



QUALYS SECURITY CONFERENCE 2018

# A 360° Approach to Securing the Cloud

Total Visibility and Comprehensive Security for Cloud workloads and infrastructure

**Hari Srinivasan**

Director, Product Management, Qualys, Inc.

# Agenda

“Shift Left” Migration & Requirements

Your responsibility in cloud security

Customer Case Studies

Qualys Security for hardening and standardizing workloads

Qualys security for Infrastructure

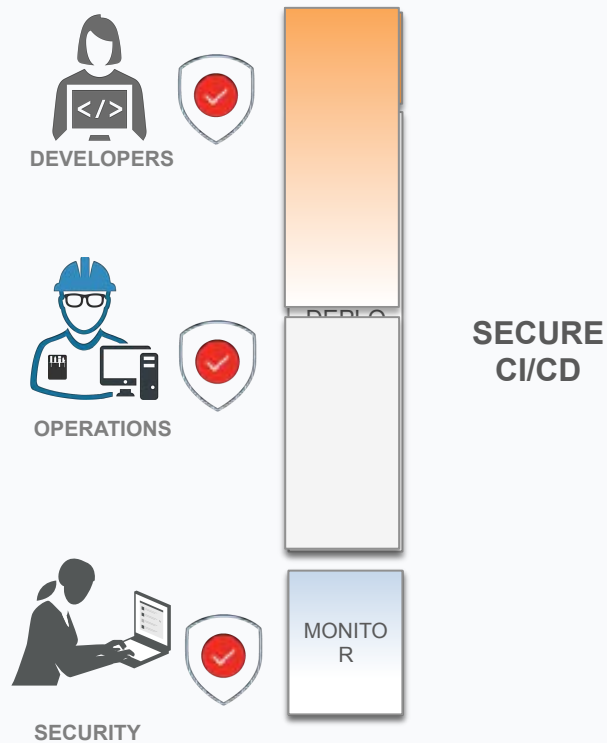
Use Cases & Demo

Q&A



# The Big Migration... in security, it is happening..

Continuous Secure Development and Deployment



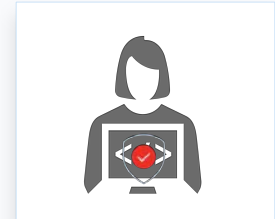
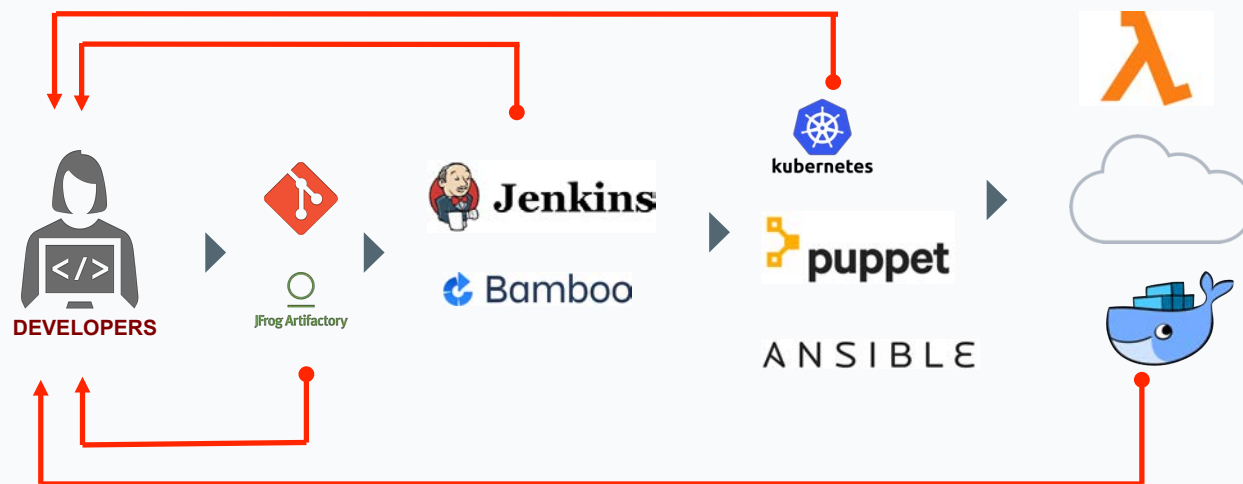
## SECURITY AT DEVELOPMENT

- ✓ Static Code Analysis
- ✓ Vulnerability Management
- ✓ Web Application Scanning
- ✓ Compliance Checks
- ✓ Configuration Assessments

## SECURITY AFTER DEPLOYMENT

- Vulnerability Management
- Compliance Checks
- Configuration Assessments
- Web Application Scanning
- Web Application Firewalls

