



# Strengthening the Cloud Security: Strategies for Comprehensive Risk Management

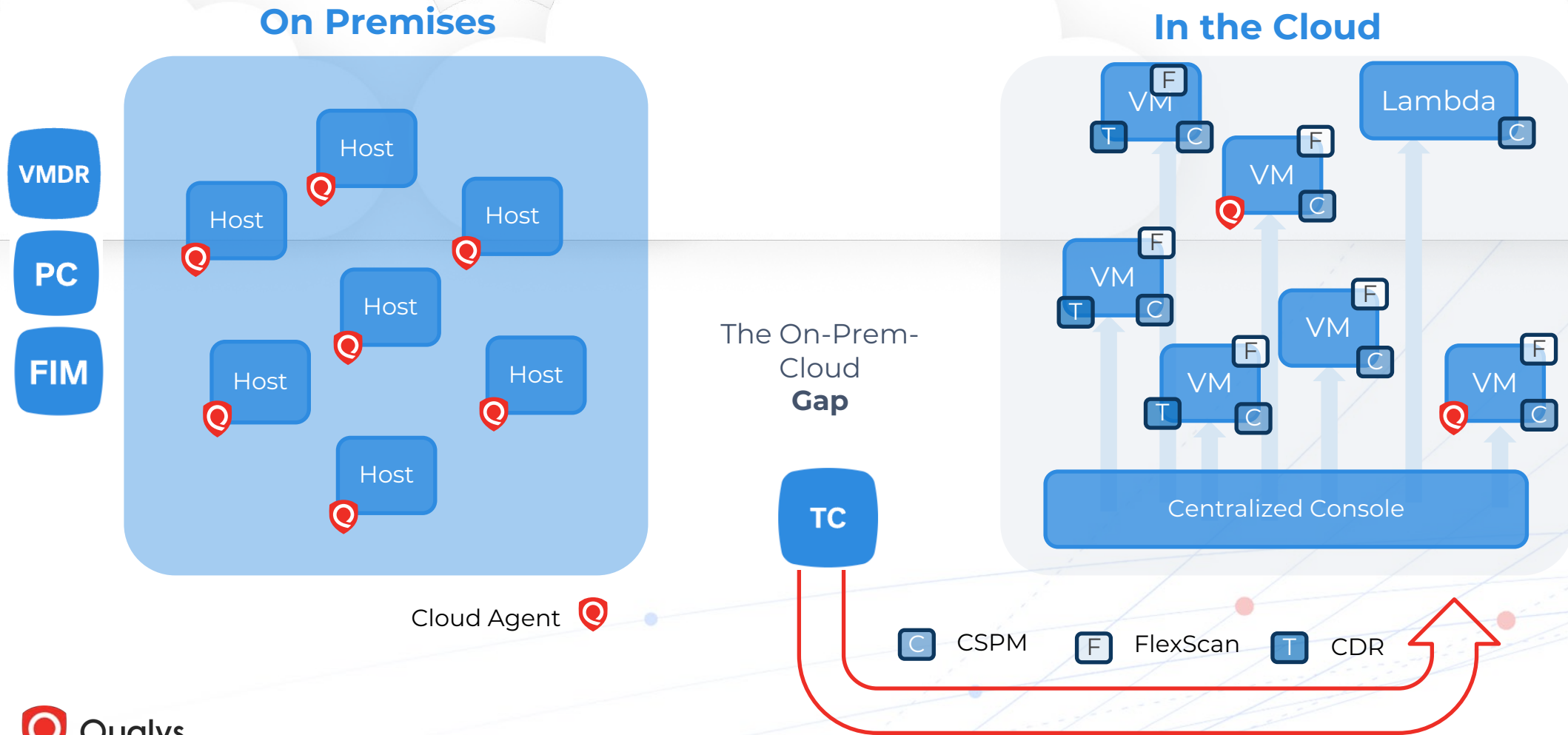


**Kunal Modasiya**

Vice President, Product Management  
Attack Surface Management, Web App & API Security  
Cloud & Container Security  
April 24

