Where Are We Now and Where is the Industry Going?

Making the World Safer - One App at a Time

Philippe Courtot
Chairman and CEO, Qualys, Inc.
Our Beginnings

Qualys Cloud Platform 1.0
The Vulnerability Management years - 1999 to 2011

Huge resistance to Cloud adoption
Scalability/accuracy
Consolidation of best-of-breed solutions
Where Are We Now?

Qualys Cloud Platform 2.0
Delivering an Integrated Suite of Security and Compliance solutions - 2012 to 2018

Major re-architecting of our Back-End
Started OPS, DevOps, Customer Support and Engineering In India
Expanded our solution to more than 10 Apps and made our first technology acquisitions
Where Are We Going?

Qualys Cloud Platform 3.0
Single pane of view that unifies IT, Security & Compliance - Entering the OT and IOT space - 2019 to 2021

Groundbreaking Global IT Asset Inventory solution

Consolidating more solutions

Bringing to market an integrated Incidence Response solution
Where is the Industry Going?

Major Consolidation
The era of the Cloud is coming fast and furious and unavoidable - 2019 to 2021

The Irresistible Rise of the Public Cloud Platforms

From Business continuity to Cyber Resilience

Building Security In - Not Bolting it on

Accelerated Industry Consolidation
Regaining Our Lost Visibility

Sumedh Thakar
Chief Product Officer, Qualys, Inc.
IT Transformation
Infrastructure & Application
Digital Transformation

Holistic Transformation of Business to Digital

Cloud, Containers, IaaS, PaaS, OT, IIoT, IoT, Mobility, Web apps, APIs, Mobile Apps
Hybrid Cloud Overview Architecture

- **Mobile Workforce**
- **Work Stations**
- **Clouds**

**On-Premise**
- **NETWORKS**
  - VMs
  - elastic
  - BARE METAL
- **STORAGE**
- **DB**

**West Coast Datacenter**
- **NETWORKS**
  - VMs
  - elastic
  - BARE METAL
- **STORAGE**
- **DB**

**East Coast Datacenter**
- **NETWORKS**
  - VMs
  - elastic
  - BARE METAL
- **STORAGE**
- **DB**
Containers

Real game changer
Hypervisor disappearing, bare metal is back
Kubernetes Infrastructure-as-code
Container-as-a-Service AWS Fargate
AWS Lambda function-as-a-service, serverless!
Kubefed?
“Priceline” for Containers?
DevOps

This is real and highly contagious

Developer decides how infrastructure runs in production

Speeds up significantly how fast code goes to production
On-Prem

Shrinking Datacenter Footprint

Increasing OT & IIoT

Corp IT – more distributed & mobile

More IoT!
Enterprise Mobility ≠ BYoD

Enterprise owned handheld devices

Indispensable to modern business

Running apps handling sensitive business & consumer data

Mobile!
Web Apps & APIs

Web Apps for the humans

APIs for the inhumans

Wide window into all your data
SaaS

More aaS everywhere

No infrastructure to manage

No Applications to code or manage
SaaS

Lead the charge against bloated cloud software.

Lehman
fresh.

Only simple.

Engagement software
Security
IBM PC AT
November 13, 1984

PC Magazine about IBM PC AT

“The AT provides the first real system for allowing executives to sleep at night:

A hard-to-duplicate ‘tubular’ key locks all but key holders out of the system”
34 years later

No magic key = No sleep at night!
Same challenges x 10
No visibility across global hybrid infrastructure
Still need to do Vulnerability & Configuration management
Still need to monitor integrity of systems(?)
More data incoming into “SIEM” deployments
Basically no visibility to respond
Compliance demands on new infrastructure
Future of Security

Transparent Orchestration

Built-in Automation the only real solution

Starts in DevOps

New generation of Security Analytics platforms
Qualys
Qualys Platform Approach

Embracing our own Digital Transformation

Massive expansion of backend for visibility – **620 Billion** security datapoints indexed