# DevOps/DevSecOps Requirements...

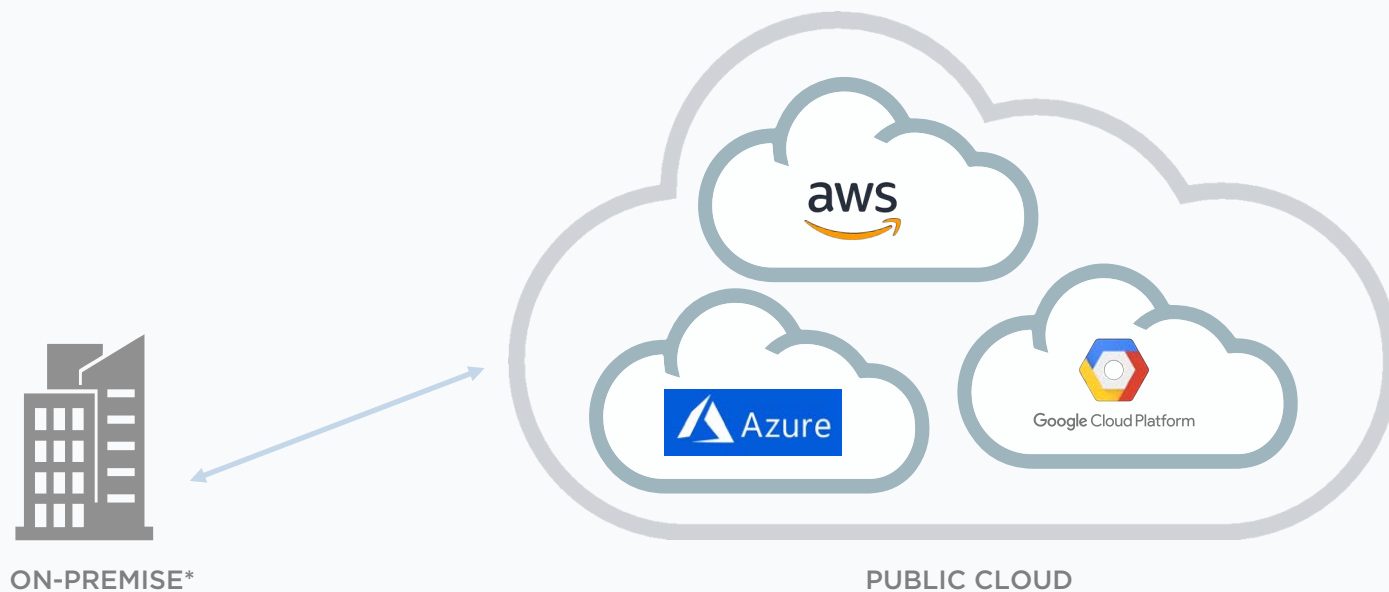


DevSecOps Engineer

Responsible for  
**automating**  
**security** checks  
and remediating  
viable security  
threats in  
development/  
deployment  
practices

AUTOMATION & ACTIONABLE DATA ....

# The New IT – Hybrid, Multi-Cloud Deployment



# Shared Security Responsibility Model

You

are responsible for securing  
your data and workloads



# Securing Cloud Workloads

## Hardening and Standardizing



### VULNERABILITY MANAGEMENT

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management\*

### POLICY COMPLIANCE

- Policy Compliance (incl. Secure Configuration Assessments)
- File Integrity Monitoring

### APPLICATION SECURITY

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall

\* Upcoming feature

# Securing Public Clouds Using Qualys

## Customer Case Studies



Reduced application releases from 2 weeks to 24 hrs by automating security with Qualys in to DevOps

### A SOFTWARE MAKER

*Private*

“Just in time” security approvals with end to End integration of Qualys Scan and Reports with ServiceNow

