Qualys TotalCloud (CNAPP)

Unified Vulnerability, Threat and Posture Management

From Development to Runtime Across Multi-cloud

Nayeem Islam
Vice President, Product Management

What we see as key Market Trends

Looking Ahead

Posture (CSPM), Workload Protection (CWPP), Threat Detection (CDR), Container Security (CS)
Can we extend Cloud security with enterprise security function?

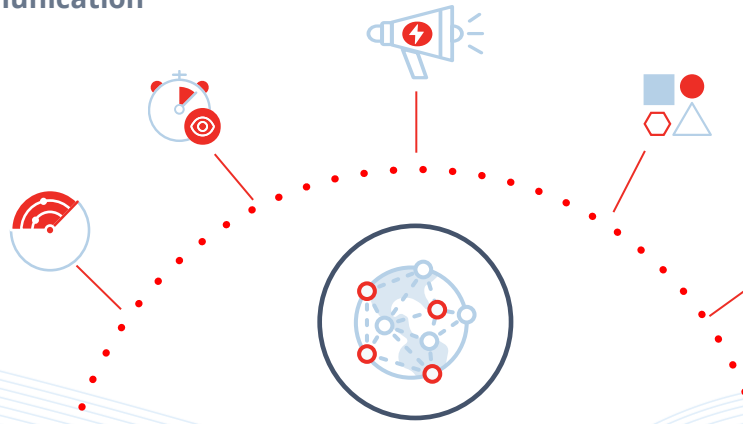
Convergence of Cloud Security

Many reports but **CIO & Board** need a view on **Cyber Risk Status?**

Board Level Risk Communication

Get More Security

End-to-end Security through integrated "mesh" of use cases, intelligence & automation
How can I get integrated actionable view



Too many vulnerabilities, misconfigurations, patches, and alerts.
What is my real risk?

Risk based Prioritization

ROI Driven Consolidation

Too many agents and tools, manual cost
How can I get better ROI from current investments

Qualys. | Get More Security

Key Market Trends

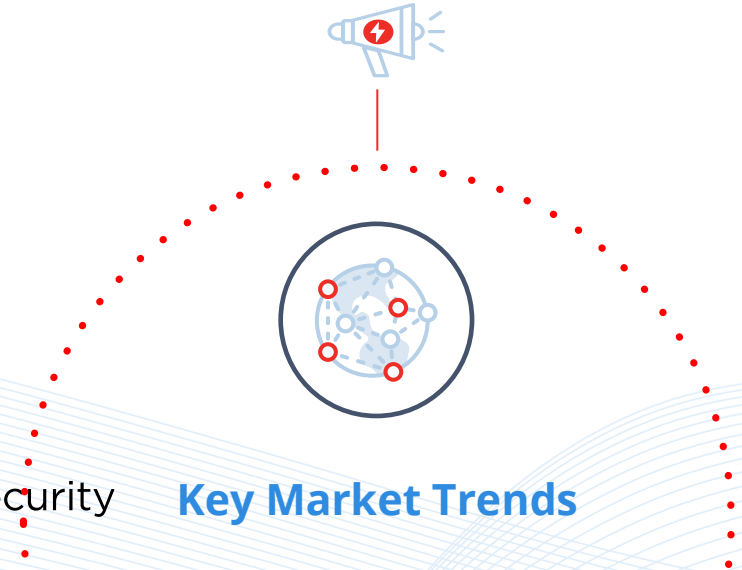
What we see as key Market Trends

Looking Ahead

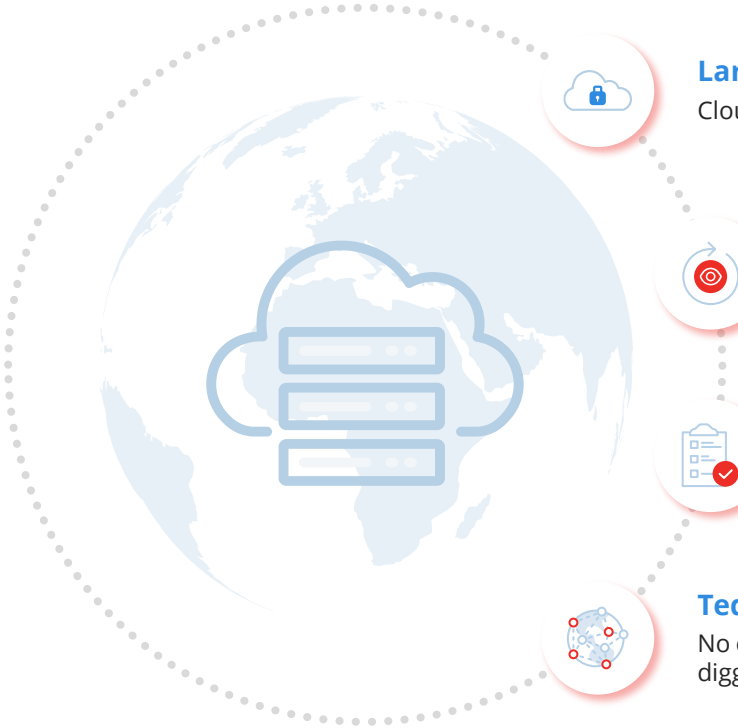
Posture (CSPM), Workload Protection (CWPP), Threat Detection (CDR), Container Security