Comprehensive coverage of sensors – scanners, agents, cloud connectors, container sensors, passive sniffers and mobile agents
Qualys Platform Approach

Extending solutions into remediation & response

Building dedicated Data science team

Rapid expansion of R&D org

Key technology acquisitions & Investments
# Acquisitions & Investments

<table>
<thead>
<tr>
<th>Company</th>
<th>Product/Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nevis</td>
<td>Passive Scanning &amp; Secure Access Control</td>
</tr>
<tr>
<td>Netwatcher</td>
<td>Event Correlation Platform</td>
</tr>
<tr>
<td>1Mobility</td>
<td>Enterprise Mobility</td>
</tr>
<tr>
<td>Layered Insight</td>
<td>Built-in Runtime Container Security</td>
</tr>
<tr>
<td>42Crunch Investment</td>
<td>API Security</td>
</tr>
<tr>
<td>Frog 1</td>
<td></td>
</tr>
<tr>
<td>Frog 2</td>
<td></td>
</tr>
</tbody>
</table>
Secure web applications with end-to-end protection

Block attacks and virtually patch web application vulnerabilities

Qualys Cloud Apps

**ASSET MANAGEMENT**

- **Asset Inventory**
  - Maintain full, instant visibility of all your global IT assets

- **CMDB Sync**
  - Synchronize asset information from Qualys into ServiceNow CMDB

- **Cloud Inventory**
  - Inventory of all your cloud assets across AWS, Azure, GCP and others

- **Certificate Inventory**
  - Inventory of TLS/SSL digital certificates on a global scale

**IT SECURITY**

- **Vulnerability Management**
  - Continuously detect and protect against attacks, anywhere, anywhere

- **Container Security**
  - Discover, track, and continuously protect containers

- **Threat Protection**
  - Pinpoint your most critical threats and prioritize patching

- **Certificate Assessment**
  - Assess all your digital certificates for TLS/SSL vulnerabilities

- **Continuous Monitoring**
  - Alerts you in real time about network irregularities

- **Indication of Compromise**
  - Continuously monitor endpoints to detect suspicious activity

**COMPLIANCE MONITORING**

- **Policy Compliance**
  - Assess security configurations of IT systems throughout your network

- **Cloud Security Assessment**
  - Get full visibility and control across all public cloud instances

- **PCI Compliance**
  - Automate, simplify and attain PCI compliance quickly

- **Security Assessment Questionnaire**
  - Minimize the risk of doing business with vendors and other third parties

- **File Integrity Monitoring**
  - Log and track file changes across global IT systems

- **Security Configuration Assessment**
  - Automate configuration assessment of global IT assets

**WEB APPLICATION SECURITY**

- **Web Application Scanning**
  - Secure web applications with end-to-end protection

- **Web Application Firewall**
  - Block attacks and virtually patch web application vulnerabilities
Q4 2018 – more apps to come

- **PM**: Patch Management – beta
- **PAS**: Passive Network Sensor (unmanaged assets) – beta
- **AM**: Global IT Asset Management (managed assets) – GA

2018 | 2019
2019 – even more apps to come!

Secure Enterprise Mobility
Secure Access Control
API Security
Software Composition Analysis
Breach and Attack Simulation
Security Data Lake & Correlation Platform
Unified Dashboards
It’s the Platform!
(a real one)
Qualys Cloud Platform

Looking Under the Hood: What Makes Our Cloud Platform so Scalable and Powerful
Cloud Platform Environment
Security at scale on hybrid clouds

15+ products providing comprehensive suite of security solutions

10,300+ customers

7 shared cloud platforms across North America, Europe & Asia

70+ private clouds platforms deployed globally... on-prem, AWS, Azure, GCP

16+ PB storage and 16,000 cores
Cloud Platform Highlights

1+ trillion security events annually
3+ billion scans annually
2.5+ billion messages daily across Kafka clusters
620+ billion data points indexed in our Elasticsearch clusters