### A BEVERAGE MNC

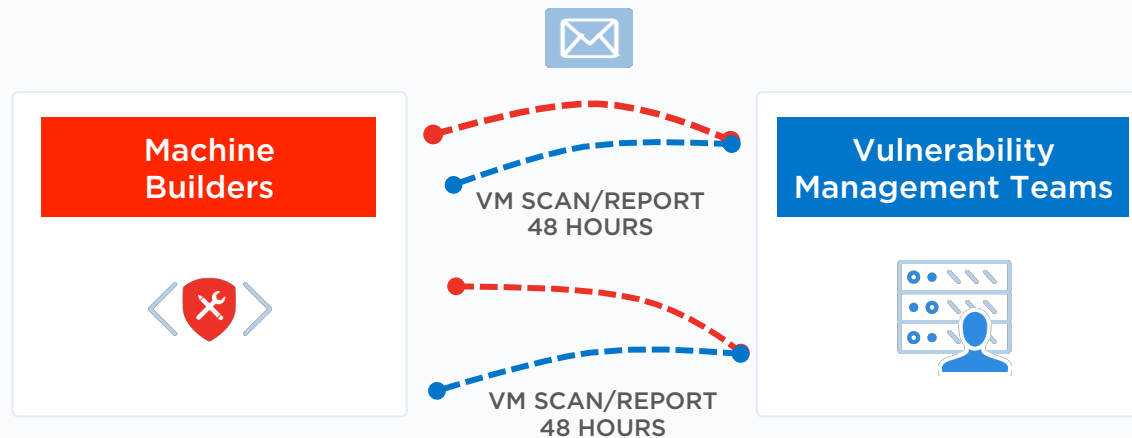
*Private*

Enabling DevOps with automated agent deployment via Azure Security Center



Capital One

# Before: Lack of Security Automation Delays Release

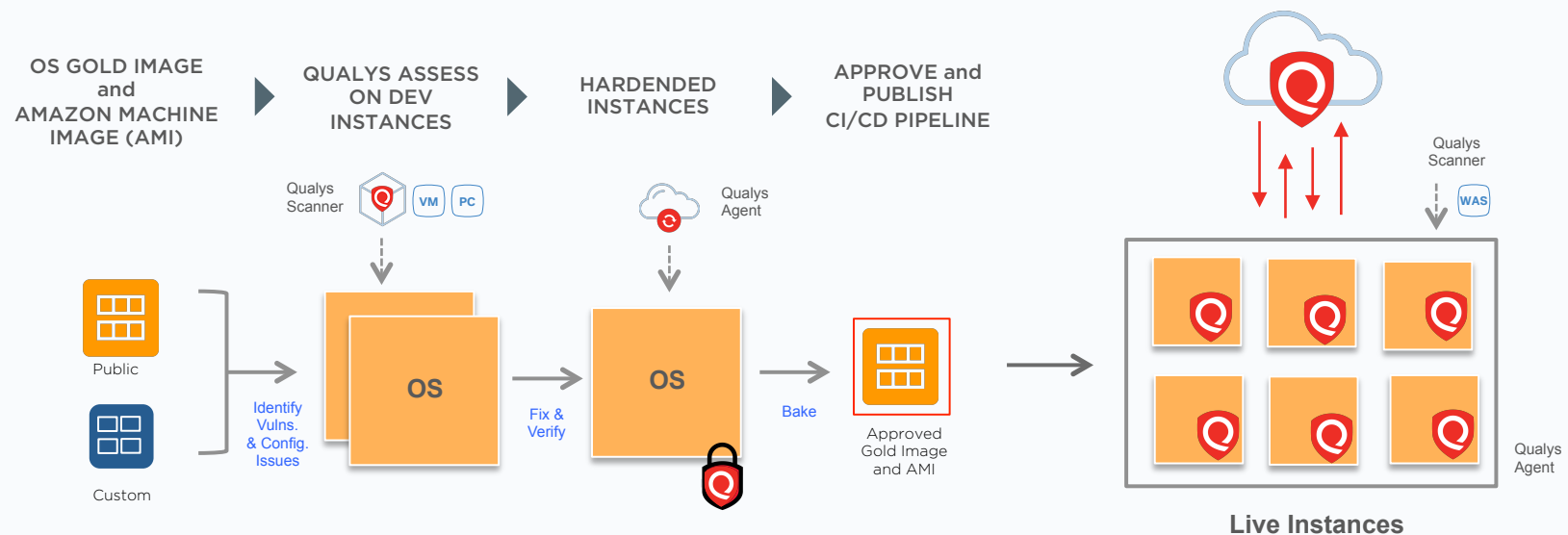


Two weeks until the Image (AMI) is certified for production

## Capital One

# Introducing Security at the Source Bake

Qualys Security into Gold Images and AMI



Bakery process happens within 24 Hrs

Private

# “Security as Service”

## Integration between Service Now and Qualys

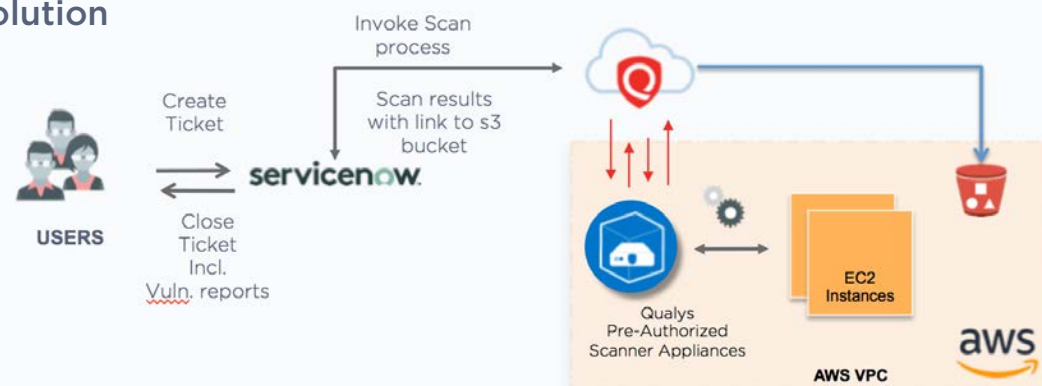
### Challenge

- Moved almost all datacenters to AWS
- Keeping up with security “Just in Time” projects with multiple teams submitting requests for spinning up infrastructure

### Requirement

- Automate Vulnerability Mgmt. from Connectors, Scans, and to Results
- Integrate into Service Now for end to end invocation

### Solution



### Company Profile

Makes software for architecture, Engg. , construction and Media

**INDUSTRY:** Software, Media, Manufacturing

**REGION:** USA

### CLOUD:

Primary Cloud - AWS  
Secondary Cloud- Azure

### DEPLOYMENT REGION:

US East, West

### SERVICES USED:

EC2, S3, RDS, EMR, EBS, Containers

### QUALYS USAGE:

VM, AV, Scanners

# A Beverage MNC Company

## Qualys Automation within Azure Security Center

Private

Fast growing deployment in Azure  
( added 10K instances in 6 months)

### Problem?

Ops wants to simplify the process of  
security tools rollout

Security wants to participate into  
DevOps

### Solution

Utilizing Qualys integration with  
Azure Security Center

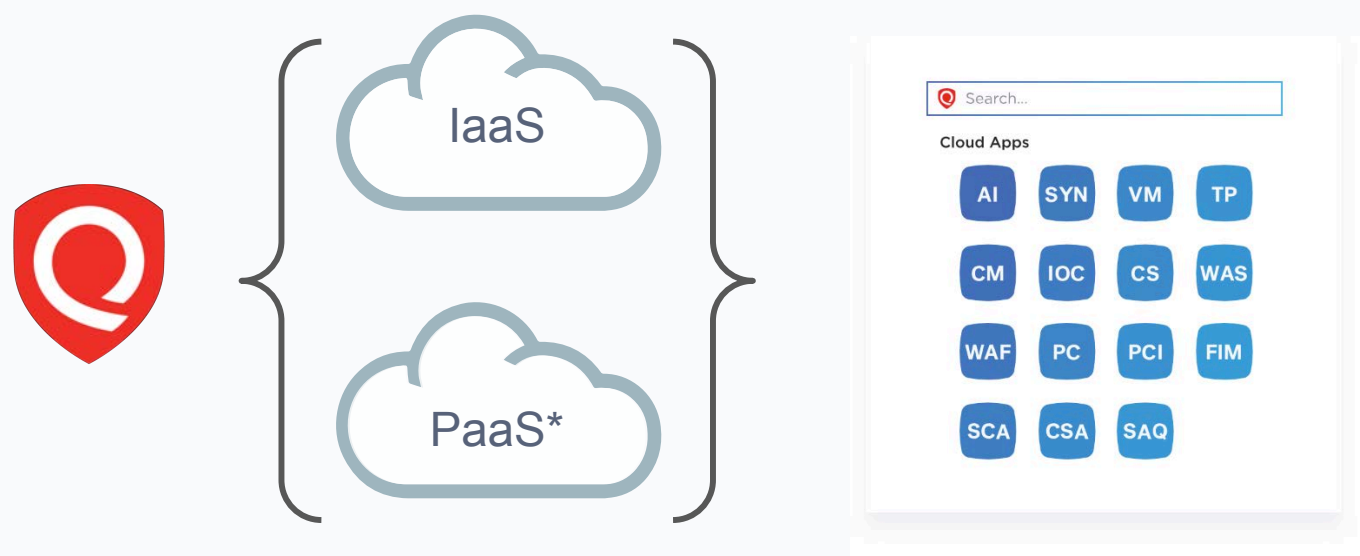
Utilize ASC automation to bake  
agents into test subscription and  
review reports with ASC

The screenshot shows the Azure Security Center interface. On the left, the navigation pane includes 'Security Center' under 'More services'. A red arrow points from this link to the main window titled 'Remediate vulnerabilities (by Qualys)'. The main window displays a table of vulnerabilities:

VULNERABILITY NAME	VENDOR	AFFECT...	STATE	SEVERITY
Enabled DCOM	Qualys	harivm2	Open	High
Allowed Null Session	Qualys	harivm2	Open	Medium
Enabled Cached Logon Cre...	Qualys	harivm2	Open	Medium
Machine Information Discl...	Qualys	harivm2	Open	Medium
Microsoft Windows Explore...	Qualys	harivm2	Open	Medium
Windows Explorer Autopla...	Qualys	harivm2	Open	Medium
Access to File Share is Enab...	Qualys	harivm2	Open	Low
ActiveX Controls Enumerated	Qualys	harivm2	Open	Low
Antivirus Product Not Dete...	Qualys	harivm2	Open	Low
Disabled Clear Page File	Qualys	harivm2	Open	Low
Enabled Caching of Dial-up...	Qualys	harivm2	Open	Low
Enabled Display Last User...	Qualys	harivm2	Open	Low
File Access Permissions for ...	Qualys	harivm2	Open	Low
File Access Permissions for ...	Qualys	harivm2	Open	Low
Host Scan Time	Qualys	harivm2	Open	Low
Hyper-V Host Information ...	Qualys	harivm2	Open	Low
Installed Applications Enu...	Qualys	harivm2	Open	Low
Internet Protocol version 6 ...	Qualys	harivm2	Open	Low

The Qualys logo is visible in the bottom right corner of the interface.

