



Qualys Security Conference Dubai

Security at a Crossroad

Regaining our lost visibility

Sumedh Thakar

Chief Product Officer, Qualys, Inc.

IT Transformation

Infrastructure & Application

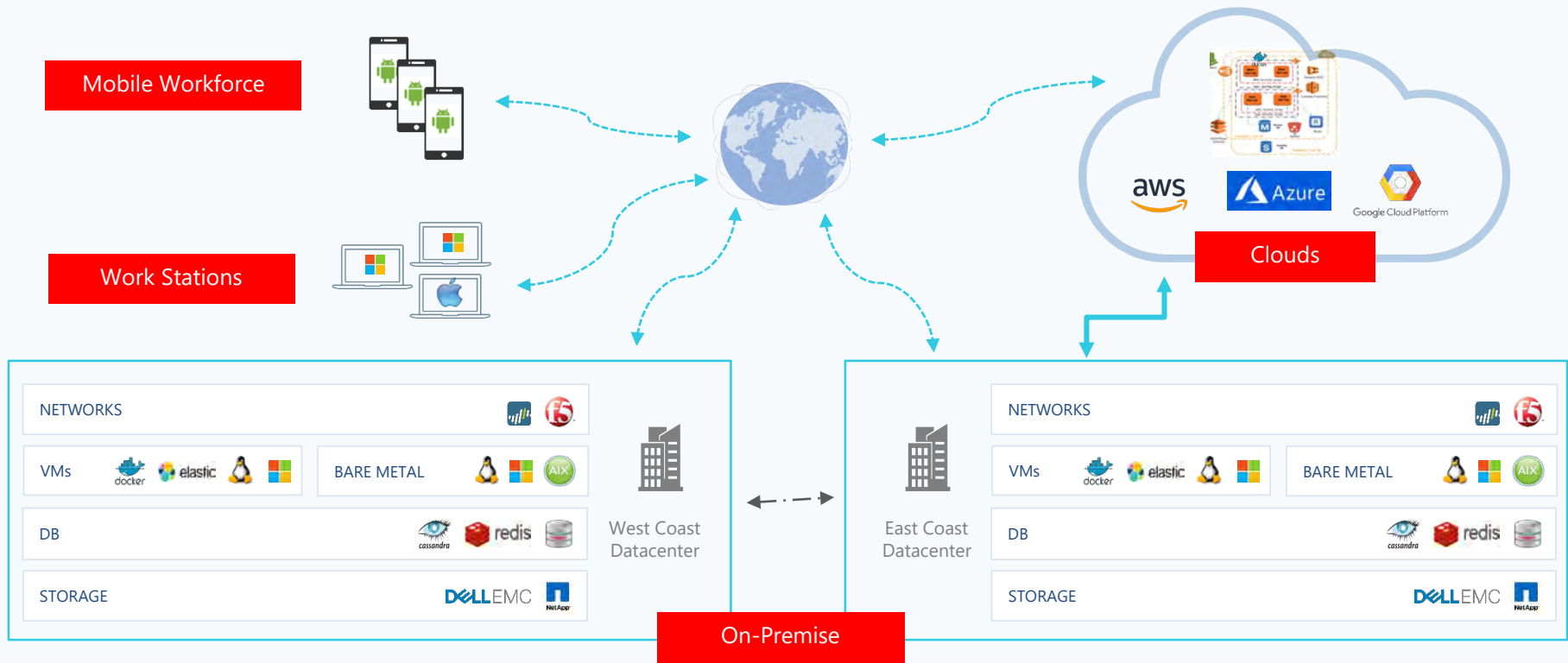
Digital Transformation

Holistic Transformation of Business to Digital

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



Hybrid Cloud Overview Architecture



Containers

Real game changer

Hypervisor disappearing, bare metal is back

Kubernetes Infrastructure-as-code



Containers – no servers?

Container-as-a-Service AWS Fargate

AWS Lambda function-as-a-service,
serverless!

Kubefed?

“Priceline” for Containers?