Can we extend Cloud security with enterprise security function?

Convergence of Cloud Security



Cloud Security Is Challenging



Large & Dynamic Attack Surface

Cloud is a transient environment with ephemeral workloads across multi-cloud

Lack of Visibility

Difficult to get a complete view of the cloud environment

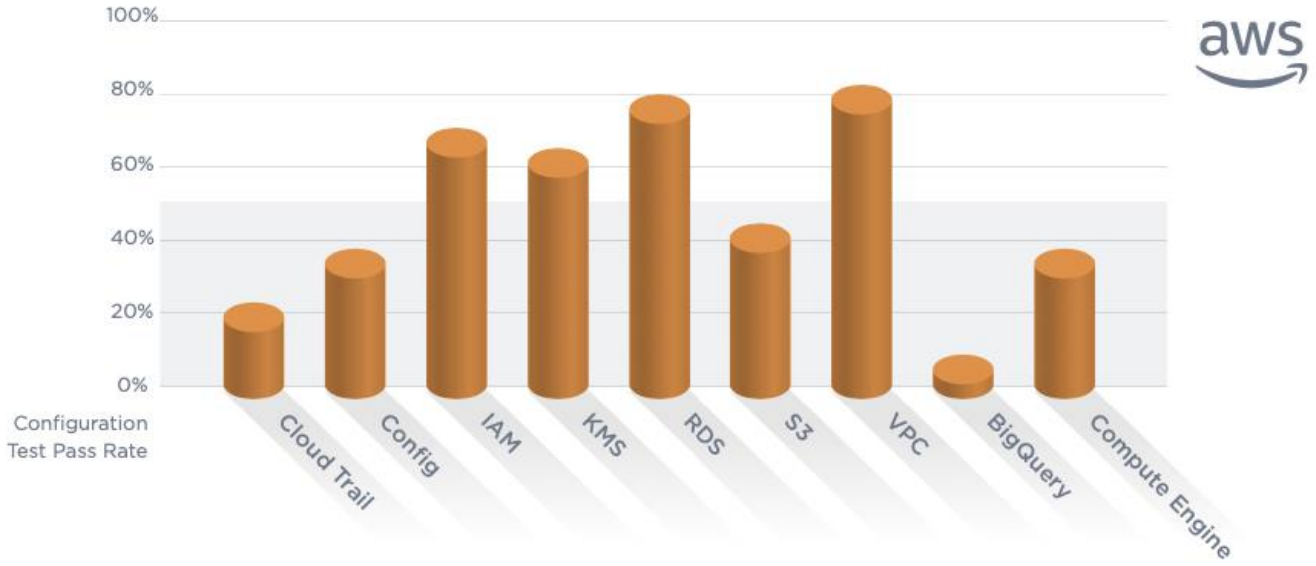
New Compliance/Benchmarks

New threats and vulnerabilities are constantly emerging in the cloud, requiring organizations to stay up-to-date

Tedious Remediation Process

No context around whether vulnerabilities are critical, and a ton of time is spent digging into multiple dashboards

