Manage Risk from Your Containerized Workloads

Abhishek Singh
Vice President, Product Management
Kubernetes & Container Security

The Great App Migration ...

"Gartner predicts that by 2028,
over 95% of organizations will run
containerized applications in production."

This is a sharp increase from under 50% in 2023

DIE for Containers

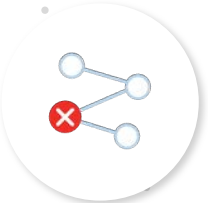
I-mmutable

Cannot patch them in place

D-istributed

Cannot hide interfaces between internal modules

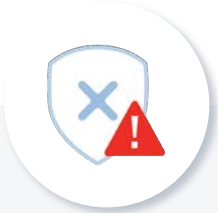
Container Security Challenges



E-phemeral

Cannot catch them with a periodic snapshot like approach

Taming Container Security in 5 Easy Steps



1. Scan Vulnerabilities

- Scan images for vulnerabilities, malware, and secrets
- Scan for insecure config and excessive entitlement and privileges

2. Remediate Vulnerabilities

- Update image after patching vulnerabilities, removing malware and secrets
- Secure config in compliance to industry benchmarks and best practices

3. Enforce Risk Compliance

- Block images that have vulnerabilities, malware, secrets or insecure config
- Prioritize and eliminate the riskiest vulnerabilities first

4. Scan for Runtime Drift

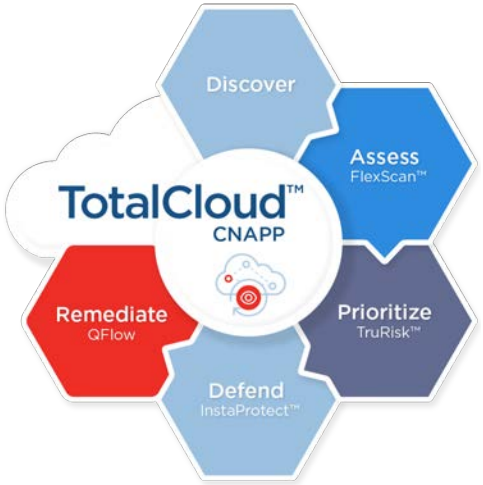
- Some cryptominer image that decides to pop up at runtime
- Drifted packages in scanned images
- Drifted vulnerabilities in scanned images

5. Manage Residual Risk

- Detect and respond to unmitigated risks
- Monitor anomalous behavior for zero-day

TotalCloud KCS: Risk Management for Containers

Start secure and stay secure with a real-time AI CNAPP solution



From **Development** to **Runtime**

Cloud Security Posture Management (CSPM)

Inventory of public cloud resources. Detection and remediation of misconfigurations and non-standard deployments, including Infrastructure as Code (**IaC**) Security.

Cloud Workload Protection (CWP)

Scanning for vulnerabilities in the cloud environment (VMDR with FlexScan).

Cloud Detection and Response (CDR)

Continuous real-time protection of the multi-cloud environment against active exploitation, malware, and unknown threats.

Kubernetes & Container Security (KCS)

Discover, track, and continuously secure containers – from build to runtime.

Cloud Infrastructure Entitlement Management (CIEM)

Discover, track, and continuously manage identities and privileges in cloud environments.

SaaS Security Posture Management (SSPM)

Manage security posture and risk across your entire SaaS application stack.

Kubernetes and Container Security (KCS)

Modes

Container Sensor

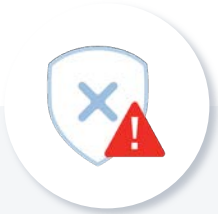
CICD | Registry | General

Network scanner

Cloud Agent

Operational since 2018, now serving over 1000 customers worldwide

KCS for Container Security



1. Scan Vulnerabilities

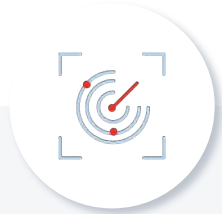
- Scan images with **Registry** Sensor and **CICD** Sensor for vulnerabilities and secrets
- Scan images for zero day malware (with **deep learning**)
- Scan images for compliance to **CIS for Docker**