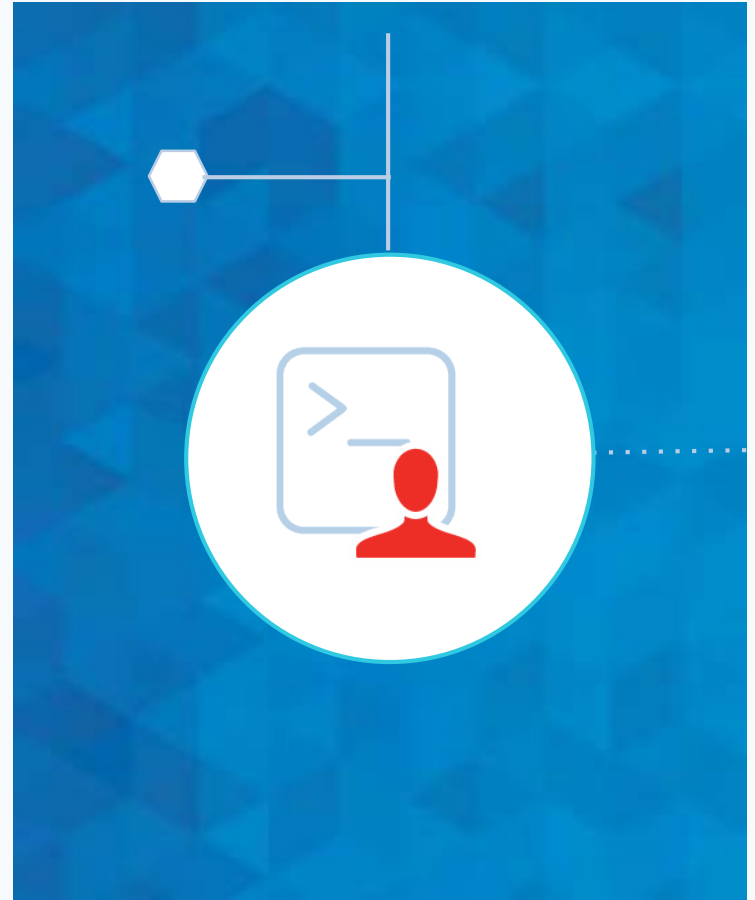


DevOps

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!



