A 360° Approach in Securing 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...

AUTOMATION & ACTIONABLE DATA....

DEVELOPERS

Jenkins

Bamboo

kubernetes

puppet

ANSIBLE

DevSecOps Engineer

Responsible for automating security checks and remediating viable security threats in development/deployment practices
The New IT – Hybrid, Multi-Cloud Deployment

ON-PREMISE*  PUBLIC CLOUD

aws
Azure
Google Cloud Platform
Shared Security Responsibility Model

You are responsible for securing your data and workloads.

Varies by layers
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

Moving towards a “Security as a Service” model with approved AMI marketplace

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

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

Enabling DevOps with automated agent deployment via Azure Security Center
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
“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
- Integration between Service Now and Qualys

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

November 16, 2018
QSC Conference, 2018
A Beverage MNC Company

Qualys Automation within Azure Security Center

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
Cloud Perimeter Scan

Launch DNS based scans on public instances auto selected from your account via connectors

Add Elastic Load Balancer DNS

Generate results with external only remote check vulnerabilities
Azure Connector in Asset View
Azure Scan Flow

Launch Cloud Scans on Azure Internal (Private) and External (Public) Virtual Machines Scanner

Launch by Virtual Machine ID and NOT by IP

Report by Virtual Machine IDs
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 Workload Security with Qualys

- IaaS
- PaaS*

* 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

Google Security Command Center – Beta in December 2018

Other Integrations
IBM Security Center
- Dec 2018/Jan 2019

Alibaba Security Center
- Q1/Q2 2019
Qualys Cloud Apps in AWS Marketplace

- Vulnerability Mgmt.
- Policy Compliance
- Web Application Scanning

Soon...
- Web Application Firewall
- Cloud Security Assessment
- Container Security
- File Integrity Monitoring
- Indication of Compromise
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 S3 buckets which have the keys stored are opened up to public

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

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 Assessments

Unparalleled Visibility and Continuous Security Monitoring across public cloud infrastructure
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

Use Case
Identify the S3 buckets which have the keys stored are opened up to public

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
Cloud Inventory
Cloud Security Assessment

What is my public cloud usage?
What is my security posture?
Do I have any publicly accessible security accounts?
Are my security groups opening unauthorized access to internet?
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
Qualys Cloud Inventory and Security Assessment

Key Capability

Visibility into your public clouds
Get topographic view of your cloud inventory (AWS, Azure, GCP)

Continuous security monitoring
Monitor against security standards. Identify threats from misconfigurations (AWS, Azure)

Actionable Insight & threat prioritization
Prioritize by understanding association with exposures linked to vulnerable instances, network placement.
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
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

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
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

Coming Dec’18

November 16, 2018
QSC Conference, 2018
Qualys Cloud Security – Comprehensive Coverage

* PaaS – Cloud Database Scanning – Roadmap 1H '19
** CSA– Google (Q4’18), IBM, Alibaba, 1H -2H ’19
Customer Sessions - Thursday

10:00 – 10:35 AM
Using Real-time visibility to unify security event response

2:50 – 3:25 PM
Security Best practices enable a DevOps data transformation in the cloud
Thank You

Hari Srinivasan
hsrinivasan@qualys.com
The Big Migration... in security, it is happening.

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

DevSecOps
Secure Development and Deployments