# Security Journey from On-Prem to Multi-Cloud

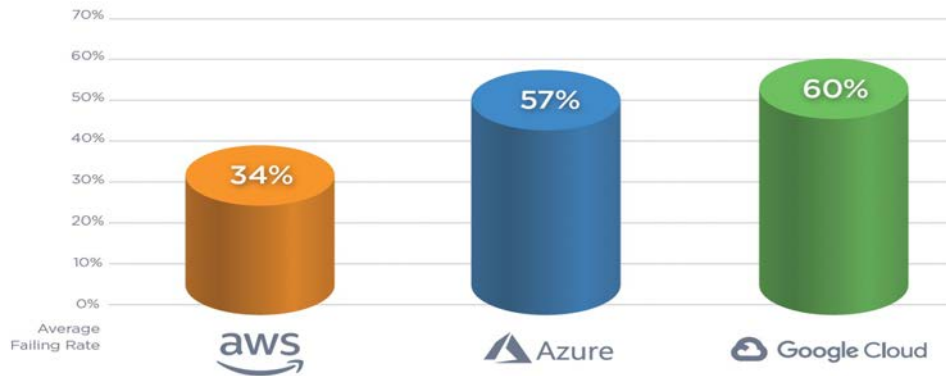
## VM, Compliance, FIM, and More



# Leading Causes of Cloud Breaches

## Vulnerabilities, Misconfigurations, and Malware

### Most Misconfigured Controls Across Major CSP

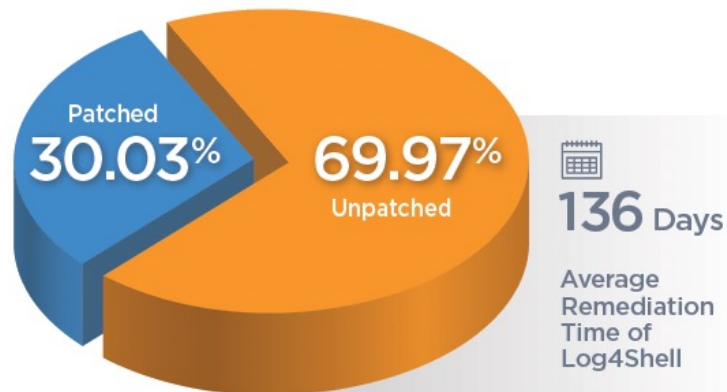


CIS benchmarks controls across major CSP's are not meet **50% time on average**



**70% of Log4Shell** vulnerabilities have still not been fixed, since last 2 years

### High Unpatched Rate



**Cryptomining malware is a growing threat**

# Challenge: Siloed View of Risk



**Hybrid Visibility:** How do I get 360 visibility and determine the risk of my resources across on-prem + multi-cloud + SaaS environments?



**Prioritization in the Cloud:** How do I prioritize risk emerging from vulnerability, misconfiguration, permissions, and threats between tools?



**Orchestrated Data:** How do I unify and orchestrate data feeds from my Cloud with on-prem, IoT, OT, external asset environments?





# Challenge: Ineffective and Inefficient Communication of Risk



**Reporting:** How do I provide risk reporting tasks for Cloud in a way that unifies risk assessment and remediation recommendations holistically?



**Mitigation Workflows:** How can I better inform Dev, Ops, and DevOps teams about the critical issues to be fixed in the cloud?



**Compliance:** How can I provide a unified compliance posture report across on-prem, multi-cloud, and SaaS to auditors?



# Challenge: Remediation Process is Too Long



**Proactive Security:** How can I **reduce the risk of all risk vectors** - on-prem, multi-cloud, and SaaS environments?



**Reactive Security:** How can I **more quickly eliminate the risk across all risk vectors** - on-prem, multi-cloud, and SaaS environments?



