



# Expand your cybersecurity program with complete visibility

Mark Holub  
Compliance Security Solutions Architect

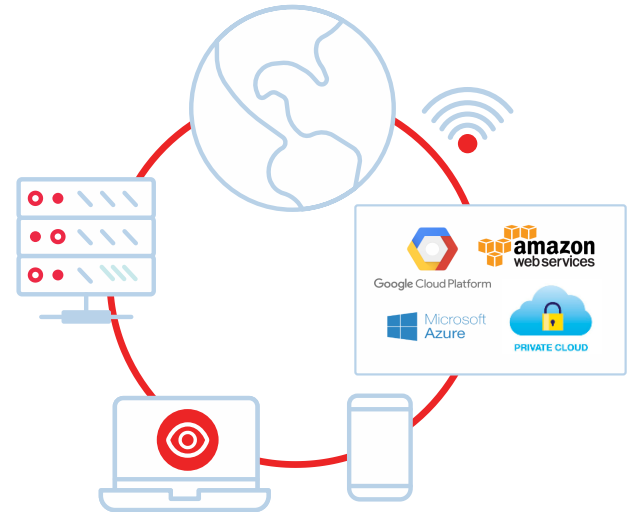
October 2019

# Digital Transformation

More than just adopting new technology

Powered by IT innovation

Security can't be after thought



# Digital Transformation

## Cloud Infrastructure

More of IaaS & PaaS

But still running your code



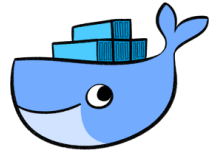
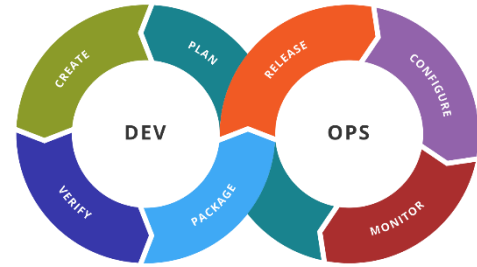
# Digital Transformation

## DevOps Innovation

Cloud Migration  
Container Revolution



Scale & Elasticity



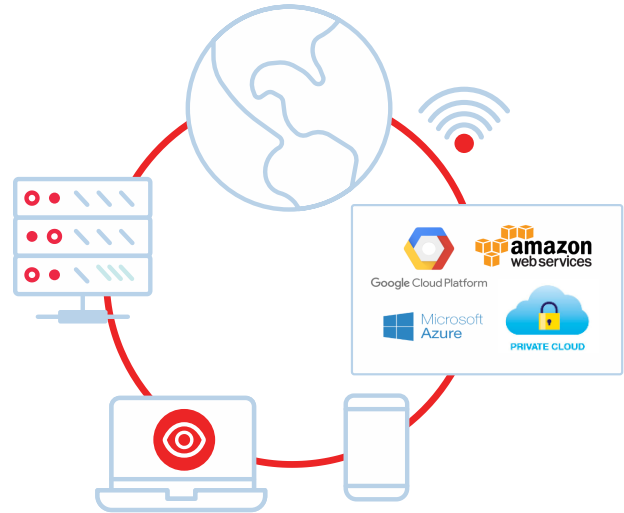
# Digital Transformation

## What about Security?

DevSecOps!

More Dev than Sec or Ops

Built-in not bolted-on



# Journey into the Cloud

## Hindered by the Silos



Datacenter Infrastructure Security



Corporate User Endpoint Security



Cloud Security



Web Application Security (AppSec)



CI/CD security automation  
(DevOps/DevSecOps)



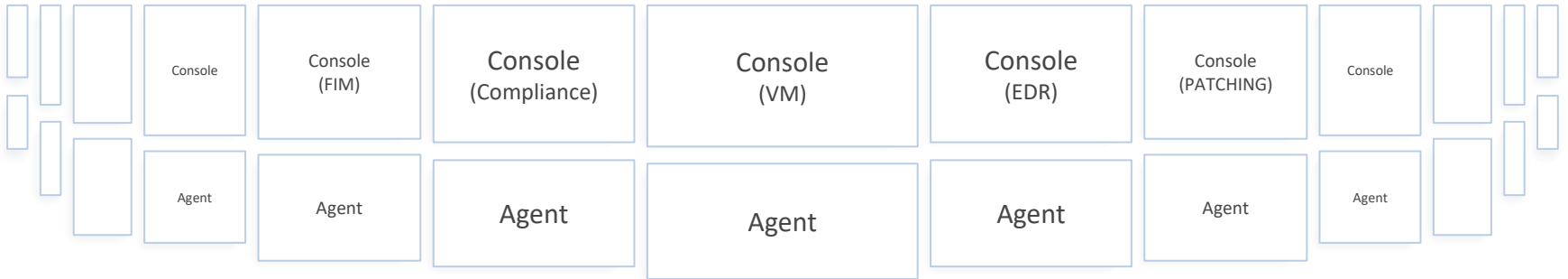
IT Asset Configuration Compliance & Audit