Unprecedented 2-second visibility
Qualys Cloud Platform
Sensors, Data Platform, Microservices, DevOps

Application Services / Shared Services / Stream & Batch Processing / Reporting / Analytics

Qualys Streaming Data Backbone

Cloud Agents  Passive Scanners  Scanners Appliances  Virtual Scanners  Internet Scanners
### Qualys Sensor Platform

Scalable, self-updating & centrally managed

<table>
<thead>
<tr>
<th>Physical</th>
<th>Virtual</th>
<th>Cloud/Container</th>
<th>Cloud Agents</th>
<th>Passive</th>
<th>API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy data centers</td>
<td>Private cloud infrastructure</td>
<td>Commercial IaaS &amp; PaaS clouds</td>
<td>Light weight, multi-platform</td>
<td>Passively sniff on network</td>
<td>Integration with Threat Intel feeds</td>
</tr>
<tr>
<td>Corporate infrastructure</td>
<td>Virtualized Infrastructure</td>
<td>Pre-certified in market place</td>
<td>On premise, elastic cloud &amp; endpoints</td>
<td>Real-time device discovery &amp; identification</td>
<td>CMDB Integration</td>
</tr>
<tr>
<td>Continuous security and compliance scanning</td>
<td>Continuous security and compliance scanning</td>
<td>Fully automated with API orchestration</td>
<td>Real-time data collection</td>
<td>Identification of APT network traffic</td>
<td>Log connectors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Continuous security and compliance on platform for security and compliance</td>
<td>Extract malware files from network for analysis</td>
<td></td>
</tr>
</tbody>
</table>

November 29, 2018

QSC Conference, 2018
Data Platform-as-a-Service

Right database for the right use case

- Highly scalable architecture
- Predictable performance at scale
- Distributed and fault-tolerant
- Multi-datacenter support
- Open-source
- Commodity hardware
Data Platform-as-a-Service

Kafka
Asynchronous, event-driven architecture
Foundation for Qualys Cloud Platform
Over 2.5 billion messages per day

Elasticsearch
Search for anything
Over 620 billion data points indexed
Estimating about 1 trillion data points by year end

Cassandra
Low latency storage
Source of truth for data across multiple products

Redis
In-memory cache
Improved system performance for frequently accessed data

Ceph
Object storage
Moving Oracle and in-house blob storage into Ceph

Over 2.5 billion messages per day

Over 620 billion data points indexed
Estimating about 1 trillion data points by year end

Source of truth for data across multiple products

Improved system performance for frequently accessed data

Moving Oracle and in-house blob storage into Ceph
Microservices & Cloud Native Architectures
Reduce risk and ship faster

Change how we design and build applications and services

- Monoliths to microservices
- Well defined APIs
- Packaged in containers
- Deployed on elastic infrastructure
- 12-Factor apps
- CI/CD, Service Registry, Config Servers
DevOps – Increased Efficiency

Goal is to make software delivery vastly more efficient

Supporting about 80 shared and private cloud deployments
Automation - Infrastructure as Code

Treat systems running your software as if they themselves are software

Automate
• Infra provisioning
• Configuration management
• Deployments...

....all using code
Monitoring Systems - Observability

Centrally monitor across all platforms using a single-pane view

End-to-end monitoring using
- Time series metrics
- Distributed tracing
- Log aggregation & analytics
- Alerting
Integrated Security - DevSecOps

Built-in security practices across the DevOps lifecycle

Qualys-on-Qualys
- Manage vulnerabilities
- Comply with policies
- Secure and shield web apps
- Validate file integrity
- Monitor systems
Qualys Cloud Platform

Integrated Suite of Applications
- CA
- AI
- VM
- CM
- TP
- FIM
- PC
- PCI
- SAQ
- IOC
- WAS
- WAF

Shared Services
- Authentication Service
- Authorization Service
- Subscription Service
- Indexing Service
- Data Sync Service
- Tagging Service