**Automation:** How can I **automate** the risk mitigation path selection process?





# Introducing TotalCloud

The Qualys Approach to CNAPP

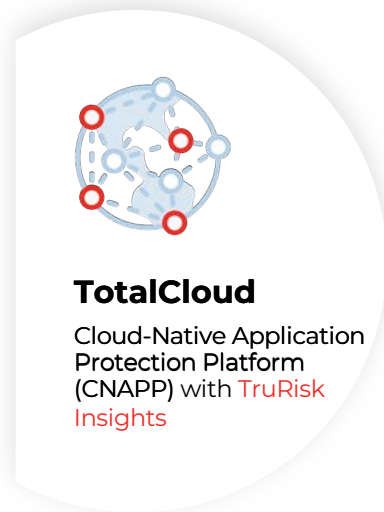


# Measure, Communicate and Eliminate

## Unified Vulnerability, Threat and Posture Management

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

Unified Vulnerability, Threat and Posture Management 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 (VM DR 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.



### SaaS Security Posture Management (SSPM)

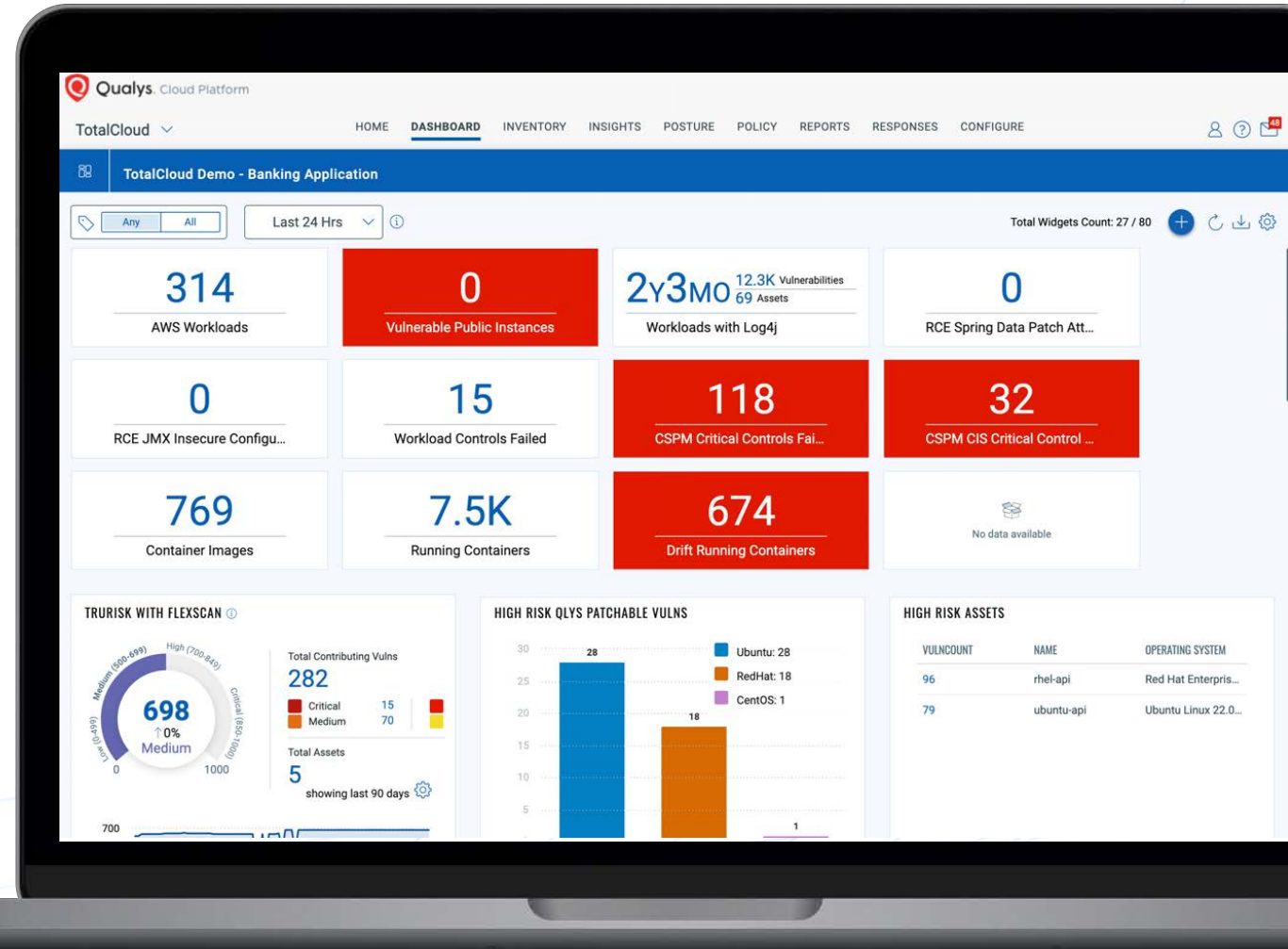
Manage security posture and risk across your entire SaaS application stack