# Multiple Point Security Solutions

## Both Legacy and Next-Gen

SIEM



# Single Pane of Glass (Desire)





# Single Pane of Glass (Reality)



# Qualys Cloud Platform

Unified approach to detection,  
prevention & response across on-  
premise, cloud and endpoints

## On-Premises



## Endpoints



## Cloud



## Container



# End-to-end Security Architecture

## Automated Continuous Monitoring & Response



### Discovery

On-Prem  
Cloud  
Mobile Devices  
OT/ICS  
IoT  
CMDB  
Inventory



### Prevention

Security Hygiene  
Vulnerability  
Assessment  
Threat Prioritization  
Patch Management  
Configuration  
Assessment



### Detection

Endpoint Activity  
Cloud Infra Monitoring  
Network Activity



### Response

*Security Orchestration*  
*Incident Response*  
*Quarantine*  
*NAC*

# 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

**Agentless + Agent Based + Passive**

# Qualys Cloud Apps

## ASSET MANAGEMENT

**AI** **Asset Inventory**  
Discover, normalize, and catalog all global IT assets

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

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

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

## IT SECURITY

**VM** **Vulnerability Management**  
Continuously detect and protect against attacks, anytime, anywhere

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

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

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

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

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

**PM** **Patch Management (March GA)**  
Select, manage, and deploy patches to remediate vulnerabilities

## COMPLIANCE MONITORING

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

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

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

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

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

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

## WEB APPLICATION SECURITY

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

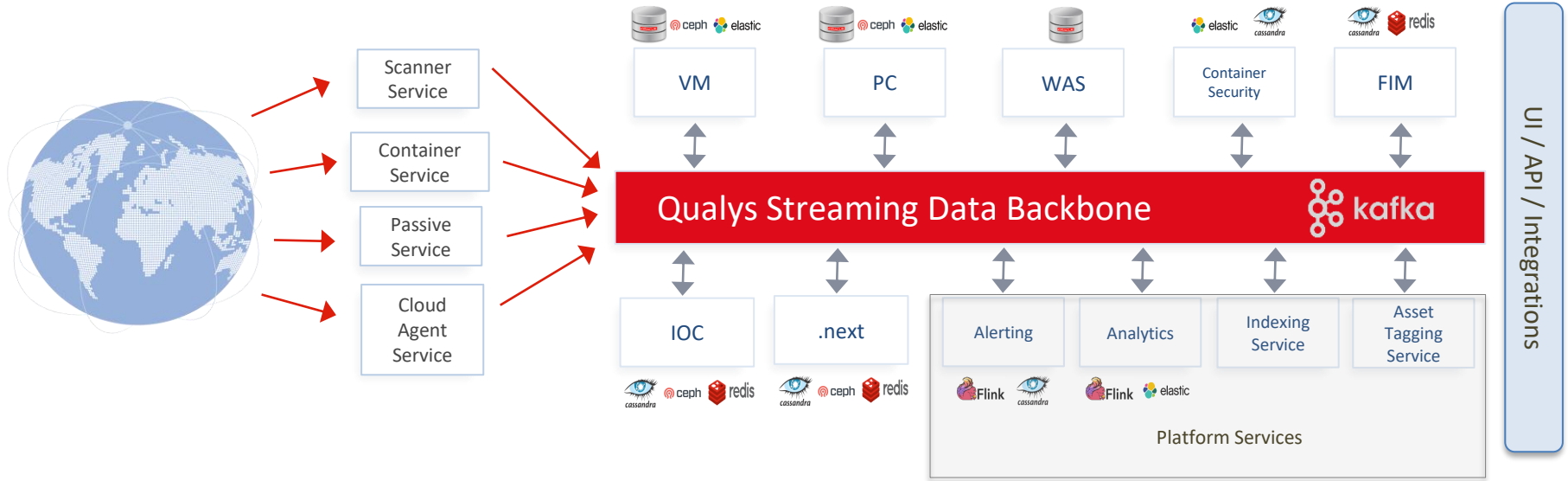
**WAF** **Web Application Firewall**  
Block attacks and virtually patch web application vulnerabilities