2. Remediate Vulnerabilities

- Qualys **QIDs** are remediation ready
- Utilize our integration with jira and **ServiceNow CVR**
- Assign to the right teams with vulnerabilities broken down by base vs app **layers**

3. Manage Risk

- Risk aware controls for **cluster admission** and **CICD**
- Eliminate toxic Risk by utilizing **TruRisk Insights**
- Leverage **TruRisk for Clusters** to drill down into what brings risk



4. Scan for Runtime Drift

- Use **General** Sensor to scan running containers for package and vulnerability drift
- Scan running containers for compliance to **CIS for Docker**

5. Manage Residual Risk

- Detect zero day malware in **running containers**
- Utilize **Zero Trust** principles for proactive risk informed resilience

Customer Story

Qualys®

McAfee

Driving Workflow Automation with QFlow

Niharika Pothani

McAfee

Niharika Pothani

CISA, CISSP

Senior Manager, Security Testing and Vulnerability Management

5 years with McAfee

Head of Vulnerability Management, Cloud Resiliency and Security Awareness team

8+ years of experience in Cybersecurity

Masters in Cybersecurity
Bachelors in Information Technology

McAfee™

- Headquarters in San Jose, CA
- Global leader in online protection for consumers

OUR VISION

A safe digital world for your home, family, and business

35+ years
of protecting people

600 million+
devices

1,800+
employees

182
countries

Workflow Automation with QFlow

1

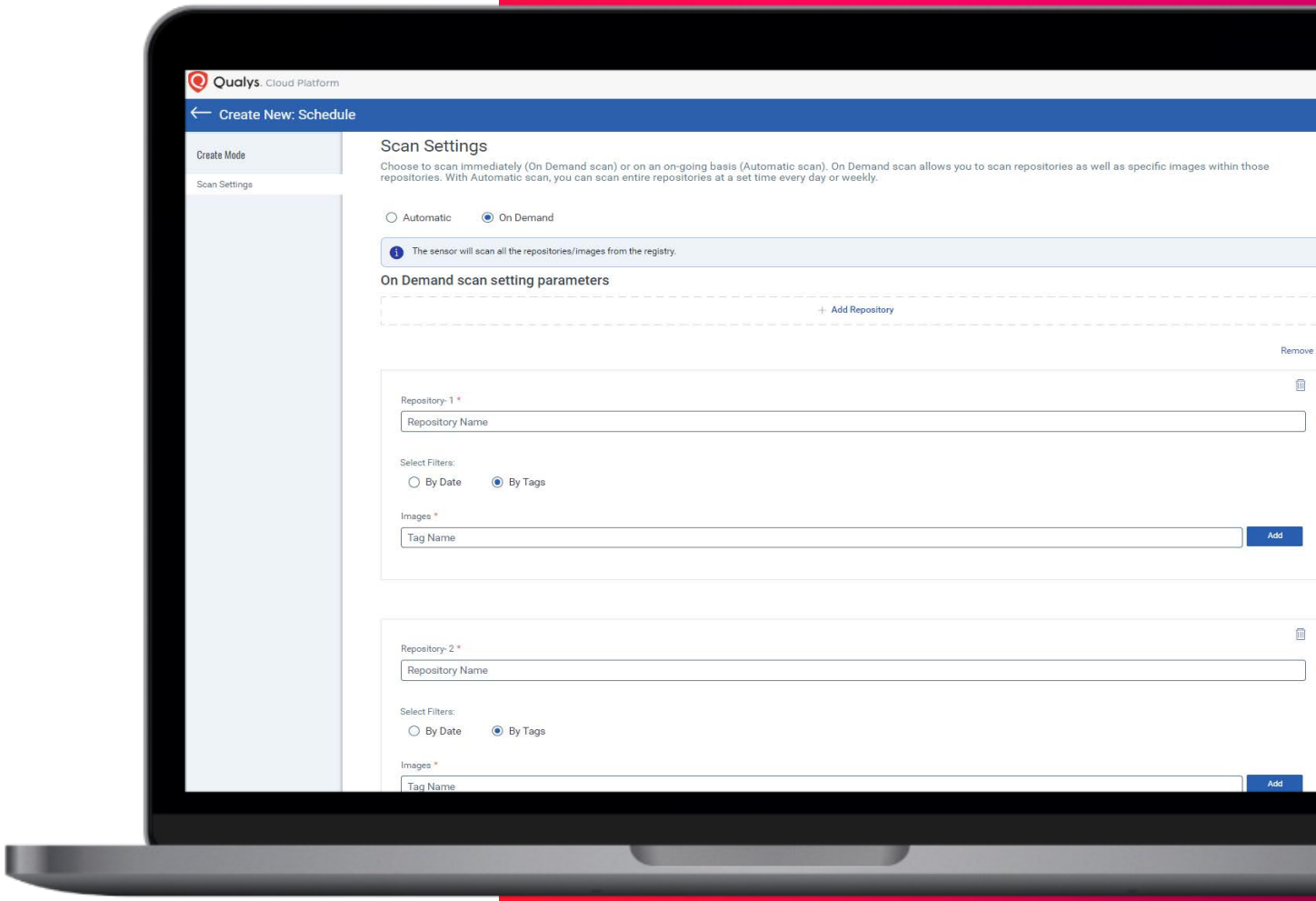
Scanning a Custom List of Images in Registry