# Measure Risk Effectively

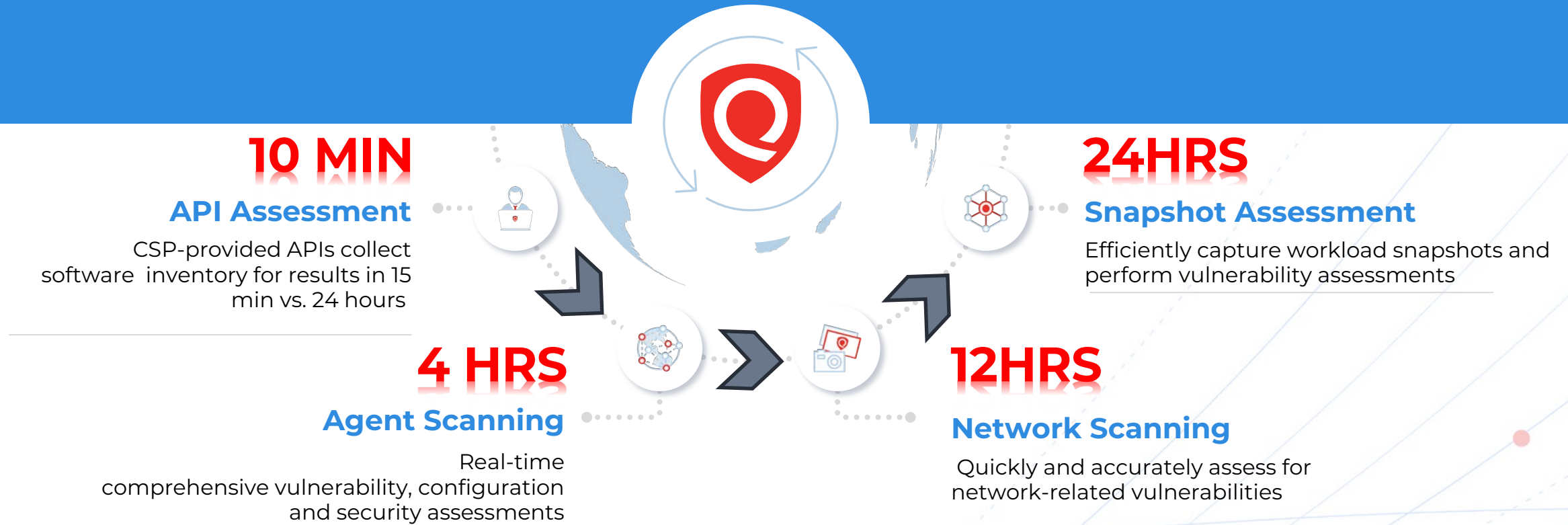
## Cloud Security it Hard. Why Make it Harder?

- ✓ Quickly onboard the connectors and see the dashboard in 30 mins!
- ✓ Select different features (CWPP, CDR, CS, CSPM, SSPM, SaaS DR) as part of the same subscription
- ✓ See the unified cyber risk picture across multi-cloud and on-prem environment







