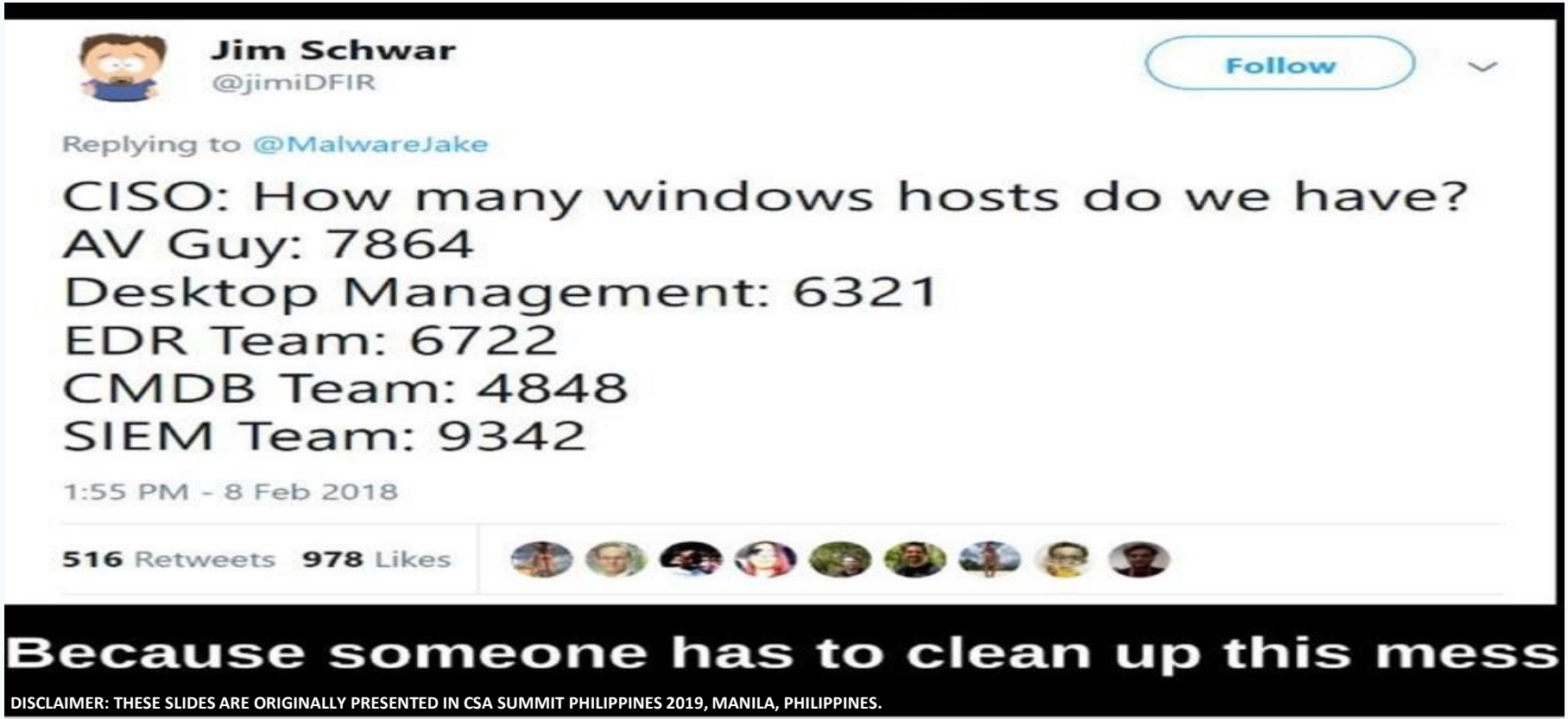
Seeing the rainbow through the clouds - Solving Visibility challenges in the cloud

Regaining our lost visibility

Deb J (DJ)
CTSO, Qualys, Inc.

Why do we need right visibility?



Need for the right visibility?

Do you know :

- All your workloads across all aaS?
- Servers running an expired cert?
- What you have in your environment?
  - Adobe, Chrome, Java…
- Bittorrenting?? CoinMining??
- EOL vs EOS / Open Source vs Commercial
- Vulns vs Patch
- Ports vs Services
- Easily exploitable vulns

Visibility – Depth & Width

Right visibility can solve :

- **87%** - Lack of cloud visibility is obscuring security threats
- **95%** - Visibility problems led to application/network performance
- **38%** - Insufficient visibility as a key factor in application outages
- **31%** - Insufficient visibility as a key factor in network outages.