Messaging, Data, Analytics Platform
- kafka
- ceph
- elastic
- cassandra
- redis
- Flink

Infrastructure and DevOps Toolchain
- Logging
- Monitoring
- Config Mgmt.
- Service Registry
- CI/CD
- Docker/Kubernetes
Qualys Cloud Applications

**ASSET MANAGEMENT**
- **Asset Inventory**
  - Maintain full, instant visibility of all your global IT assets
- **CMDB Sync**
  - Synchronize asset information from Qualys into ServiceNow CMDB
- **Cloud Inventory**
  - Inventory of all your cloud assets across AWS, Azure, GCP and others
- **Certificate Inventory**
  - TLS/SSL digital certificates on a global scale

**IT SECURITY**
- **Vulnerability Management**
  - Continuously detect and protect against attacks, anytime, anywhere
- **Threat Protection**
  - Pinpoint your most critical threats and prioritize patching
- **Continuous Monitoring**
  - Alerts you in real time about network irregularities
- **Indication of Compromise**
  - Continuously monitor endpoints to detect suspicious activity

**COMPLIANCE MONITORING**
- **Policy Compliance**
  - Assure security configurations of IT systems throughout your network
- **Cloud Security Assessment**
  - Assess your security and control across all public cloud instances
- **PCI Compliance**
  - Automate, simplify and attain PCI compliance quickly
- **Security Configuration Assessment**
  - Continuous assessment of global IT assets

**WEB APPLICATION SECURITY**
- **Web Application Scanning**
  - Scan your applications with end-to-end protection
- **Web Application Firewall**
  - Detect and virtually patch web application vulnerabilities
- **Vulnerability Management**
  - Block attacks and virtually patch web application vulnerabilities

**AI**
- Asset Inventory
- CMDB Sync
- Cloud Inventory
- Certificate Inventory
**SYN**
- Asset Inventory
- CMDB Sync
- Cloud Inventory
- Certificate Inventory
**CI**
- Asset Inventory
- CMDB Sync
- Cloud Inventory
- Certificate Inventory
**TP**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**TPA**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**CM**
- Continuous Monitoring
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**CMR**
- Continuous Monitoring
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**PM**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**PC**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**SAQ**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**CM**
- Continuous Monitoring
- Patch Management (Beta)
- Indication of Compromise
**CMR**
- Continuous Monitoring
- Patch Management (Beta)
- Indication of Compromise
**PM**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**PC**
- Threat Protection
- Certificate Assessment
- Patch Management (Beta)
- Indication of Compromise
**CM**
- Continuous Monitoring
- Patch Management (Beta)
- Indication of Compromise
Advanced Correlation & Analytics

ML/AI Service
- Patterns
- Outlier
- Predictive SoC

Orchestration & Automation
- Integration
- Playbooks
- Response

UEBA
- User & Entity Behavior Analytics

Threat Hunting
- Search
- Exploration
- Behavior Graph

Security Analytics
- Anomaly
- Visualization
- Dashboard

Advanced Correlation
- Actionable Insights
- Out-of-box Rules

Qualys Security Data Lake Platform
- Data Ingestion
- Normalization
- Enrichment
- Governance

Qualys Quick Connectors

- Network
- Security
- Server
- End Point
- Qualys Apps
- Apps
- Cloud
- Users
- IoT

Qualys Apps
- CA
- VM
- AI
- PC
- IOC
- WAS
- WAF
Thank You

Sumedh Thakar
sthakar@qualys.com
Cloud Agent Platform

Chris Carlson
VP, Product Management, Qualys, Inc.
Digital Transformation is Driving IT Transformation for Organizations

- Private Clouds
- Public Clouds
- Enterprise On Premise
- Remote End Users

Internet
... 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

Central Management / API

Qualys Suite of Applications

Efficient Network Usage
*(Delta Processing average)*

Lightweight Metadata Collection *(tunable)*

Windows, Linux, Mac, AIX

50 - 350 KB / day

~1-2% CPU

3 MB application
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

(Units in millions)