Desired Outcome

Scan latest container images pushed to a registry

Challenges

- Unable to use image creation date
- Entering repositories manually was tedious



1

Scanning a Custom List of Images in Registry

Solution

Unable to use image creation date

QFlow to call Registry Sensor API to scan images

Benefits

Bring your own (higher level) abstraction

No need to find servers to run the script

Extend/customize Qualys platform

2

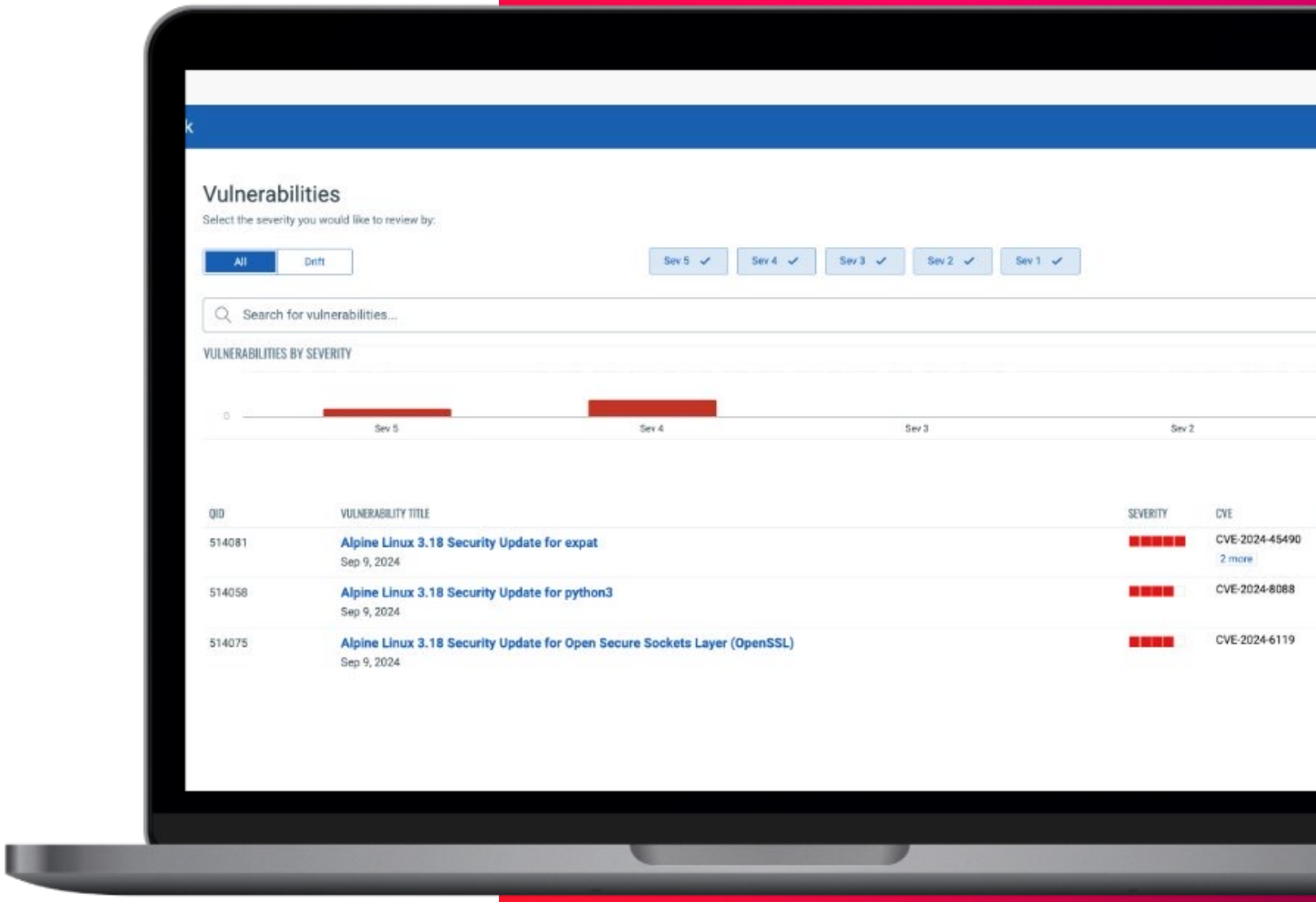
Custom Reporting for Remediation

Desired Outcome

Generate custom vulnerability reports for remediation

Challenges

- Asset centric-view
- No account/VPC context for containers
- Tedious to generate reports per internal customer needs



2

Custom Reporting for Remediation