# Cloud Workload Security with Qualys



\* PaaS - Cloud Database Scanning - Roadmap 1H '19

# Integrating within the process and response pipeline with Partners

Securing by Micro segmentation and segregation



Configuration and Change Management



Keeping track of assets (CMDB)



Pumping data into SIEM for analysis



# Cloud Integrations

Azure Security Center (VM)  
-Production

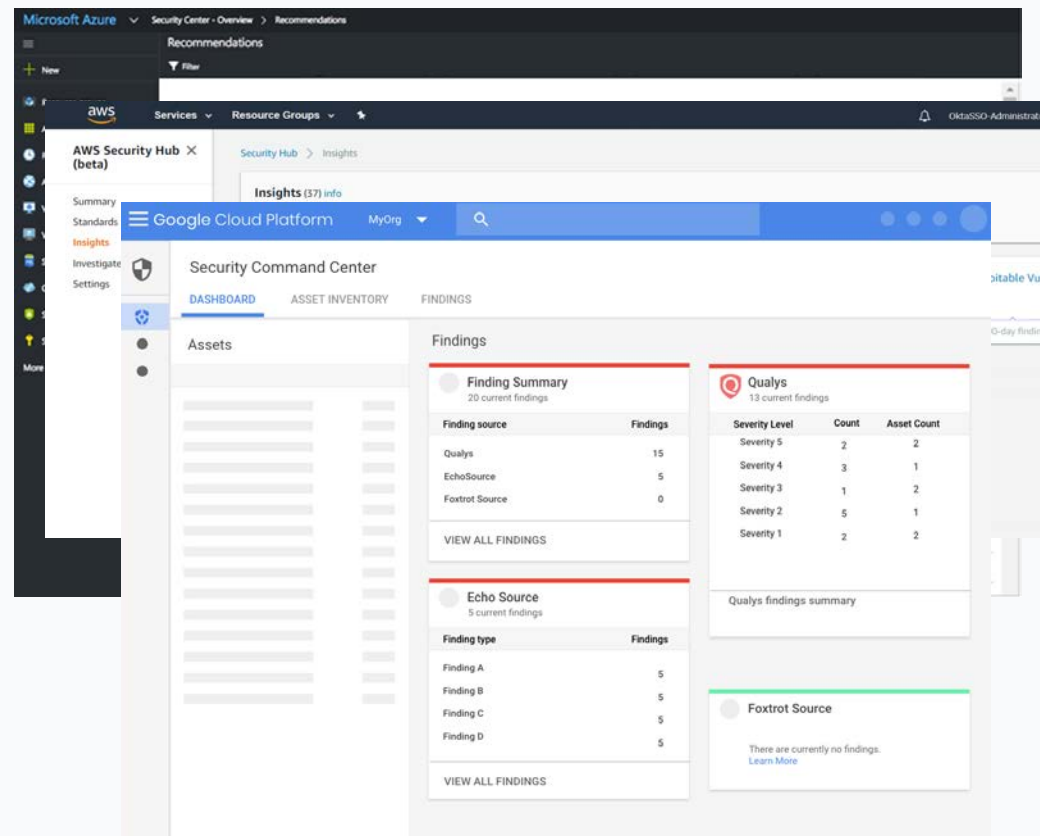
AWS Security Hub  
- Public Preview – Nov 28, 2018!!!

Google Security Command Center  
- Beta in December 2018

## Other Integrations

IBM Security Center  
- Dec2018/Jan 2019

Alibaba Security Center  
- Q1/Q2 2019



# Securing Azure Stack using Qualys

Qualys is the only distributor of Infra's VM,PC reports



User Workloads  
Virtual machines, SQL  
databases, containers, storage,  
web apps, load balancers, vpn...

Networking and other  
OEM components

Infrastructure



- ✓ Qualys Security Solution suite – VM, PC, AppSec,..
- ✓ Network Scan using Qualys Vulnerability Management
- ✓ Vulnerability and Compliance Reports available from MSFT Azure Stack

Register @ <https://www.qualys.com/azure-stack/>



# Cloud Infrastructure

Australian Insurance Company

# Visibility of deployments stop misuse of keys



AWS sent a notice of compromised keys attempting to create multiple accounts in EU

## Use Case

Identify the resources in EU region, find the Amazon S3 buckets which are open to public and have the keys stored

## Requirement

- Identify where the deployments are located
- Identify Amazon S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

### Company Profile

Largest provider of Auto and Agriculture insurance



**INDUSTRY:** Insurance

**REGION:** Australia

### CLOUD:

Primary Cloud - AWS  
Secondary Cloud- Azure

### DEPLOYMENT REGION:

Australia

### SERVICES USED:

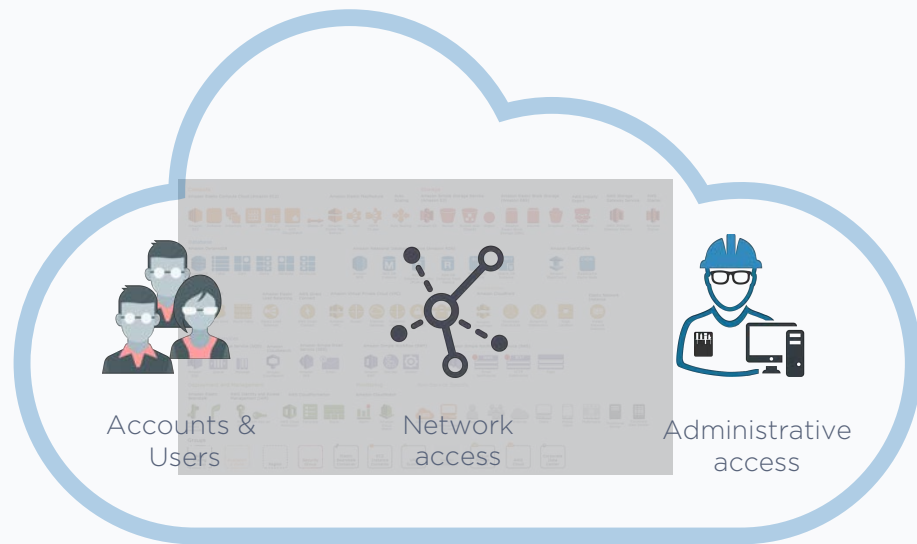
EC2, S3, RDS, EMR, Cloud Front

# We need to secure against...

Misconfigurations

Malicious behavior

Non-standard deployments



# Qualys Cloud Inventory and Security Assessment

Unparalleled Visibility and  
Continuous Security Monitoring  
across public cloud infrastructure