Number of Cloud Agents Sold

<table>
<thead>
<tr>
<th></th>
<th>LTM Q4 2017</th>
<th>LTM Q1 2018</th>
<th>LTM Q2 2018</th>
<th>LTM Q3 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units in millions</td>
<td>6.0</td>
<td>7.3</td>
<td>8.1</td>
<td>13.9</td>
</tr>
</tbody>
</table>
Cloud Agent VM Usage and Growth Drivers

2016
- Deploy on servers to overcome customer limitations with their network scanning
  - Auth issues
  - Scan windows
  - More frequent VM assessments

2017
- Increasing adoption for Servers
- Initial adoption for end-users (WannaCry)
- Early CA deployments in AWS and Azure

2018
- Growth in endpoint deployments (50-300K)
- Growth in public cloud (AWS primarily)
- Initial work to build CA into CI/CD/DevOps pipelines

2019
- Visibility + Lightweight agent increases adoption
- Increase endpoints
- Increase in public cloud
- Capture migration from on-premise servers to public cloud
Cloud Agent CPU Tuning - Linux

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

AWS t2.micro instance running Cloud Agent

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

0.5% CPU when idle / heartbeat
Cloud Agent CPU Tuning - Windows

Tunable CPU Limit
Example: 8% configured max on 1-core
  (Effective: <2% on 4-core)
### Selected Cloud Agent Deployments

<table>
<thead>
<tr>
<th>Category</th>
<th>Deployment Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecommerce / Technology</td>
<td>40,000,000/yr AWS + 210,000 Windows</td>
</tr>
<tr>
<td>Technology Company</td>
<td>2,000,000 Azure</td>
</tr>
<tr>
<td>Ecommerce</td>
<td>3,500,000/yr AWS</td>
</tr>
<tr>
<td>Financial Services</td>
<td>485,000 Windows (+ 500,000 Linux 2H 2018)</td>
</tr>
<tr>
<td>Financial Services</td>
<td>200,000 (AWS and users) + 20,000 FIM</td>
</tr>
<tr>
<td>Professional Services</td>
<td>340,000 user and servers</td>
</tr>
<tr>
<td>Retailer</td>
<td>100,000 in datacenter and 2,500 stores</td>
</tr>
<tr>
<td>Financial Services</td>
<td>3,000 ATM machines</td>
</tr>
</tbody>
</table>
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>accountId</td>
<td>dnsservers</td>
<td>hostname</td>
</tr>
<tr>
<td>amiId</td>
<td>ipv6</td>
<td>instanceld</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>instanceType</td>
<td>privatelIpAddress</td>
<td>resourceGroupName</td>
</tr>
<tr>
<td>kernelId</td>
<td>privatelIpAddress</td>
<td>tags</td>
</tr>
<tr>
<td>macAddress</td>
<td>publicIpAddress</td>
<td>subnet</td>
</tr>
<tr>
<td>privatelIpAddress</td>
<td>publicIpAddress</td>
<td>subscriptionId</td>
</tr>
<tr>
<td>publicIpAddress</td>
<td>region</td>
<td>version</td>
</tr>
<tr>
<td>region</td>
<td>reservationId</td>
<td>vmId</td>
</tr>
<tr>
<td>reservationId</td>
<td>securityGroupIds</td>
<td>vmSize</td>
</tr>
<tr>
<td>securityGroups</td>
<td>subnet</td>
<td></td>
</tr>
<tr>
<td>subnetId</td>
<td>securityGroupIds</td>
<td></td>
</tr>
<tr>
<td>VPCId</td>
<td>securityGroups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnetId</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subscriptionId</td>
<td></td>
</tr>
<tr>
<td></td>
<td>version</td>
<td></td>
</tr>
</tbody>
</table>

Agent collects metadata locally
<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>privatelp</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.imageId
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)