Interestingly, **99%** of respondents identified a direct link between comprehensive network visibility and business value. This shows visibility contributes directly to the business bottom line.

A full **86%** of respondents also stated visibility was important for network and application performance monitoring, and **93%** stated it was valuable for security.

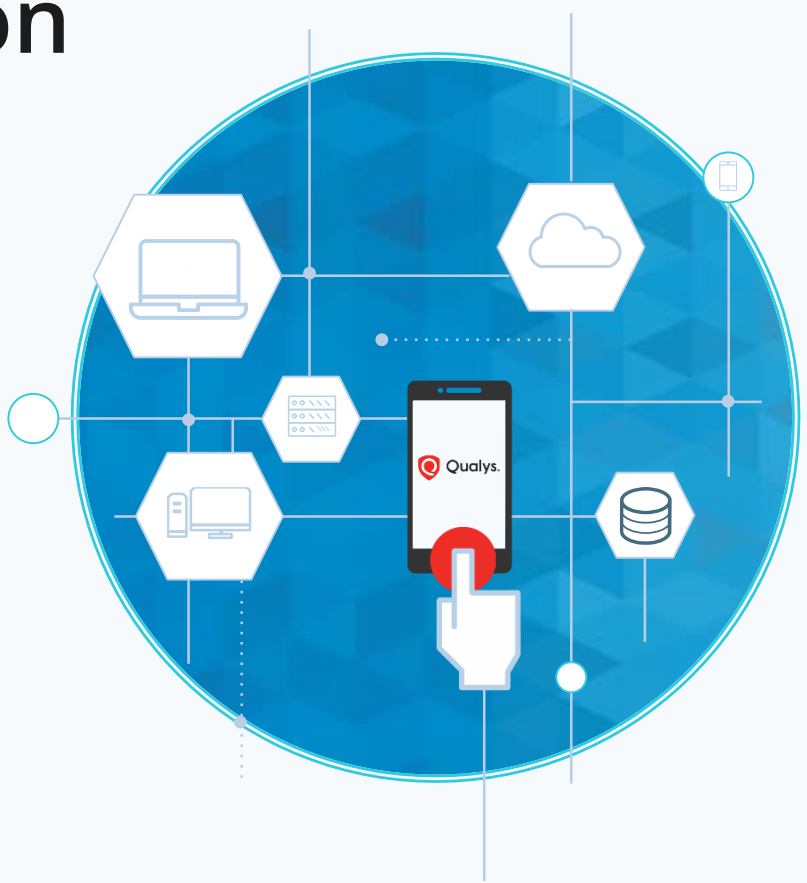
Everything is an inventory

- Organization
- Directories
- Vulnerability
- Compliance

What caused the visibility challenge?