Cloud  
Inventory



Cloud  
Security  
Assessment

## Use Case #1

# Visibility into your public clouds

### View into

- Resource Distribution by Type
- Resources by Region

Personalize and add custom widgets



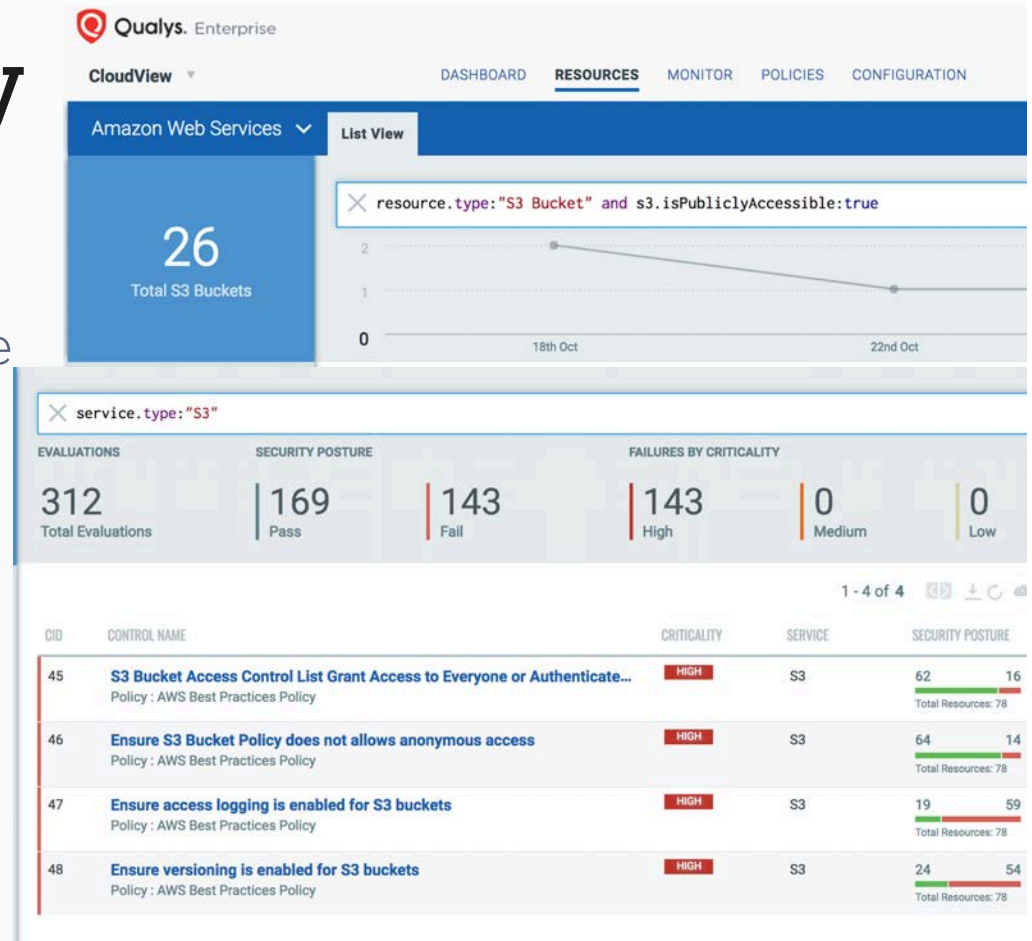
## Use Case #2

# Identify Leaky S3 buckets

Misconfigured S3 Buckets are vulnerable for data leaks

Check the S3 Bucket Access Permissions Regularly

- Review Access Control List
- Check Bucket Policy



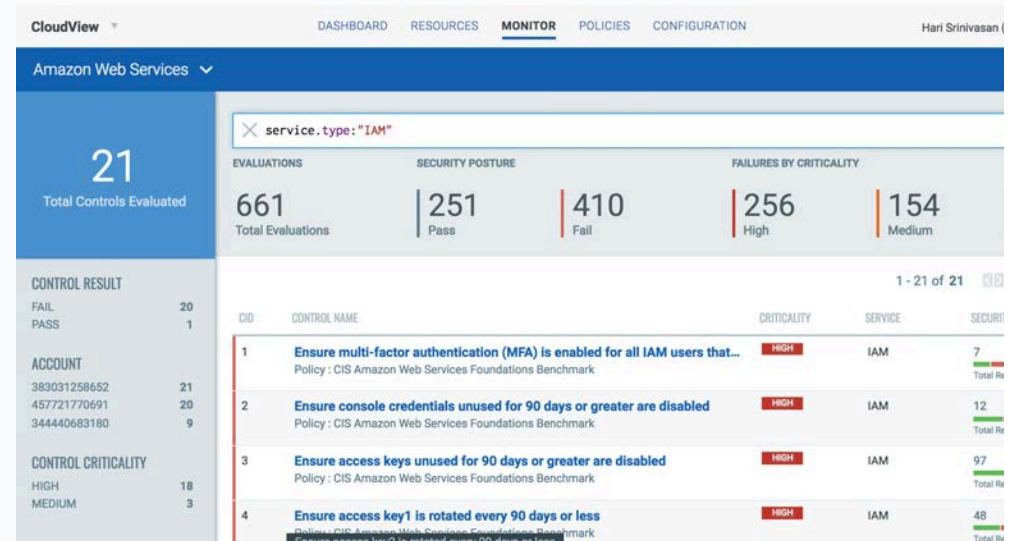
## Use Case #3



# Detect Compromised IAM Users

### Check for:

- Configure Strong Password Policy for Account
- Enforce MFA for Console Users
- Rotate IAM Access Keys Every 90 Days
- Removed Unnecessary Credentials
- Audit Process
  - Create separate user for console & API access ( Segregation of duty)
  - Track password age
  - Deactivate unused keys