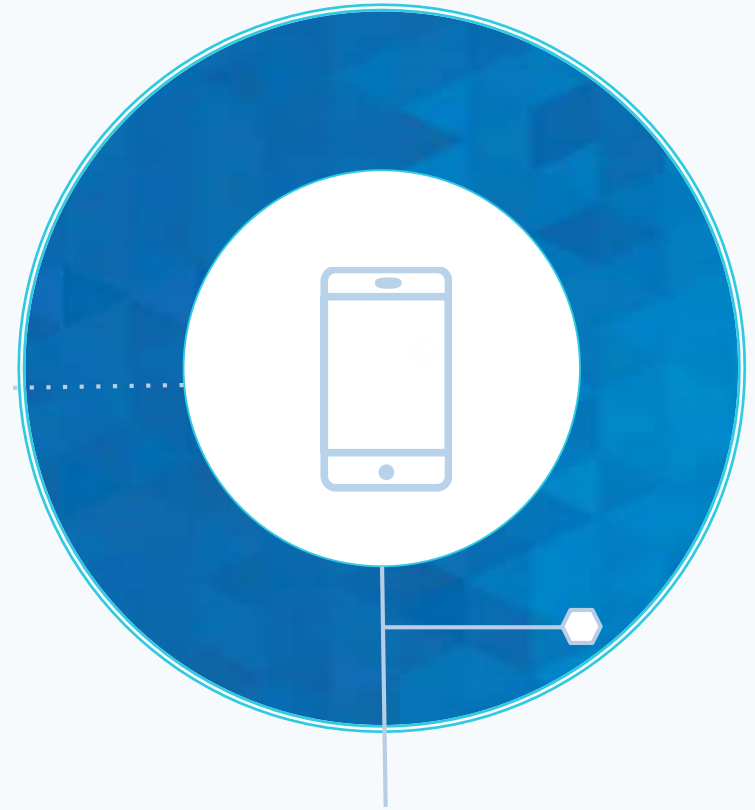
Enterprise Mobility != BYoD

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



Security



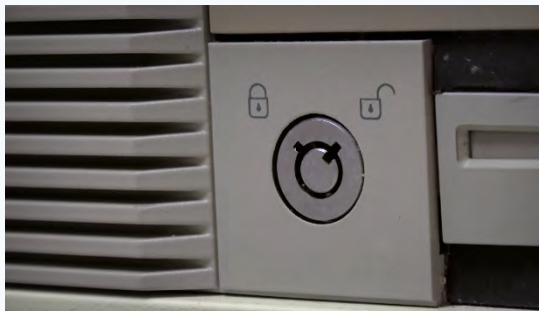
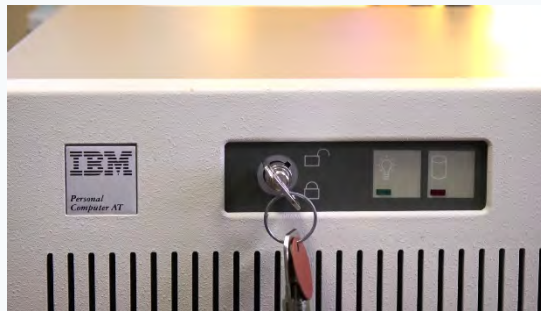
IBM PC AT

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

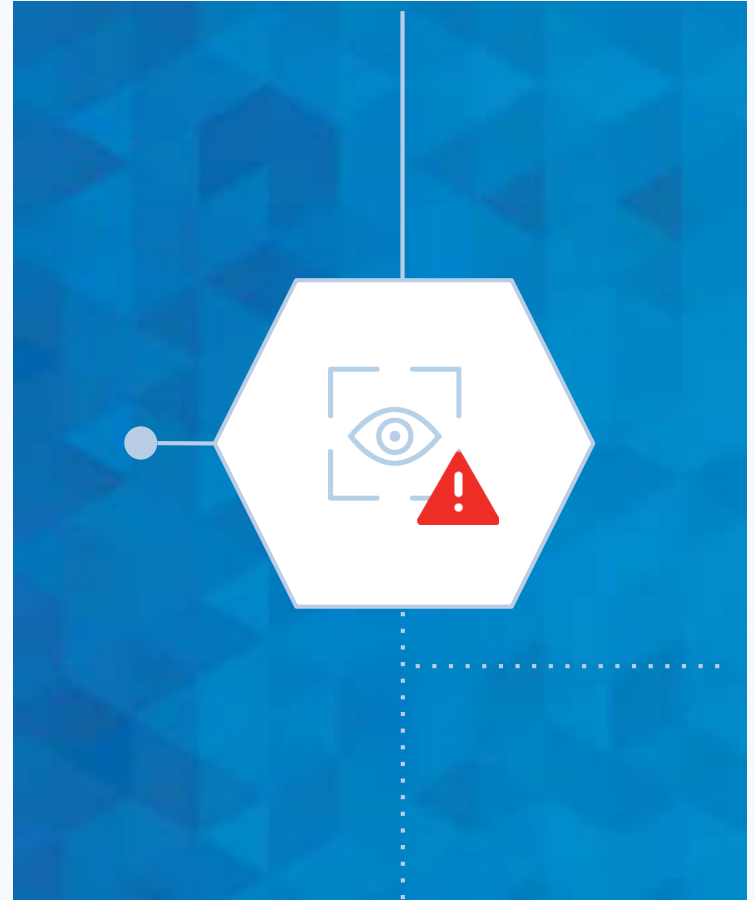
Still need to do Vulnerability & Configuration management

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

DevSecOps

Strict CI/CD pipeline controls

CI: Eliminate majority issues before prod

CD: Embed security artifacts in Image



Agile SecOps

SecOps focus on monitoring & response

Drastically reduce security solutions deployed after the fact

New generation of Security Analytics platforms – Data Lake



Qualys

Qualys Platform Approach

Embracing our own Digital Transformation

Massive expansion of backend for visibility – 2+ Trillion security datapoints indexed