Available on Cloud Agent

Free Service for External

# Qualys Cloud Platform

## Scalable, Micro-services, DevOps



# Qualys Cloud Platform

## Unified approach to prevention and response

Integrated Suite of Applications



Analytics and Reporting Engines



Distributed Sensors



# Single Pane of Glass

Dynamic and customizable dashboards

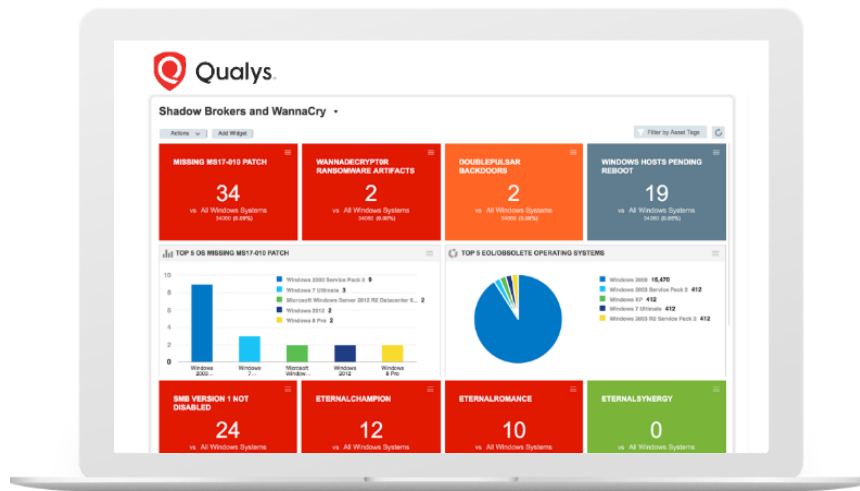
Centrally managed, self-updating, integrated Cloud Apps

1+ trillion

Security Events

3+ billion

IP Scans/Audits a Year



250+ billion

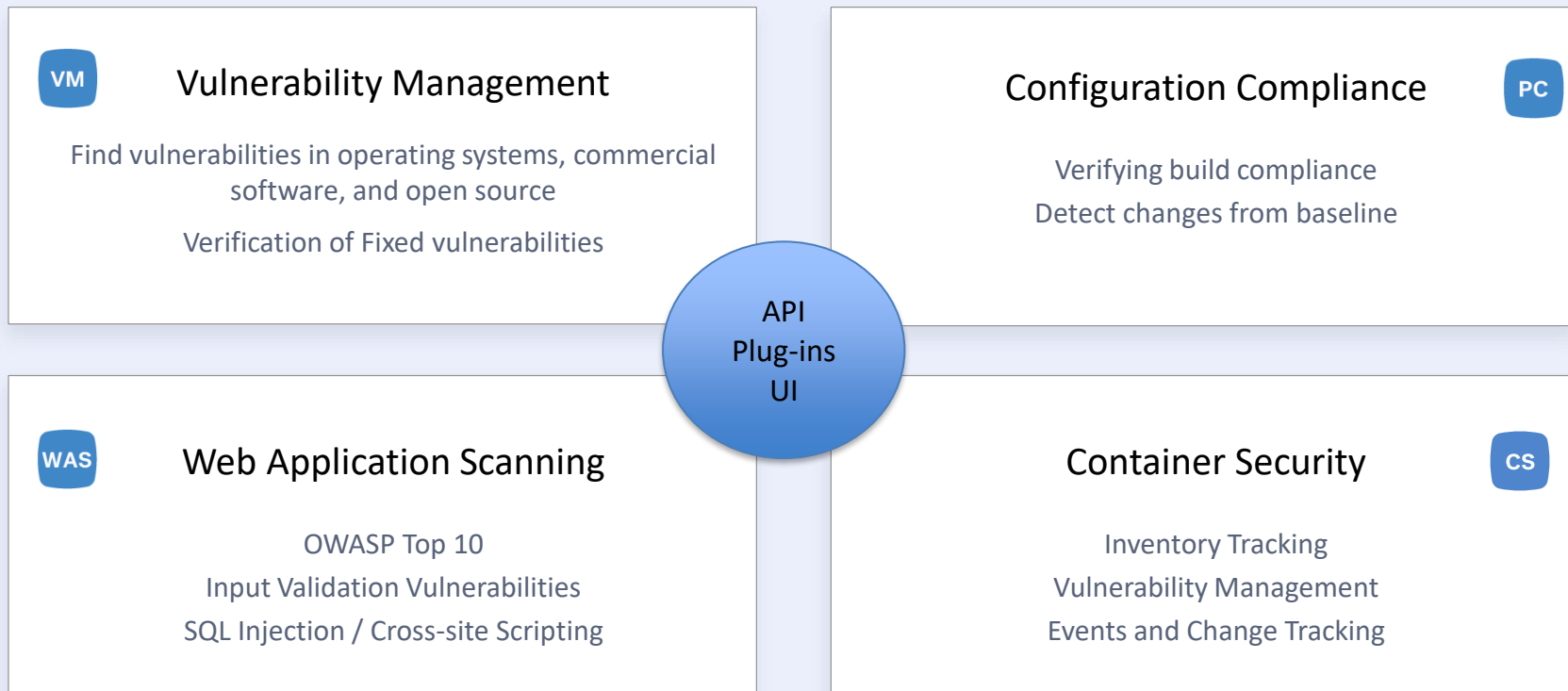
Data Points Indexed on  
Elasticsearch Clusters