## Australian Insurance Company

# Visibility of deployments stop misuse of keys



AWS sent a notice of compromised keys attempting to create multiple accounts in EU

### Requirement

- Identify where the deployments are located
- Identify S3 buckets that are public and fix it
- Ensure best practices are followed by IAM users of the account

### Solution

With Qualys Cloud Inventory and Assessment

- ✓ Gain visibility into the global deployments
- ✓ Identify S3 buckets that are public and required fixing
- ✓ Identify the IAM users and their security posture

### Company Profile

Largest provider of Auto and Agriculture insurance



**INDUSTRY:** Insurance

**REGION:** Australia

### CLOUD:

Primary Cloud - AWS  
Secondary Cloud- Azure

### DEPLOYMENT REGION:

Australia

### SERVICES USED:

EC2, S3, RDS, EMR, Cloud Front



# Visibility – Get started with a FREE service



## **CloudView**

A FREE inventory and monitoring service for your public clouds

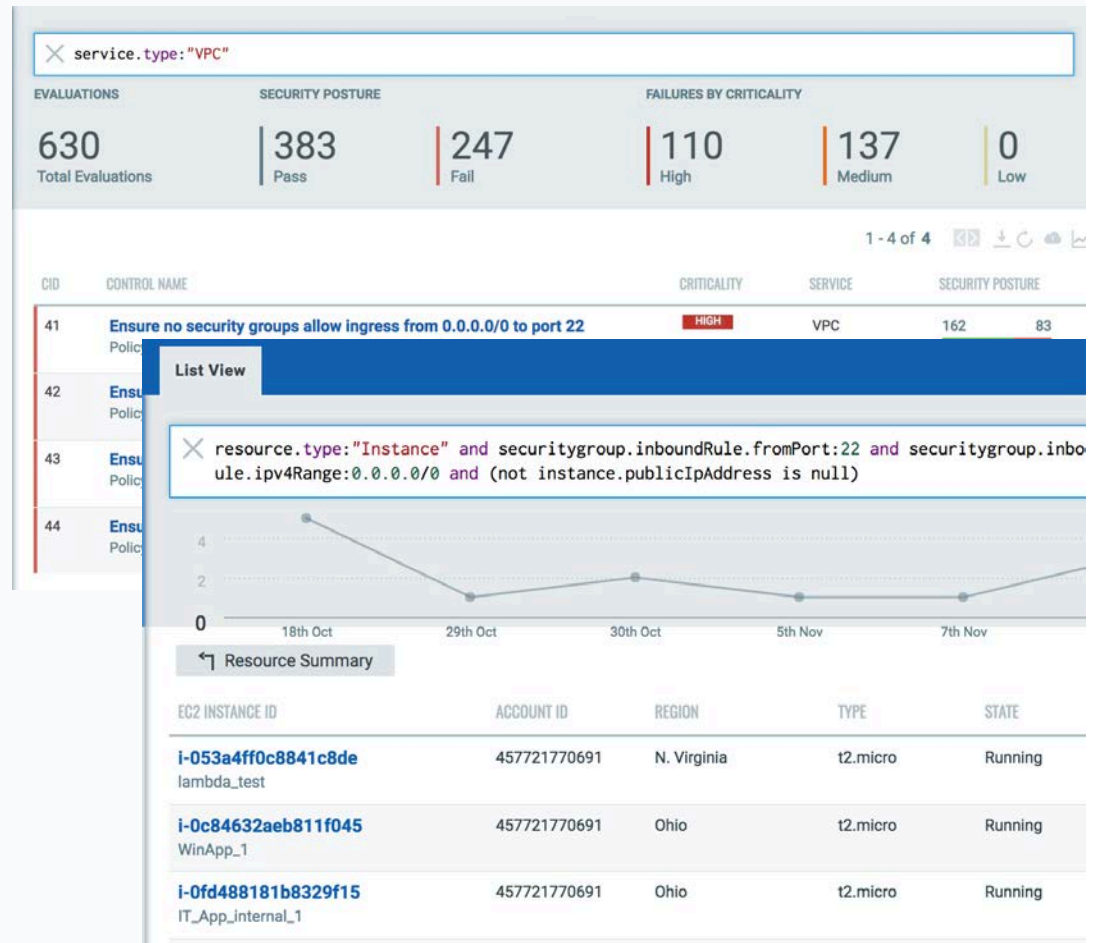
\* FREE version is for Cloud Inventory, defaults to 3 accounts per cloud, can be extended further

## Use Case#4

# Misconfigured Security Groups

Security groups with default rule, allowing access on port 22, 3389

With Qualys Vulnerability Mgmt. - Identify Security Groups exposing Vulnerable instances