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



Qualys Sensor Platform

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 Platform Approach

19 solutions on single platform .. and counting – reduced agent fatigue

DevOps friendly capabilities

Solutions for CI/CD

Extending solutions into remediation & response



Qualys Platform Approach

Rapid expansion of R&D org

Building dedicated Data Lake & Data
Science team

Key technology acquisitions &
Investments



Acquisitions & Investments

Nevis

Passive Scanning & Secure Access Control

Netwatcher

Event Correlation Platform

1Mobility

Enterprise Mobility

Layered Insight

Built-in Runtime Container Security

42Crunch Investment

API Security

Adya

SaaS Security and Compliance

Frog 1

Qualys Cloud Apps

ASSET MANAGEMENT

AI **Asset Inventory**
Maintain full, instant visibility of all your 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

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

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

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

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

PM **Patch Management**
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

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

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

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

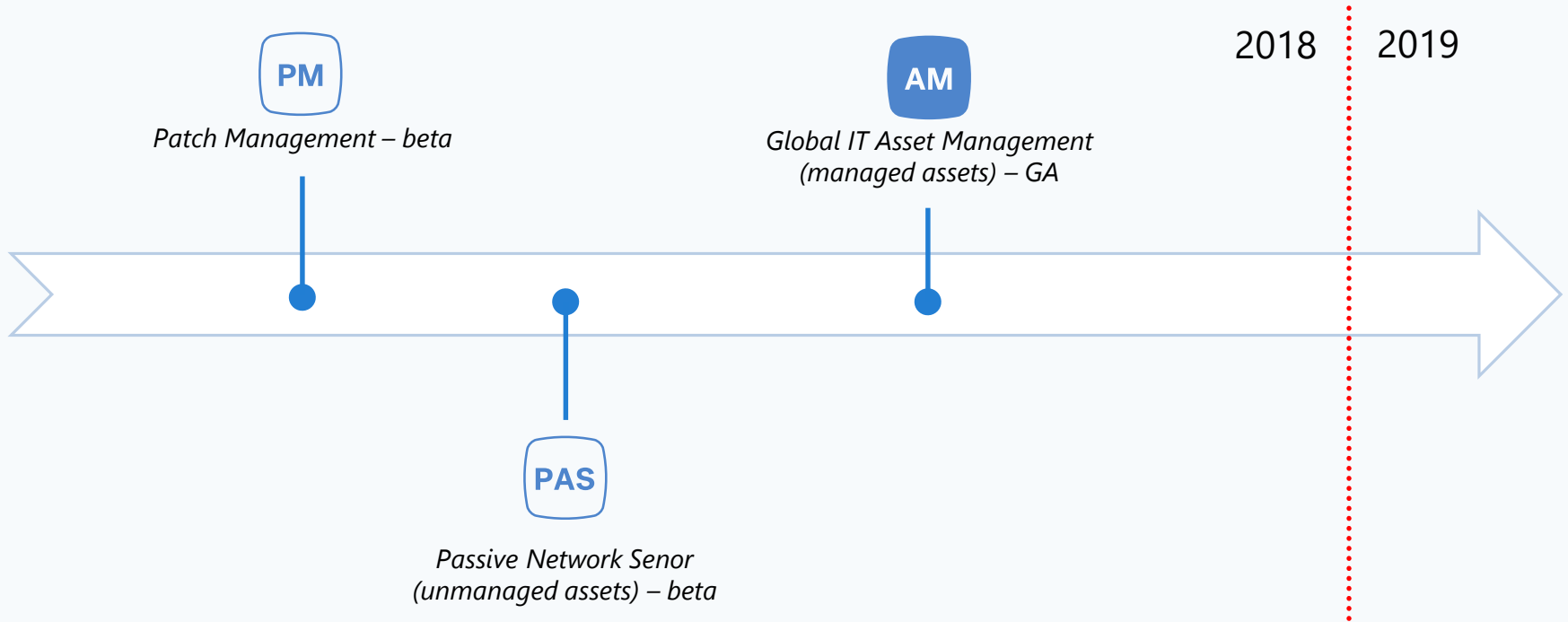
SAQ **Security Assessment Questionnaire**
Minimize the risk of doing business with vendors and other third parties

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

Q4 2018 releases



2019 – even more apps to come!