Digital Transformation

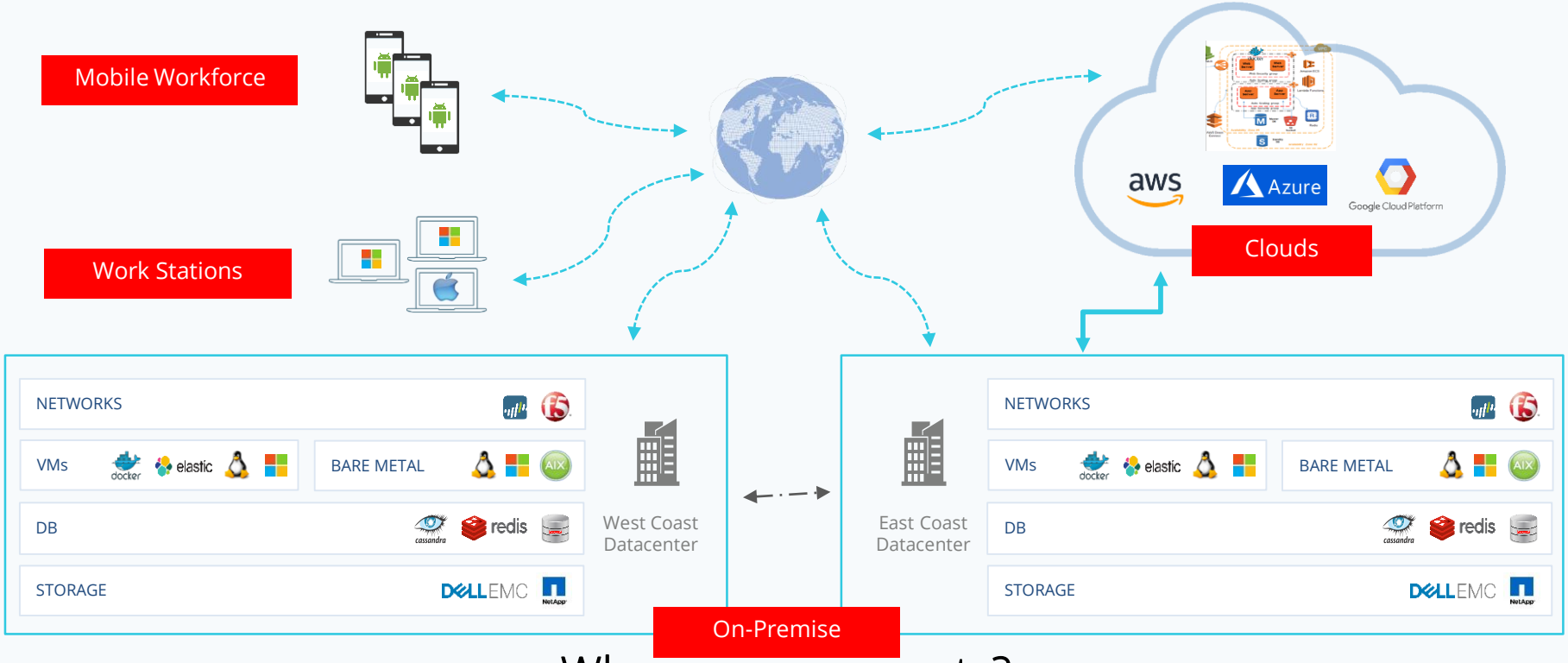
Holistic Transformation of Business to Digital



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

Qualys.

Hybrid Clouds



Where are my assets?
Is Software, App and API an asset too?

Qualys.

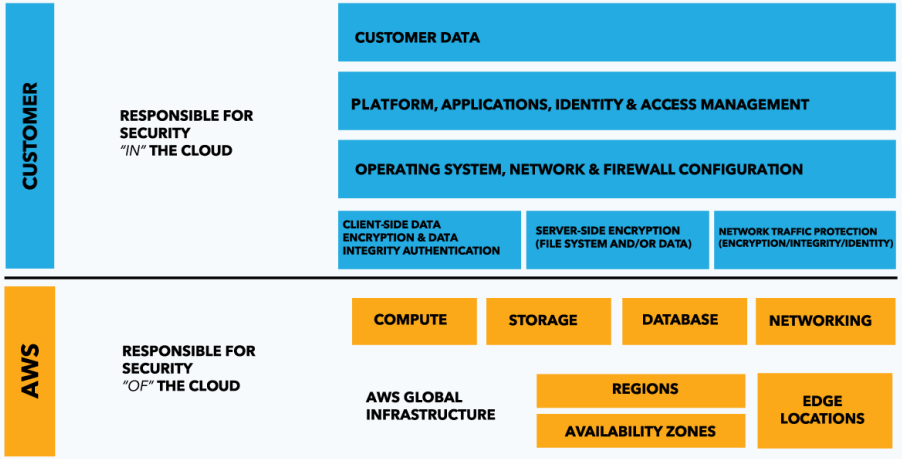
Shared Security Responsibility Model

You

are responsible for securing your data and workloads

Cloud

Is just a new address of your assets.



Qualys.

