*

~1-2% CPU

Windows, Linux, Mac, AIX

3 MB application
Deploy and Manage Apps on One Cloud Agent

End the fight with IT to deploy security agents!

Enabling an application does not require redeployment or reboot of the system

Self-updating, version control, elastic lifecycle management
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 CPU Tuning - Linux

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

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

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>
<th>IBM Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountId</td>
<td>dnsservers</td>
<td>hostname</td>
<td>Coming June 2019</td>
</tr>
<tr>
<td>amiId</td>
<td>ipv6</td>
<td>instanceId</td>
<td>datacenterId</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>location</td>
<td>macAddress</td>
<td>deviceName</td>
</tr>
<tr>
<td>hostname</td>
<td>name</td>
<td>offer</td>
<td>publicIp</td>
</tr>
</tbody>
</table>
| hostnamePublic          | offer                      | osType                        | privatelp  
| instanceId              | offer                      | privatelpAddress              | id             |
| instanceType            | offer                      | publicIpAddress               | publicVlan                 |
| kernelId                | offer                      | publisher                     | domain                     |
| macAddress              | offer                      | resourceGroupName             | privateVlan                |
| privatelpAddress        | publisher                  | tags                           |                            |
| publicIpAddress         | publisher                  | subnet                         |                            |
| region                  | publisher                  | subnetId                       |                            |
| reservationId           | publisher                  | subscriptionId                |                            |
| securityGroupId         | publisher                  | version                        |                            |
| securityGroups          | publisher                  | vmId                           |                            |
| subnetId                | publisher                  | vmSize                         |                            |
| VPCId                   | tag                        |                                |                            |

Agent collects metadata locally without Connector
<table>
<thead>
<tr>
<th>Cloud App</th>
<th>Q1 Released</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Management</td>
<td>General Availability</td>
<td></td>
<td>Linux</td>
<td>Mac</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td></td>
<td></td>
<td>Middleware Auto-Discovery</td>
</tr>
<tr>
<td>Policy Compliance</td>
<td>User Defined Controls</td>
<td>Middleware Auto-Discovery</td>
<td>Remediation</td>
<td></td>
</tr>
<tr>
<td>Indication of Compromise</td>
<td>Threat Feed Alerts/Actions</td>
<td>Linux</td>
<td></td>
<td>Mac Network IOCs</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td></td>
<td>Detect Unmanaged Assets on the Network</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Roadmap schedule subject to change
Announcing

Cloud Agent Gateway

Available Now on Shared Platforms
Cloud Agent Deployment Questions

<table>
<thead>
<tr>
<th>#1</th>
<th>I am not able to run Cloud Agent on assets that <strong>do not have direct access to the Internet</strong> due to security policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>#2</td>
<td>I am (A) not able to use existing proxies deployed by IT or (B) are not able to buy/manage an open-source or full-fledged commercial proxy</td>
</tr>
<tr>
<td>#3</td>
<td>I wish to <strong>optimize the bandwidth</strong> utilized by large Cloud Agents deployments and Patch Management</td>
</tr>
</tbody>
</table>
Qualys Cloud Agent Gateway (CAG)

A Qualys-developed HTTP proxy/cache running on a new virtual appliance platform

- Separate appliance from the Virtual Scanner

CAG appliances are downloaded and managed from Qualys Platform UI

Cloud Agents use existing agent proxy capabilities to connect through CAG to connect to the Qualys platform
How it works

Qualys Platform:
CAG virtual appliance is downloaded from UI by customer, run locally, and registers appliance.

Cloud Agent Gateway (CAG):
Virtual appliance with Docker containers providing HTTPS Proxying, Caching, Load Balancing, High-Availability, and Logging.