Cloud Agent – Available now
aws.ec2.accountId
aws.ec2.availabilityZone
aws.ec2.hostname
aws.ec2.imageId
aws.ec2.instanceId
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

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

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data collection installation status</td>
<td>31 of 56 VMs</td>
</tr>
<tr>
<td><strong>Vulnerability assessment not installed</strong></td>
<td>2 of 56 VMs</td>
</tr>
<tr>
<td>Endpoint Protection not installed</td>
<td>4 of 56 VMs</td>
</tr>
<tr>
<td>Missing scan data</td>
<td>11 of 56 VMs</td>
</tr>
<tr>
<td>RemEDIATE OS vulnerabilities (by Microsoft)</td>
<td>5 of 56 VMs</td>
</tr>
<tr>
<td>Missing system updates</td>
<td>1 of 56 VMs</td>
</tr>
<tr>
<td>Endpoint Protection health failures</td>
<td>1 of 56 VMs</td>
</tr>
<tr>
<td>Missing disk encryption</td>
<td>5 of 56 VMs</td>
</tr>
<tr>
<td>OS version not updated</td>
<td>2 of 4 Roles</td>
</tr>
<tr>
<td>Vulnerabilities found</td>
<td>2 of 56 VMs</td>
</tr>
<tr>
<td>Healthy</td>
<td>6 of 60 VMs &amp; Roles</td>
</tr>
<tr>
<td>RESOURCE GROUP</td>
<td>HS_RESOURCEGROUP</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>SUBSCRIPTION</td>
<td>Visual Studio Premium with MSDN</td>
</tr>
<tr>
<td>VIRTUAL IP</td>
<td></td>
</tr>
<tr>
<td>OPERATING SYSTEM</td>
<td>Windows</td>
</tr>
<tr>
<td>VERSION</td>
<td>Compute</td>
</tr>
<tr>
<td>STATUS</td>
<td>Deallocated</td>
</tr>
<tr>
<td>MONITORING STATE</td>
<td>Monitored by Azure Security Center</td>
</tr>
<tr>
<td>PREVENTION STATUS</td>
<td>High severity</td>
</tr>
<tr>
<td>Security Solutions</td>
<td></td>
</tr>
<tr>
<td>SYSTEM UPDATES</td>
<td>Microsoft (Last scan time - 10/3/2016 1:22 PM)</td>
</tr>
<tr>
<td>OS VULNERABILITIES</td>
<td>Microsoft (Last scan time - 10/3/2016 1:22 PM)</td>
</tr>
<tr>
<td>VULNERABILITY SCANNER - PREVIEW</td>
<td>Qualys (Last scan time - 10/3/2016 11:56 PM)</td>
</tr>
</tbody>
</table>

### 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>

<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 CRE...</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>Access to File Share is Enabled...</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 Detected...</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 Used File...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Low</td>
</tr>
<tr>
<td>File Access Permissions for User...</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 Enumeration...</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 Attempting Login...</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>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 Cre...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Machine Information Disc...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Microsoft Windows Explo...</td>
<td>Qualys</td>
<td>harivm2</td>
<td>Open</td>
<td>Medium</td>
</tr>
<tr>
<td>Windows Explorer Autop...</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 Detec...</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>
</tbody>
</table>

**VULNERABILITY NAME**

**SEVERITY**

- **High**

**DESCRIPTION**

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

The image shows a screenshot of a vulnerability management tool interface, displaying the number of confirmed vulnerabilities and potential vulnerabilities categorized by severity levels. The tool is used to manage and monitor security threats in an IT environment.
Threat Protection Exploitability 😞
Cloud Agent Roadmap

Agent Releases
• Mac 1.7.2 – released Aug 29
• Linux 2.1 upgrade from 2.0 (FIM) – released Aug 29
• Linux 2.2 – Dec rollout for Policy Compliance UDCs
• Windows 2.1.1 rollout – started Oct 17 / complete Oct 22
• 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