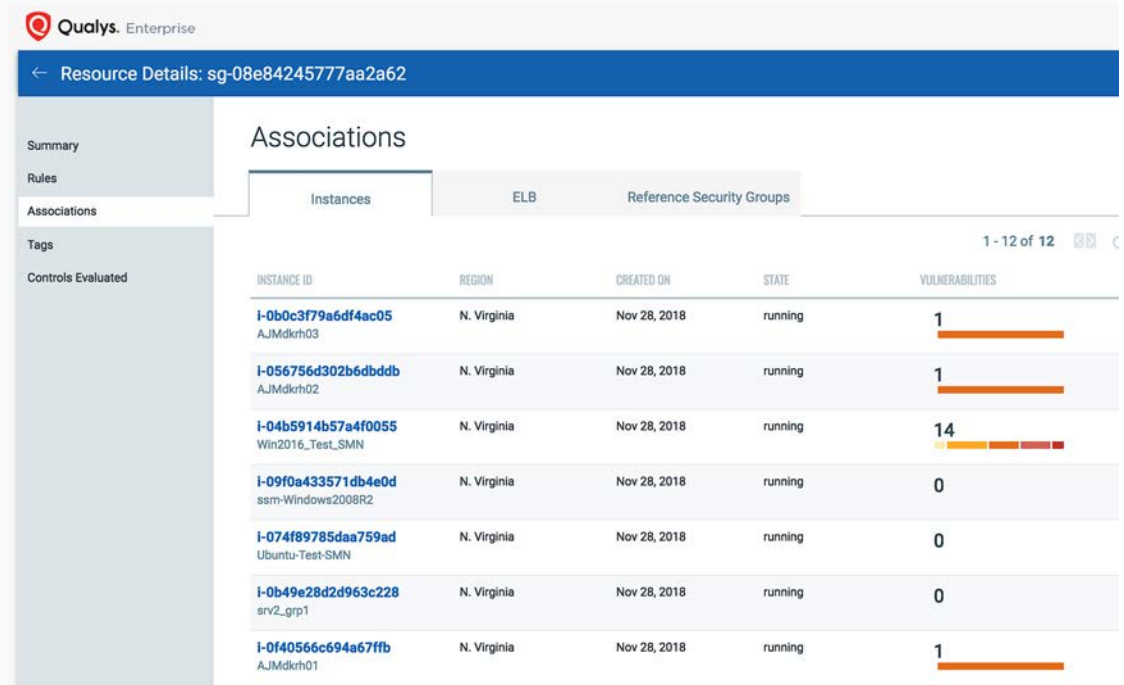


## Use Case#5

# Correlate with Vulnerability Data

Identify vulnerable instances associated with the security groups

Reduce effort to pull info to SIEM for correlation



Qualys. Enterprise

← Resource Details: sg-08e84245777aa2a62

Summary  
Rules  
Associations  
Tags  
Controls Evaluated

Associations

Instances ELB Reference Security Groups

1 - 12 of 12

INSTANCE ID	REGION	CREATED ON	STATE	VULNERABILITIES
<a href="#">i-0b0c3f79a6df4ac05</a> AJMdkrh03	N. Virginia	Nov 28, 2018	running	1
<a href="#">i-056756d302b6dbddb</a> AJMdkrh02	N. Virginia	Nov 28, 2018	running	1
<a href="#">i-04b5914b57a4f0055</a> Win2016_Test_SMN	N. Virginia	Nov 28, 2018	running	14
<a href="#">i-09f0a433571db4e0d</a> ssm-Windows2008R2	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-074f89785daa759ad</a> Ubuntu-Test-SMN	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-0b49e28d2d963c228</a> srv2_grp1	N. Virginia	Nov 28, 2018	running	0
<a href="#">i-0f40566c694a67ffb</a> AJMdkrh01	N. Virginia	Nov 28, 2018	running	1

# New and Upcoming Features

Threat Analysis

Remediations

Reports

# Threat Analysis

Correlating Vulnerability data to provide risk insights

## Use Cases

Security Groups allowing access on the same ports where network vulnerabilities have been identified

Vulnerable EC2 Instances with Instance profiles accessing S3 buckets

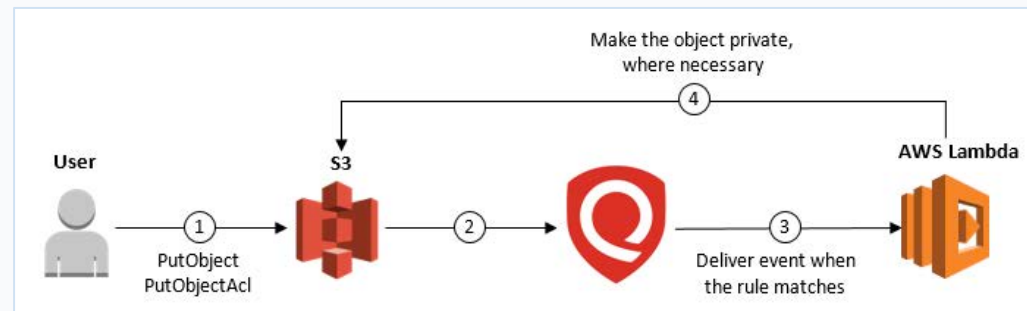
Coming Dec. 2018

The screenshot displays the Qualys Enterprise Threat Analysis interface. The top navigation bar shows 'Resource Details: sg-5c324e25'. The left sidebar contains a menu with 'Summary', 'Rules', 'Associations', 'Tags', 'Threats' (selected), and 'Controls Evaluated'. The main content area, titled 'Threat Details', features three summary cards: 'PORTS WITH TREATS' (20 Ports), 'IMPACTED RESOURCES' (20 Resources), and 'OPEN PORT VULNERABILITIES' (3 Vulnerabilities). Below these cards are controls for 'Actions', 'Show Issues by: Ports', and 'Open Rule Simulator'. A table titled 'RULES' lists the following data:

PORT	TYPE	PROTOCOL	PORT RANGE	SOURCE	PORT WITH TREATS	IMPACTED INSTANCES	VULNERABILITIES
80	Custom	TCP	0-100	0.0.0.0/0	9	2	2
8080	Custom	TCP	8080	0.0.0.0/0	9	2	2

# Remediation

Automate in real time actions to protect against risks



Lambda function that reads the state of the S3 bucket, updates to make bucket and its object private.

Integration into Qualys Cloud View  
**(Coming in Q1'2019)**

- Collect evaluation results
- Execute update permissions

# Cloud Infrastructure Reports

Coming  
Jan'19

Generate reports for CIS Benchmarks, mandates like PCI, HIPAA, ISO27001, NIST 800-53,...

Configure for specific accounts, and regions

Schedule reports for daily, weekly or monthly

Coming Jan. 2019

Qualys Enterprise

CloudView ▾ DASHBOARD RESOURCES MONITOR **REPORTS** CONFIGURATIONS

Dave Jones (qyays\_dj) ▾

Search

Actions ▾ Create New Report

REPORT TITLE

PCI Report for MyAWS Quick Actions

CIS Report for MyAWS

Run Now

Download

Edit

Delete

Qualys Enterprise

PCI Report for MyAWS Storefront

Report Info

Created date: 05/23/2018 at 00:09:52

Created by: Hari Srinivasan

User name: quays\_id

Role: Manager

Company: Qualys

Address: 501 The Metropolitan  
Wakdevad  
Pune, Maharashtra 411005  
India

Report Settings

Policies: CIS Amazon Web Services Foundations Benchmark

Asset Selection: All Assets in Policy

Template: Payment Card Industry Data Security Standard (PCI - DSS) v3.2

Report Summary

Mandates: 1	Requirements: 12	PCI - DSS 96.6%
Connector Name: MyAWS Storefront	Account ID: (383031258652)	Controls: 44
		Total Evaluations: 294
		Policies: 1