Cloud Misconfigurations



Misconfigurations Leading to Ransomware

Failing Controls

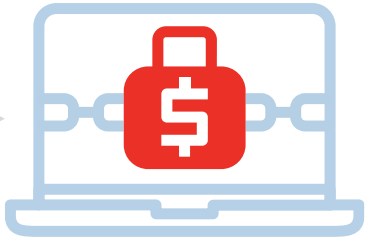
Top Cloud Techniques

1. T1210: Exploitation of Remote Services
2. T1485: Data Destruction
3. T1530: Data from Cloud Storage Object

Failing Controls

Top On Premise Techniques

1. T1110: Brute Force
2. T1021.001: Remote Desktop Protocol
3. T1548: Abuse Elevation Control Mechanism



Qualys TotalCloud

A Comprehensive CNAPP Solution

Unified Vulnerability, Threat and Posture Management from development to runtime

Qualys. | Get More Security

Qualys TotalCloud Differentiator

Fast Time to Value

Flexibility of Scanning

Choose the scanning method (**Snapshot, API,** Agent, Network) to get best coverage and continuous assessments

Highest Level of Accuracy

Six sigma Accuracy based on the Qualys custom DB and research **and risk prioritization**

Low TCO and Higer ROI

Flexibility to deploy - what you want, when you want it

Instant Protection

Detect unknown and known threats quickly **at runtime time using AI**

Qualys.

TotalCloud Differentiator: Flexibility of Scanning

Agentless and Agent-based scanning

Agent-based

Real-time comprehensive vulnerability, configuration and security assessment

Detect runtime threats but the challenge is to get access to all workloads to run agents

Network-based Assessment

Assess for network-related vulnerability

Continuous, no need to stop the workload to inspect it but at times, getting access to the workload could be challenging

API-based Assessment

Use CSP-provided APIs to collect software inventory and perform assessments

Fastest setup and assessment but lack of OSS coverage

Snapshot-based Assessment

Take snapshot of the workload and perform vulnerability assessment on it

Fast and easy setup without access to the workload but scanning is 24 hrs. due to resource limitations

Highest Level of Accuracy

Low false positives so you are not wasting time, effort, and resources addressing non-existent or low priority vulnerabilities

Low false negative reducing the risk of leaving systems vulnerable to exploitation by attackers

Unmatched accuracy of detection **powered by same backend**

- Agentless or agent, highly accurate because of our backend infrastructure

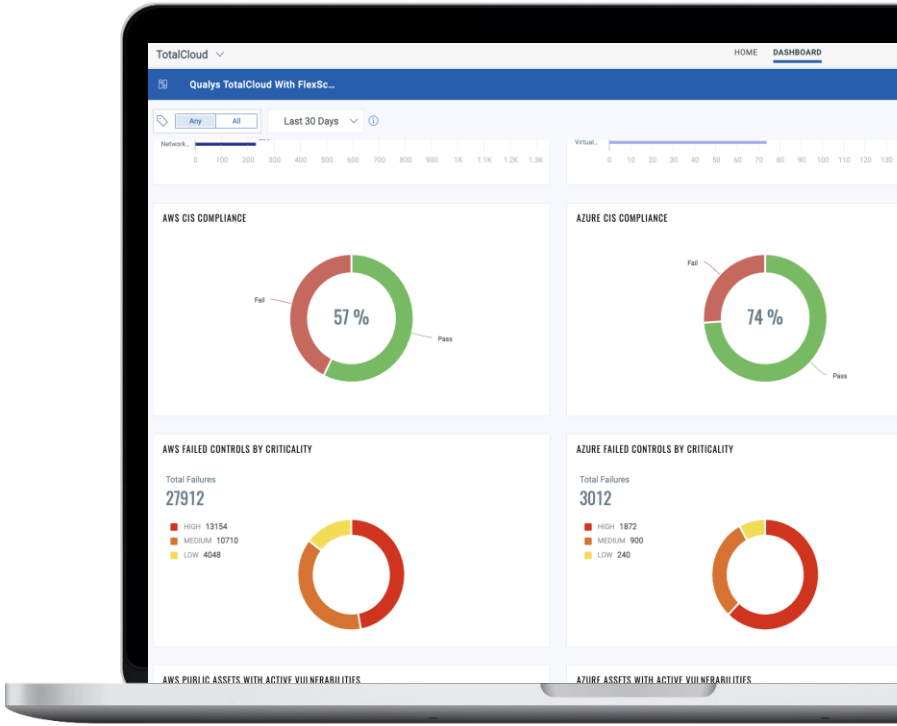
Cloud environment is dynamic, but our research moves even faster

- Dedicated Inhouse research, not open-source threat intel
- Over 100 dedicated security researchers with 2 decades experience