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 brings more assets

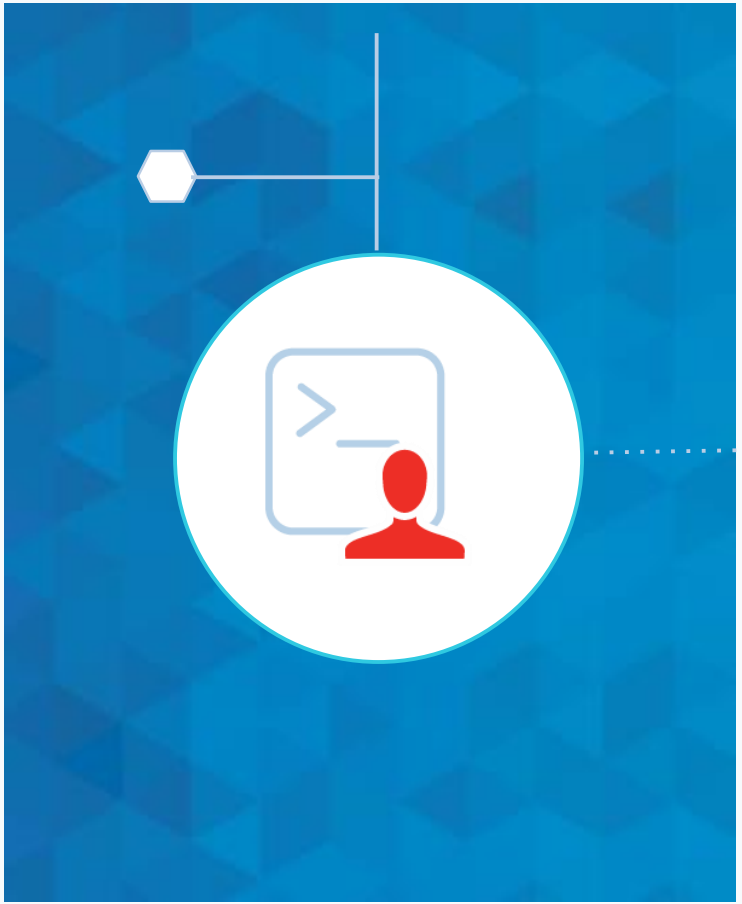
This is real and highly contagious

Developer decides how infrastructure runs in production

Speeds up significantly how fast code goes to production

The DevOps ToolChain

(Track, Build, Manage, CI-CD, Run)



On-Prem

Shrinking Datacenter Footprint

Corp IT – more distributed & mobile

More IoT!

ICS & OT security is now CISO ownership.