Patch Management – GA

Passive Sensor – GA

Secure Enterprise Mobility

Secure Access Control

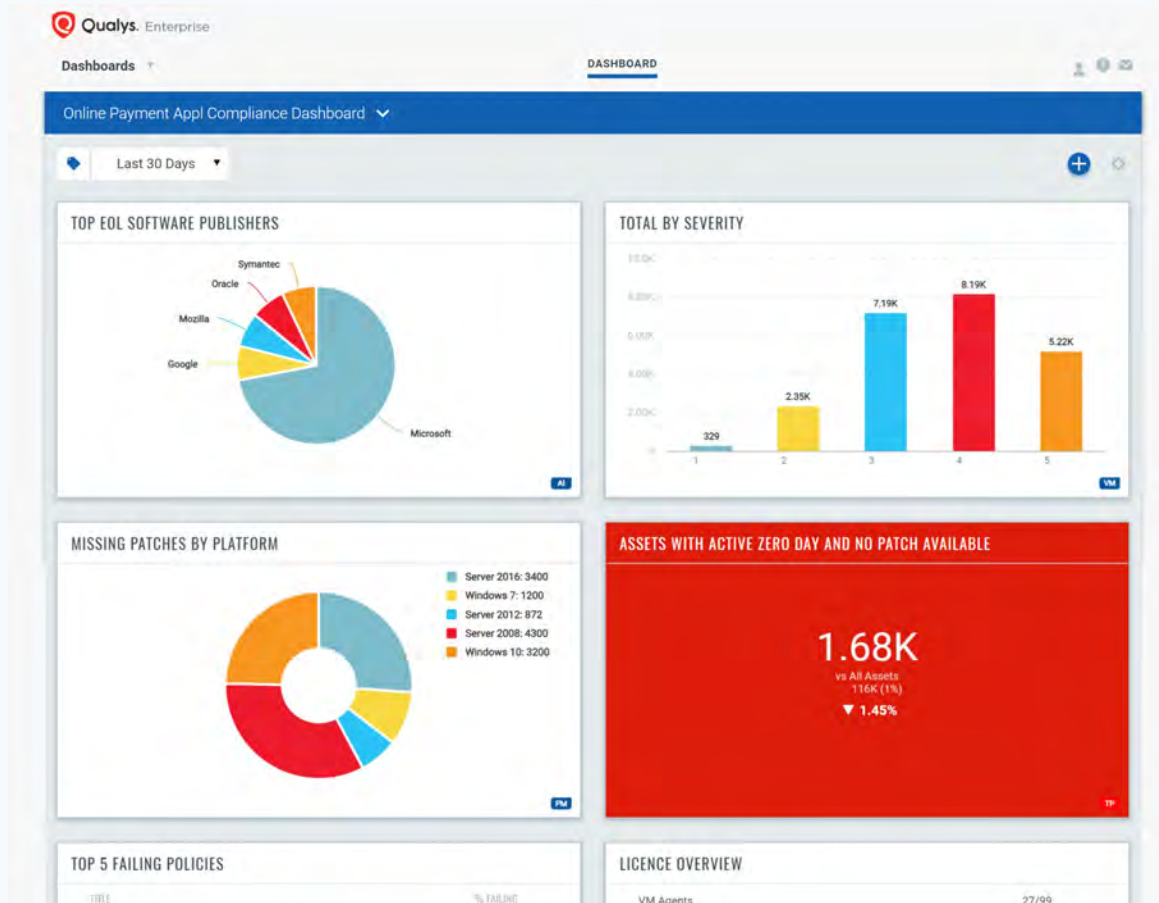
API Security

Software Composition Analysis

Breach and Attack Simulation

Security Data Lake & Correlation Platform

Unified Dashboards



DEMO

It's the Platform!
(a real one)