Cloud Security Posture Management

Comprehensive inventory of your public cloud workloads and infrastructure

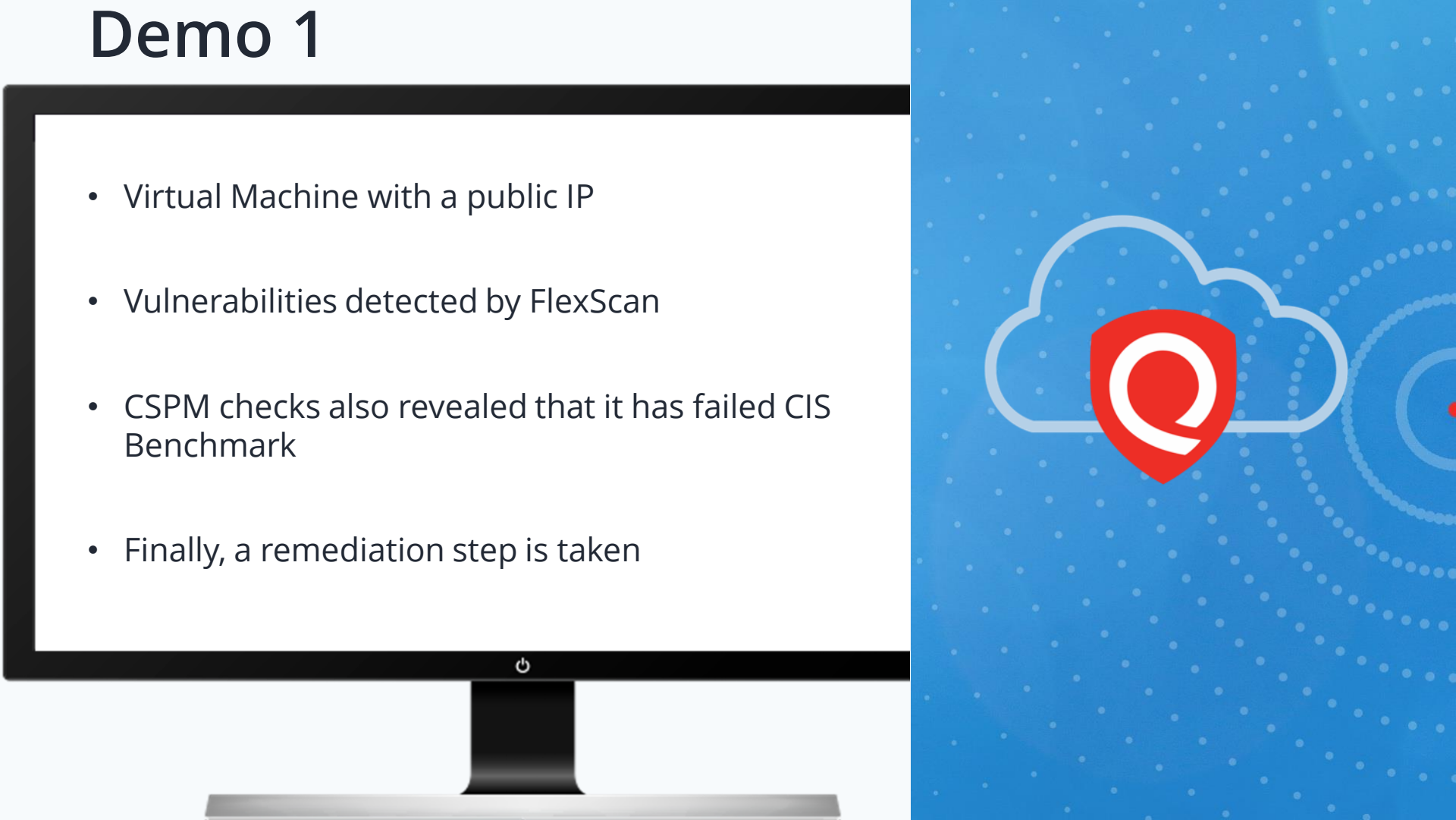
- Identify and remediate misconfiguration across 100% of your cloud assets
- 1000+ out of box controls including Qualys best practices and CIS standards
- Supports 30+ compliance mandates such as PCI DSS, and HIPAA and complete coverage of CIS benchmarks
- Automatically alert, ticket, or remediate misconfigurations
- One click remediation for many high visibility controls



Qualys.