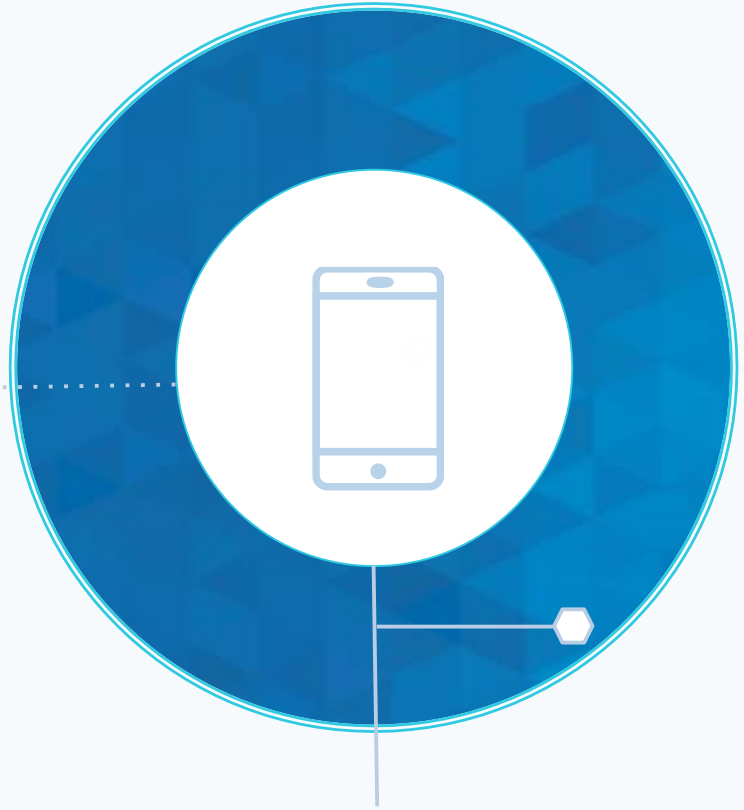
Enterprise Mobility != BYoD

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 in-humans

SaaS

Cover your aaS

No infrastructure to manage

No Applications to code or manage

CASB Managed assets

2017-2019 - Cloud centric attacks

verizon

VIACOM

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

REPUBLICAN NATIONAL COMMITTEE

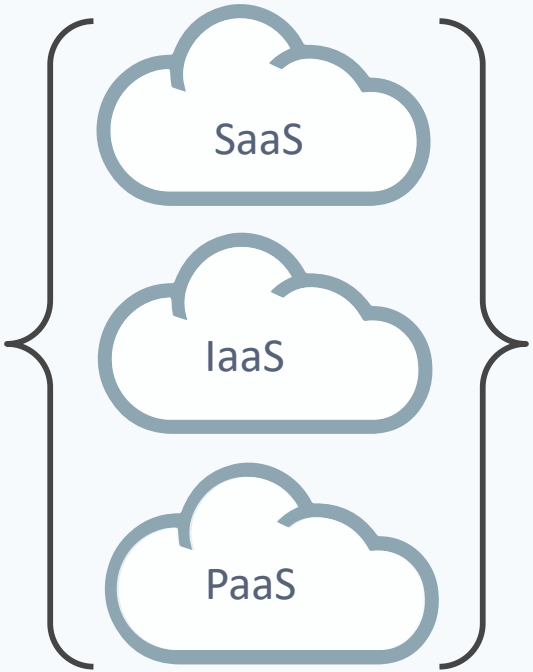
TESLA

ABC CORP. AUSTRALIA

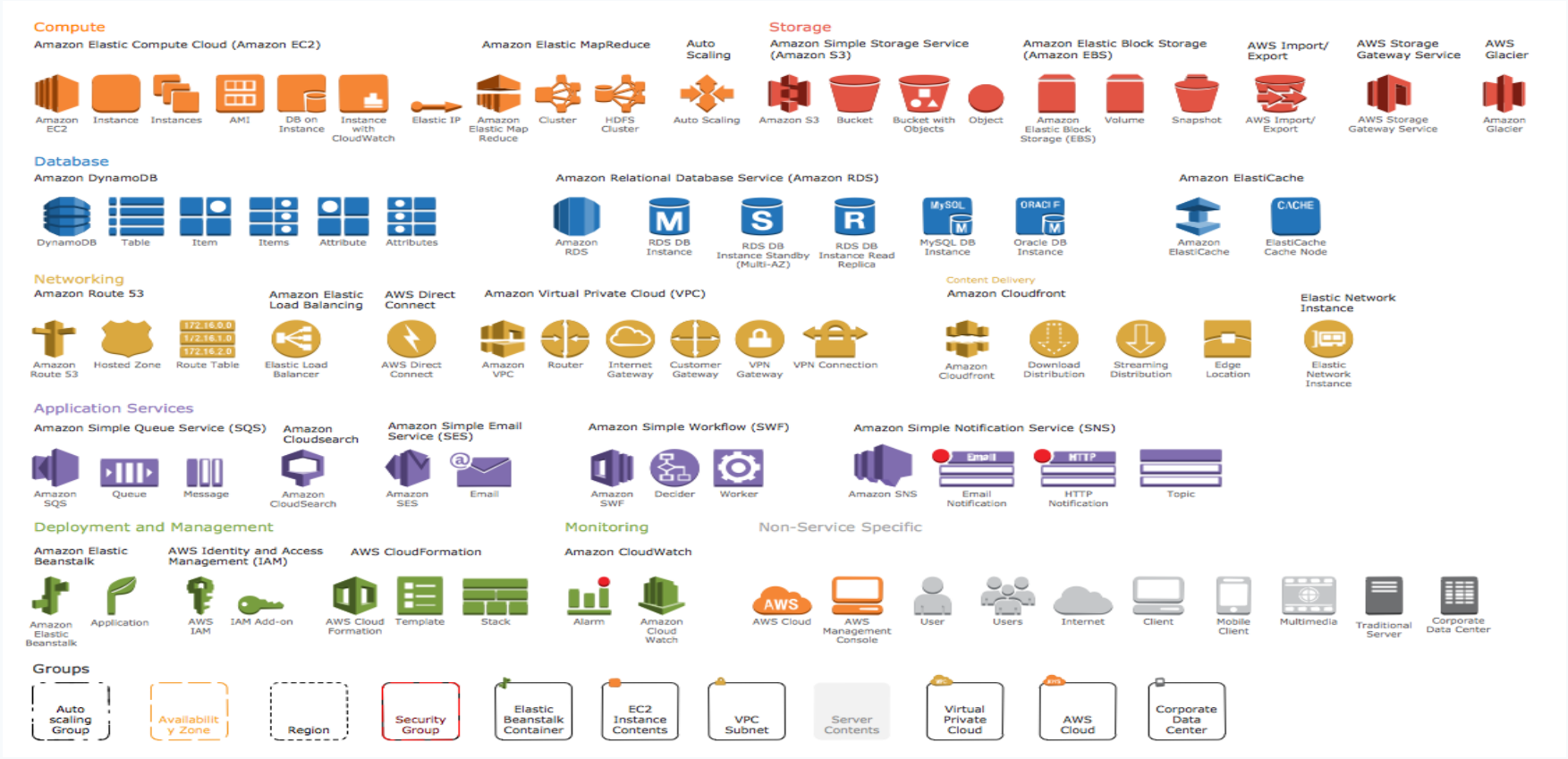
DOWJONES

CapitalOne

Cover your *aaS



We use more resources than we know



Qualys.