Cloud Agent:
Agents use existing HTTPS Proxy features to connect to CAG
(if no proxy, fail over to direct connection)
CAG Deployment

Customer Remote Network

Customer Data Center

Restricted Access Network

Direct Connection Network

Shared Platform

Proxy

Internet
Expanded CAG Use Cases

Proxy/caching for Patch Management patch downloads

Recommended/Required for on-premises agents
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
(Lesser Nation State, Industrial, Organized Crime)
Good, Fast, Cheap – Pick all 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 y/y
Adversaries are Evading Anti-Virus Detection

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
- Report & Research
- Prioritize Threats
- Remediate / Patch
- Discover at Scale

Vulnerability Management

Threat Risk and Prioritization
Get Proactive – Reduce the Attack Surface

Immediately Identify Vulnerabilities in Production

Notify IT Asset Owner to Patch/Stop the Instance

Change Configuration to Limit Access (Policy Compliance)

Control Network Access / Cloud Security Groups

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?
Organizations Struggle to Answer Basic Threat Questions

Are these hashes on/running in my network?
Or 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 – Visibility Beyond Anti-Virus

**Threat Intel Verification**

Threat Intel Feeds / Mandated to Verify
“Is this hash, registry, process, mutex on my network?”

**Detect Malware missed by Anti-Virus**

Using Qualys Malware Labs behavior models and leading commercial Threat Feed

**Hunting / Find Suspicious Activity**

Indicator of Activity hunting with pre-built and user-defined queries

**“Look Back” Investigation after a known breach**

Go back over months of stored endpoint events and find the first occurrence of a breach
Threat Intel Verification

1. Threat Intelligence lists attack information...

2. Search for the file hash here...

3. Find the object there.
Detect Malware Missed by Anti-Virus

UK Government Contractor
- “Big 4” Anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents

Qualys IOC discovered...
- Dridex Banking Trojan (51)
- 4 Domain Controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed
Event Telemetry:
file, process, mutex, network, registry

Malware Detection & Scoring – Actionable Responses

- Commercial Threat Feed
- Qualys IOC Detection and Scoring Engines

Qualys Malware Labs

Confirmed – Malicious Process w/ Network Connection
Confirmed – Malicious Process
Confirmed – Malicious File
Medium Confidence Suspicious – Process w/ Network Connection
Medium Confidence Suspicious – Process
Medium Confidence Suspicious – File
Low Confidence Suspicious – Process w/ Network Connection
Low Confidence Suspicious – Process
Low Confidence Suspicious – File
Remediated – Indicator no longer present
Known Good
Pre-Defined & Ad Hoc Threat Hunting

Suspicious process analysis to detect:

- “Fileless” malware attacks
- Non-malware attacks
- Malware evasion techniques
- Compromised processes
Find Malware using Stolen Code-Signing Certificates

July 2018
Certificates stolen from D-Link and others used by cyberespionage group


March 2019
Hackers dropped a secret backdoor in Asus’ update software

https://techcrunch.com/2019/03/25/asus-update-backdoor/
Indication of Compromise

Rules

Activity | Rule Manager | Actions

Search for alerts...
22 Apr 2019 1...

2.48K Total Activities

RULE NAME
RL score LT 10 2.48K
All malware infections 8

ACTION NAME
Verifying_RL_slac... 2.16K
Verifying_RL_Env... 314
Post to Slack 4
Send Email to Send... 4

EMAIL RECIPIENTS
priya.porwal2992... 318
pporwal@qualys... 318

1 - 50 of 2484

<table>
<thead>
<tr>
<th>RULE NAME</th>
<th>STATUS</th>
<th>AGGREGATE</th>
<th>ACTION</th>
<th>MATCHES</th>
<th>CREATED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>All malware infections</td>
<td>Success</td>
<td>No</td>
<td>Post to Slack</td>
<td>1</td>
<td>Qualys Demo</td>
</tr>
<tr>
<td>RL score &gt; 0</td>
<td>23 minutes ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All malware infections</td>
<td>Success</td>
<td>No</td>
<td>Send Email to Security...</td>
<td>1</td>
<td>Qualys Demo</td>
</tr>
<tr>
<td>RL score &gt; 0</td>
<td>23 minutes ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All malware infections</td>
<td>Success</td>
<td>No</td>
<td>Post to Slack</td>
<td>1</td>
<td>Qualys Demo</td>
</tr>
<tr>
<td>RL score &gt; 0</td>
<td>23 minutes ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All malware infections</td>
<td>Success</td>
<td>No</td>
<td>Post to Slack</td>
<td>1</td>
<td>Qualys Demo</td>
</tr>
<tr>
<td>RL score &gt; 0</td>
<td>23 minutes ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Indication of Compromise

Threat Intel Verification / Hunting
Malware Detection
Alerting
Thank You

Chris Carlson
ccarlson@qualys.com