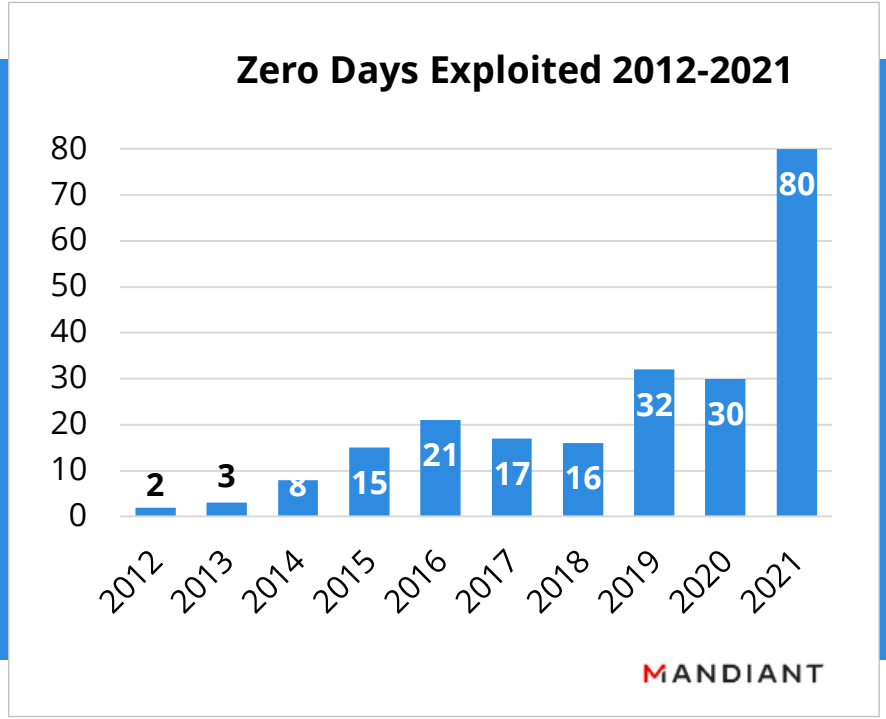
Demo 1

- Virtual Machine with a public IP
- Vulnerabilities detected by FlexScan
- CSPM checks also revealed that it has failed CIS Benchmark
- Finally, a remediation step is taken



More Zero-Day Exploits

250% Zero-Day Exploitation more than doubled from 2020 to 2021



Sources: NVD and Mandiant Threat Intelligence

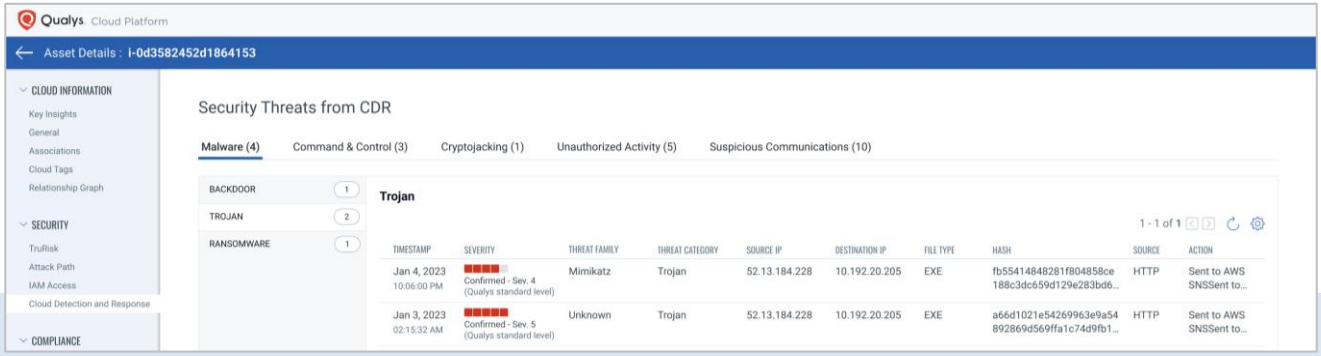
Qualys Cloud Detection and Response (CDR)

Our solution monitors cloud network and cloud activity logs which provide visibility and Qualys deep learning algorithms provides threat detection