Challenges of visibility on 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

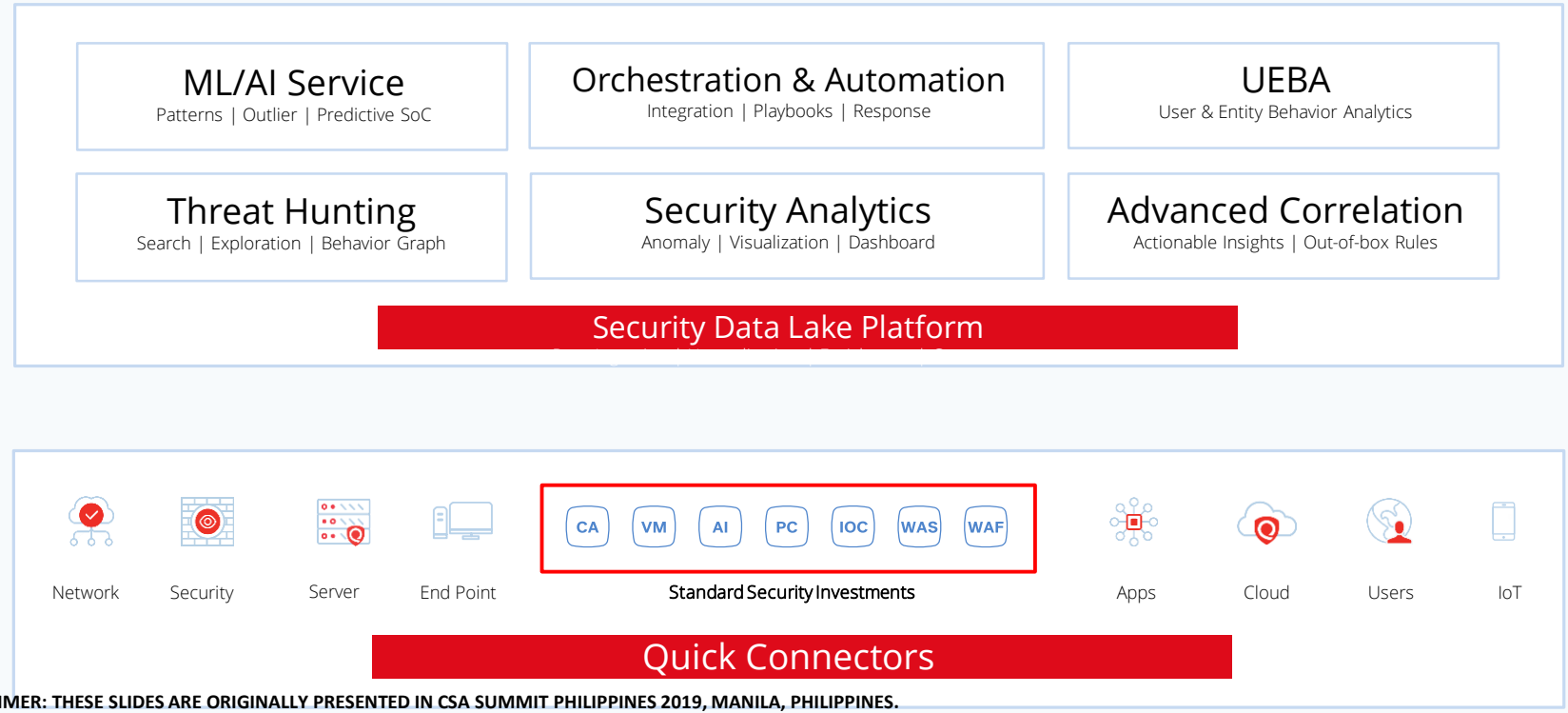
Still need to monitor integrity of systems (?)