99.9996%

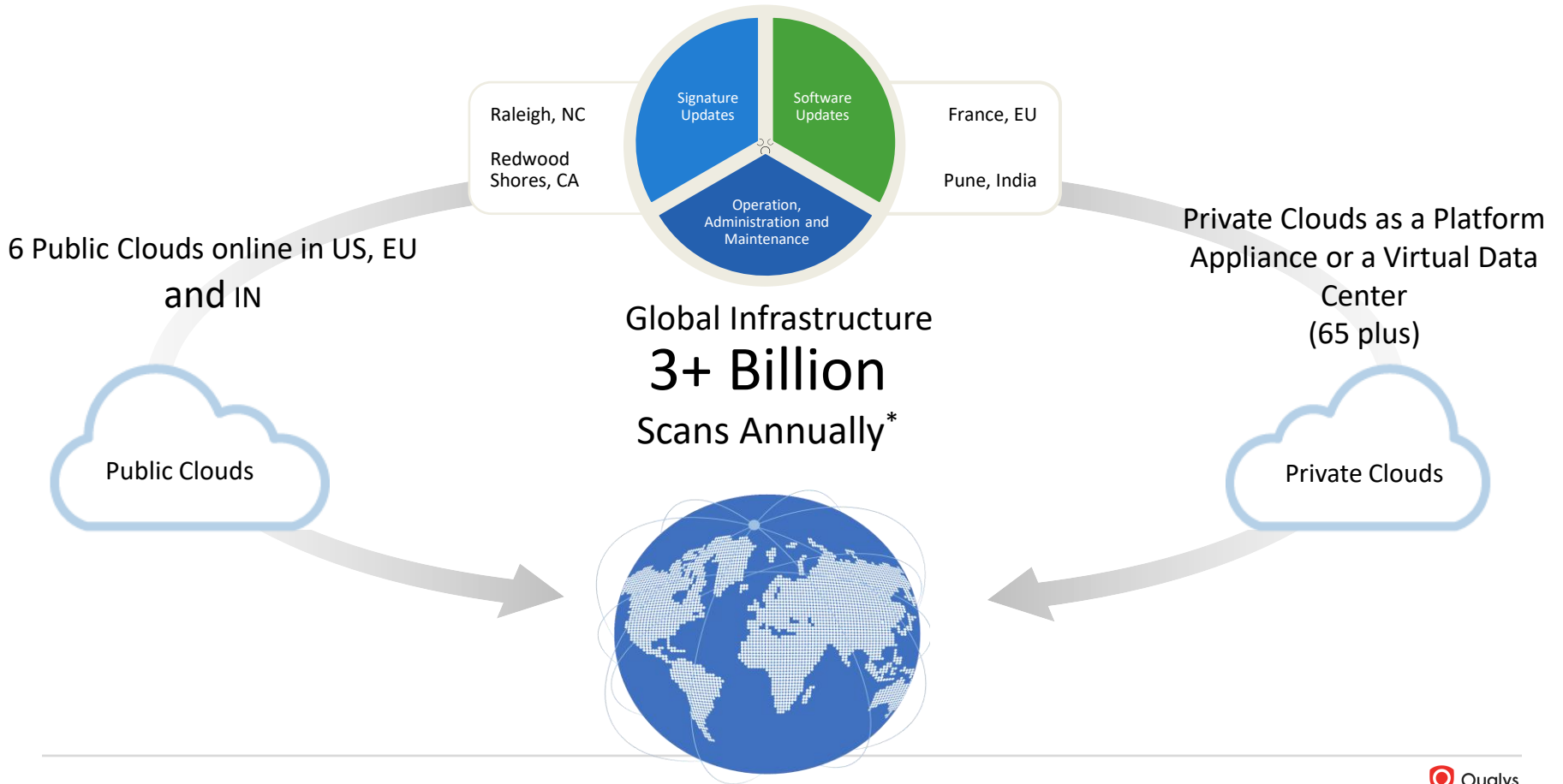
Six Sigma Scanning Accuracy



# Qualys Platform for Hybrid Cloud and DevSecOps



# Qualys Cloud Platform Operations



# Qualys Cloud Platform

A new unified to enhance your security program



2-second visibility across all of your global IT assets  
(on premise, endpoints and cloud assets)



Continuous assessment of your global security &  
compliance posture



Identify compromise-able and compromised assets



Consolidate all your security and compliance stacks



Secure your digital transformation



Drastically reduce your spend



Thank You

Mark Holub  
mholub@qualys.com