Deep Learning AI detection are fast and accurate

- Malware
- Suspicious Communications
- Beaconing
- Unauthorized Activity

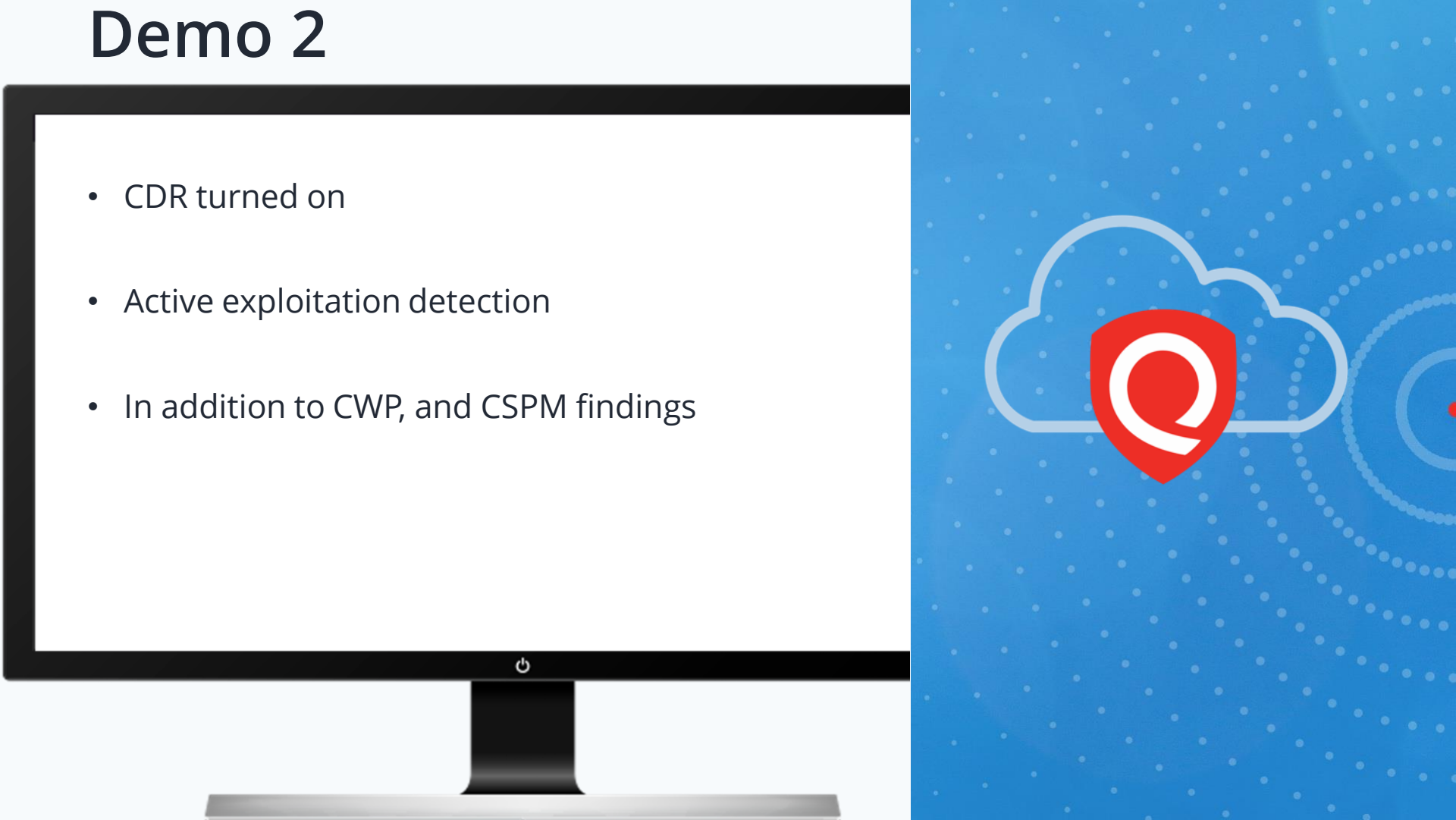
Cloud Threat Stages



	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Threat stage	**Recon/ Incursion**	**C&C**	**Installation**	**Lateral movement**	**Action on objectives**
TTPs	**Exploits, Scanners**	Encrypted and unencrypted channels	Malware, Cryptominer, ELF binaries	Bruteforcing → SSH, RDP, Port scan	Cryptomining, Data exfiltration, Ransomware

Demo 2

- CDR turned on
- Active exploitation detection
- In addition to CWP, and CSPM findings