Cloud Platform Environment

Security at scale on hybrid clouds

19+ products providing comprehensive suite of security solutions

12,000+ 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

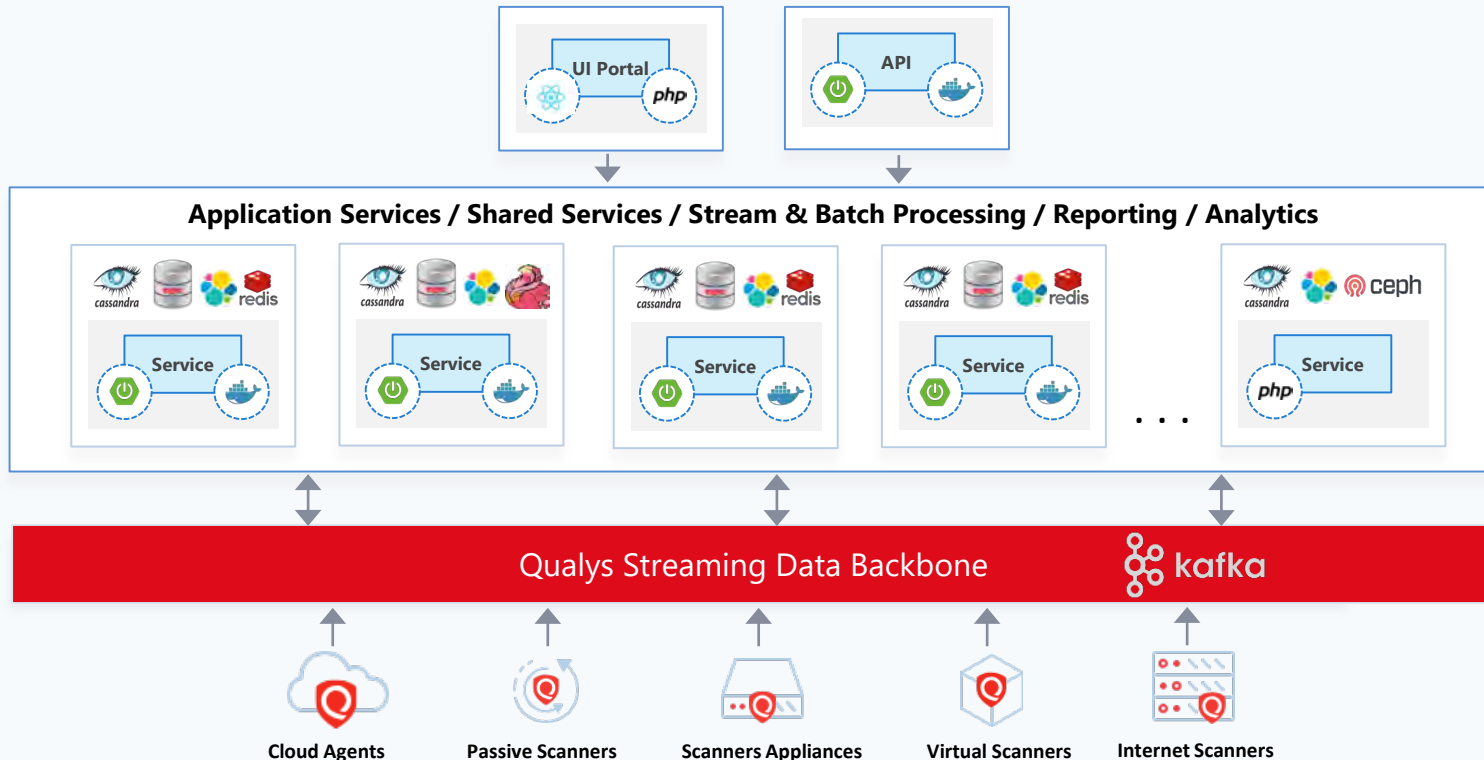
2+ Trillion data points indexed in our Elasticsearch clusters

Unprecedented 2-second visibility



Qualys Cloud Platform

Sensors, Data Platform, Microservices, DevOps



Qualys Cloud Platform

Integrated Suite
of Applications



Shared Services

Authentication
Service

Authorization
Service

Subscription
Service

Indexing
Service

Data Sync
Service

Tagging
Service

Messaging, Data,
Analytics Platform



Infrastructure and
DevOps Toolchain

Logging

Monitoring

Config Mgmt.

Service Registry

CI/CD

Docker/
Kubernetes

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



Network



Security



Server



End Point

CA

VM

AI

PC

IOC

WAS

WAF

Qualys Apps



Apps



Cloud



Users



IoT

Qualys Quick Connectors



Thank You

Sumedh Thakar

sthakar@qualys.com