Solution

Use CSAM APIs to find Cloud Account and VPC details

Use Qflow to tag containers with Account and VPC details

Benefits

Continuous enrichment

Able to meet internal customer needs

Qualys as our reporting data lake

Outcomes

1

Container Image Scan

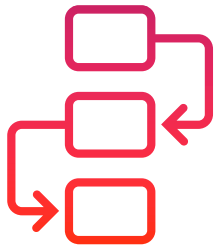
↓ 30 min to 2 min

2

Custom Report Generation

↓ 3 hours to 10 min

What's Next?



Automate workflows for actionable remediations

Further reduce average time to remediate container vulnerabilities

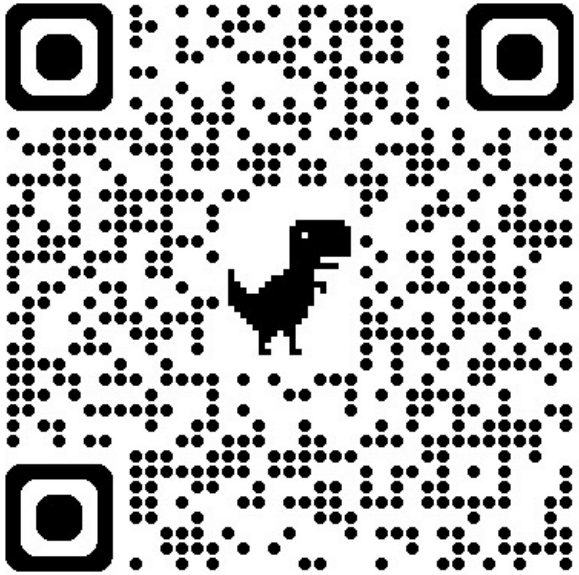
Automate Registry scans straight from DevOps

Thank You

McAfee™

Demo Time

Qualys



QR Code

Book a meeting with me to discuss how we can help you manage risk from your containerized workloads

Qualys®