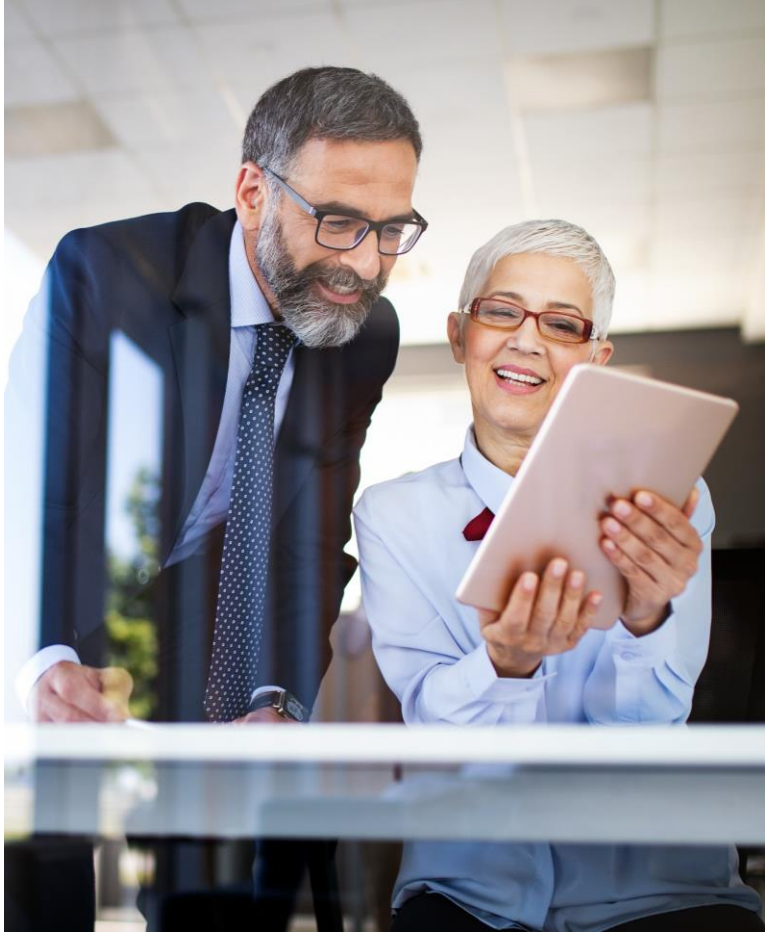


Shift-left Security Across the DevOps Pipeline

- Support for all cloud service provider build tools, registries, and Kubernetes implementations

Innovative Packing and Licensing for Frictionless Cloud Adoption

- You can transfer current VMDR licenses TotalCloud – 1:1
- With a TotalCloud SKU can select different features (CSPM, CWP, CS, CDR) without re-licensing
- Combined volume pricing based on both VMDR licenses and cloud licenses
- Flexibility of reallocation of units based on your needs



QLU Mapping

01 CWP:
- VMDR Cloud Agent = 1 QLU
- VMDR FlexScan = 4 QLU

02 CSPM = 8 QLU

03 CDR = 8 QLU

04 Container Security for virtual machines = 30 QLU

05 Container Security for Registries = 8 QUL

06 Serverless Container Security = 30 QLU

What is QLU

Conversion unit within TotalCloud to interchangeably use different cloud assets

Pacific Dental Services

Enhanced protection for mission-critical cloud services

Company

- Founded: 1994
- HQ: California, US
- Employees: 10,000+
- Operations: 900 supported offices in 25 states

Challenges

- Current solutions did not catch the threats quickly.
- Multiple point solution increased investigation time
- Lacked insights on prioritization and recommendations of what to fix first.
- Meeting stringent regulatory requirements due to evolving threat landscape

RESULTS

4 hrs — **Detect threats faster than existing tools**

60% — **Reduction in investigation time per incident**

Clear, accurate insights on prioritization and recommendations for resolving them

Helped meet the audit requirements of regulators by strengthening security

> We are **extremely impressed with the speed and accuracy** of Qualys. In fact, we have such trust in the data we're getting from TotalCloud that we now **feed data from Qualys into our other security solutions**—enriching our data and helping analysts to make better-informed decisions.

Nemi George, MBCS, CCISO, ITIL, CISA,CISM, CDPSE

Vice President, Information Security Officer | Service Operations

PACIFIC DENTAL SERVICES®

Centrica

Fast Tracking Cybersecurity Compliance

Company

- Founded: 1997 (200 years legacy)
- HQ: London, UK
- Employees: 25,000+
- Industry: Energy and services company

Challenges

- Lack of comprehensive security posture against advanced threats in a multi-cloud environment.
- Accurately identifying threats
- No real-time visibility
- Complex infrastructure with multiple point products

RESULTS

Protected entire multi-cloud infrastructure with a **single unified cloud hardening and real-time security**

>99% Detected **known** and **unknown** threats with the **highest accuracy**

1 sec **Real-time** detection of threats at **sub-second** speed

Seamless integration with existing tools enhanced productivity and provided higher ROI

> We selected Qualys TotalCloud because of its forward-looking approach to securing multi-cloud environments with unparalleled threat detection capabilities based on advanced deep-learning AI technology.