More data incoming into “SIEM” deployments

Basically no visibility to respond

Compliance demands on new infrastructure

Bring More Visibility
Advanced Correlation & Analytics



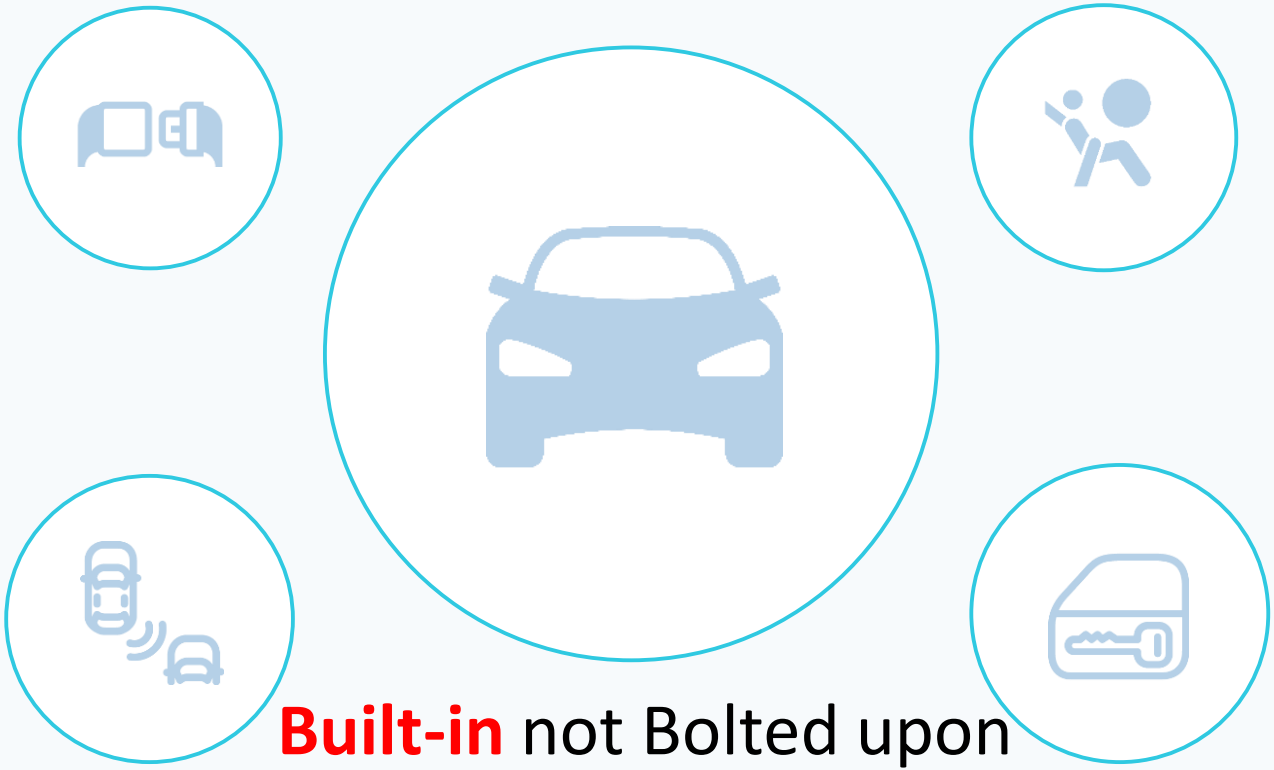
Qualys.

Digital Jobs in the future
(Completely untraditional meaning of assets)

- Genomic Portfolio manager
- AR/VR Specialists
- Nano Medic
- Waste Data Handler
- Digital Detective
- Thought Hacker
- 3D organ Designer
- Man-Machine Teaming manager
- Digital Identity Cop

Successful ways to improve visibility & reduce problems

Make your approach more **inclusive**



Built-in not Bolted upon

Consolidation is the name of the game now

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

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

Qualys.

Solving the challenge.

More metadata, more telemetry from assets

Ultra comprehensive asset inventory strategy

Built-in Automation and not bolted on

Starts in DevOPS and DevSecOPS

Embrace New generation of Security Analytics platforms

Vendor stack consolidation is must

Shift from automation to Orchestration

Good security must cover Scale, Precision and Accuracy

He can, but we can’t!

Reduce 50% of your problems by just snapping fingers……

Thank You

Deb J

dj@qualys.com

CTSO – APAC, ANZ & Japan

Qualys Inc