Report Statistics

Requirement Posture

Requirement Posture for Payment Card Industry Data Security Standard (PCI - DSS) v3.2

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications
- Requirement 7: Restrict access to cardholder data to business need-to-know

Coming  
Dec'18

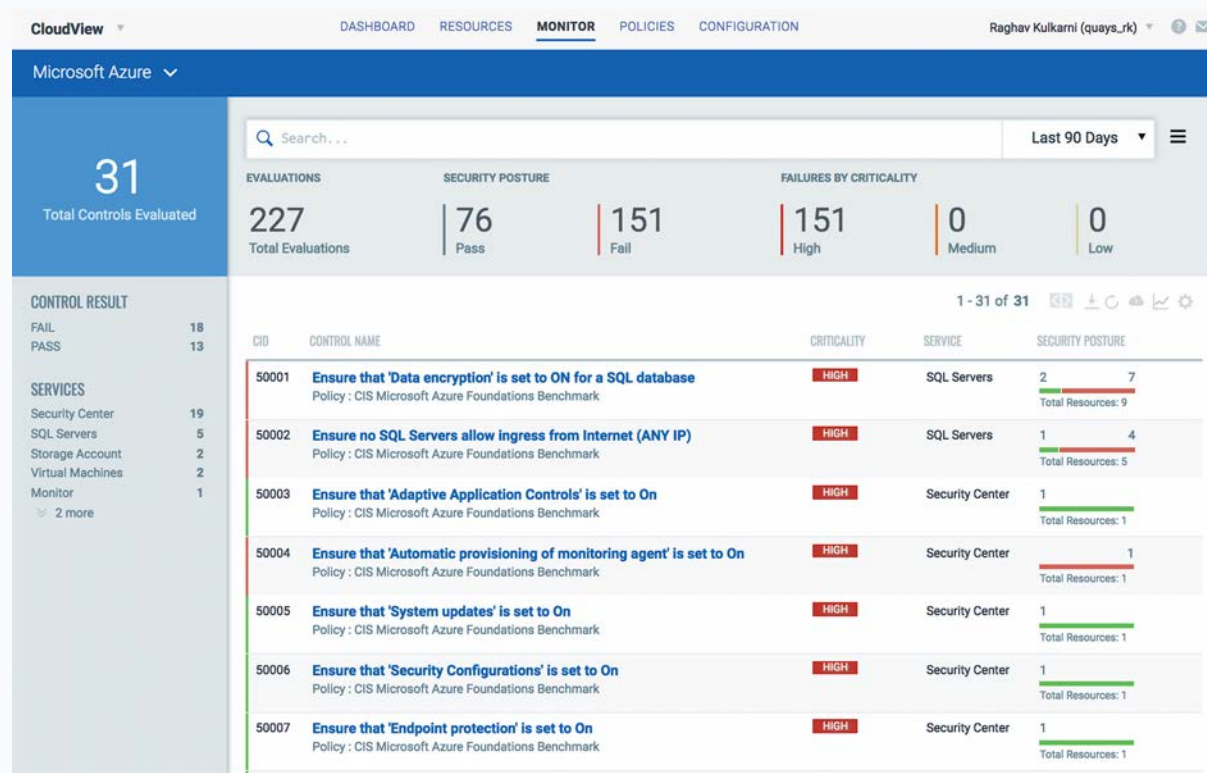
# Azure CIS 1.0.0 Benchmark Controls

~ 40 checks

Azure Assets Evaluated

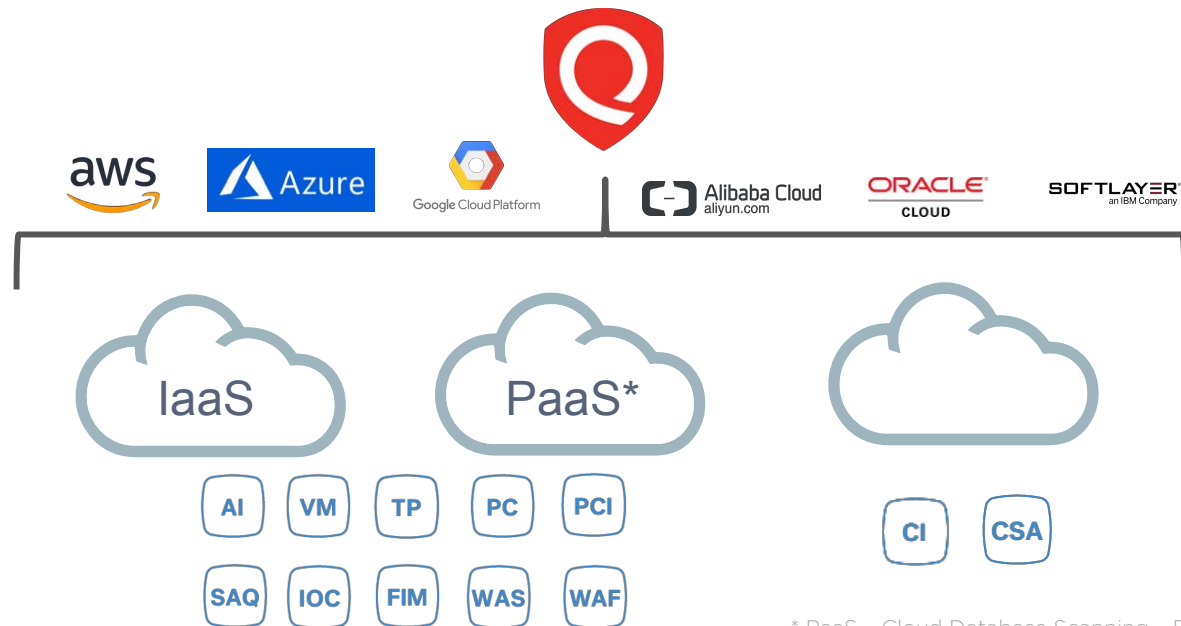
- Azure Virtual Machines
- Azure Virtual Networks
- Azure Blob Storage
- Azure Network Security groups
- Azure SQL Databases
- Azure Security Center
- Storage Accounts
- Logging & Monitoring services

Coming Dec. 2018





# Qualys Cloud Security – Comprehensive Coverage



\* PaaS – Cloud Database Scanning – Roadmap 1H '19

\*\* CSA – Google (Q4'18), IBM, Alibaba, 1H -2H '19

# Q&A