Mark Wootton
Head of Threat and Vulnerability Management

TotalCloud Strategic Initiatives

Customer focused innovation

Single Platform Experience
Unified Experience for CSPM, CWP, CDR, and Container

FlexScan for policy compliance, malware, FIM using Snapshot as a platform

TruRisk Insights based on CWP CSPM, CDR to providing a single prioritized view for remediable actions

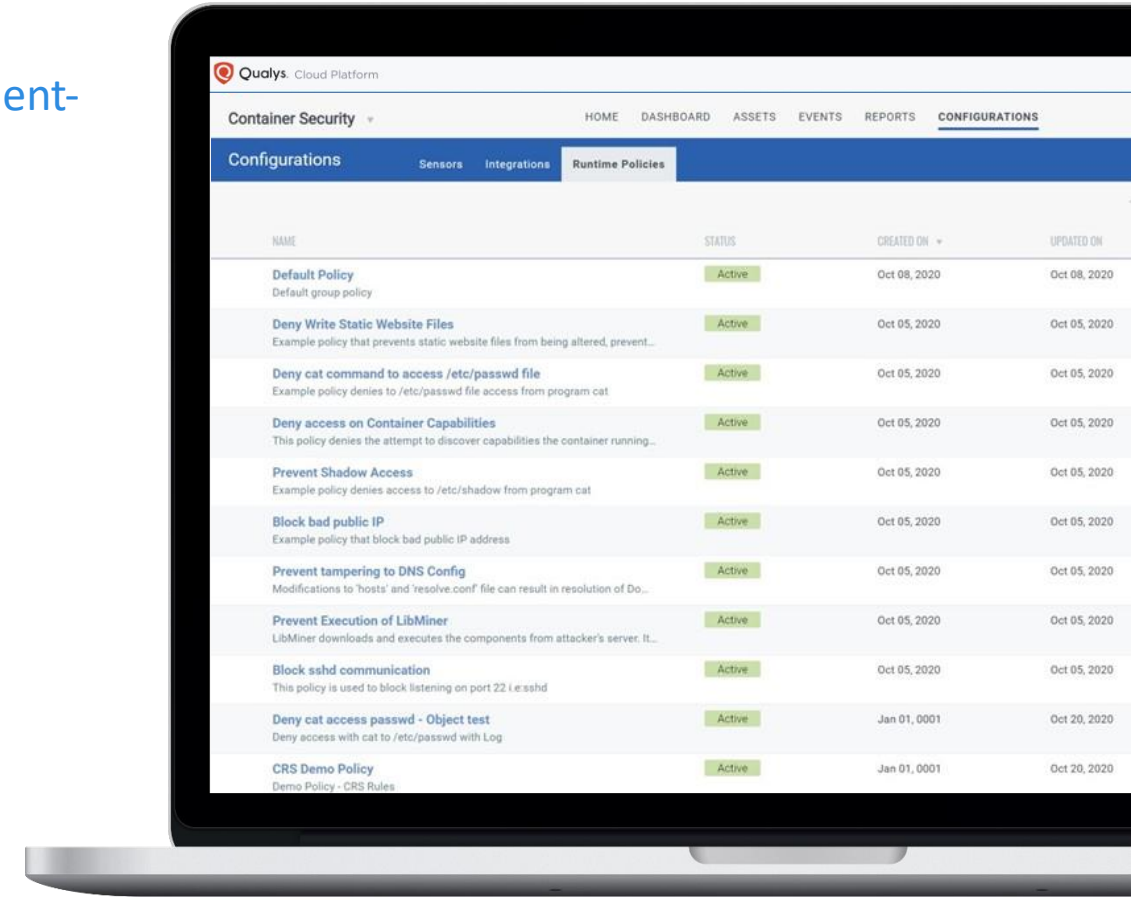
CIEM – Identity and Entitlement as a key new component to address issues like privilege escalation

Thank you!

Container Security

Security across the entire development-deployment lifecycle

- Discover vulnerabilities across the full lifecycle of your container images and running containers
- Detect malicious or unauthorized activity in running containers
- Works both on-premises and in public clouds
- Broadest support for CI/CD tools, registries, and Kubernetes environments



Qualys.