# Measure: Comprehensive Scanning

## Qualys FlexScan - *Fast, Flexible, Ongoing Scanning Results*



# Scalable Scanning

## Overview of Different Scanning Methods

Assessment Method	Strengths	Limitations
 <p><b>API-based</b> Use CSP-provided APIs to collect software inventory and perform assessments</p>	<ul style="list-style-type: none"> <li>• <b>Fastest setup and assessment</b></li> <li>• Ephemeral instances</li> <li>• Quick assessment on startup</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Lack of OSS coverage</b></li> </ul>
 <p><b>Snapshot-based</b> Take snapshot of the workload and perform vulnerability assessment on it</p>	<ul style="list-style-type: none"> <li>• <b>Fast and easy setup without access to the workload</b></li> <li>• Quick assessment</li> <li>• Can scan suspended instances</li> <li>• M&amp;A, Cloud migration, large scale deployment</li> </ul>	<ul style="list-style-type: none"> <li>• Requires deployment of a scanner</li> <li>• Does not work for a hybrid environment, only public cloud</li> <li>• <b>Periodic scanning, 24 hrs. due to resource limitations</b></li> </ul>
 <p><b>Agent-based</b> Real-time comprehensive vulnerability, configuration and security assessment</p>	<ul style="list-style-type: none"> <li>• Long-running workloads</li> <li>• <b>Detects vulnerabilities based on runtime-context</b></li> <li>• Workloads on which high accuracy vulnerability coverage is desired</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Getting access to all workloads to run agents</b></li> <li>• Difficult to deploy agent to ongoing deployments (shutdown workloads to deploy new agent)</li> </ul>
 <p><b>Network-based</b> Assess compute and non-compute</p>	<ul style="list-style-type: none"> <li>• Outside in view of vulnerabilities</li> <li>• Assessment of non-compute workloads</li> <li>• Meet compliance requirements</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Need to have authentication details</b></li> <li>• Deployment complexity</li> </ul>

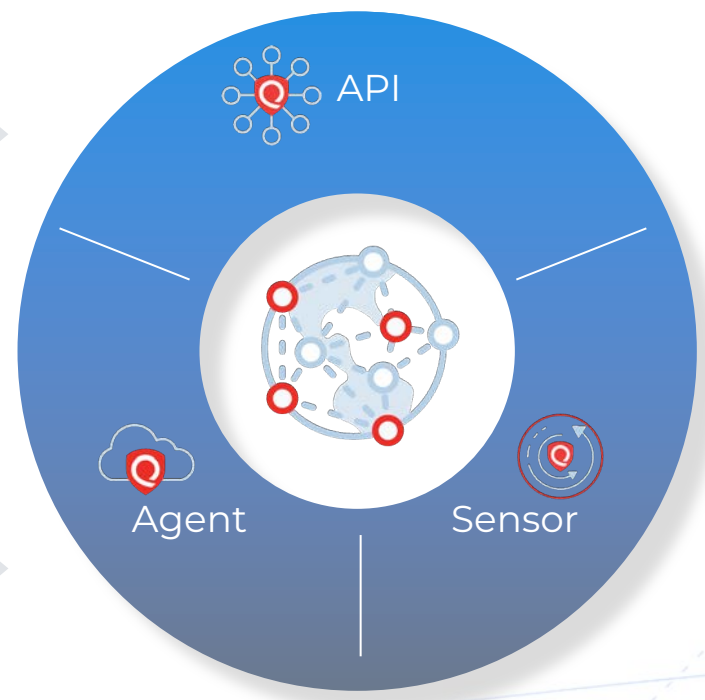
Measure

Communicate

Eliminate

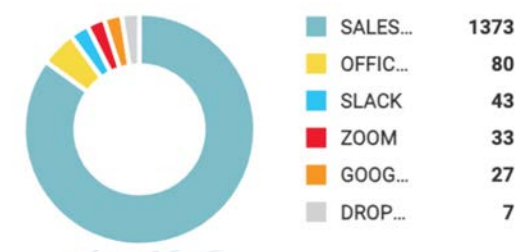
# Comprehensive Inventory

## Users, Resources and SaaS Applications



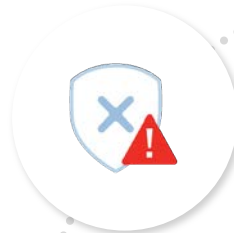
INVENTORY TYPE	SERVICE
Instance	EC2
VPC	VPC
RDS	RDS
Subnet	VPC

INTERNAL USERS



# Data from Many Sources with Independent Priorities

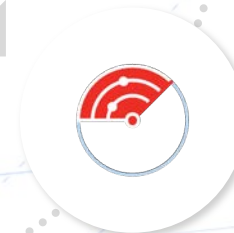
Vulnerability Assessments (CWP)



Misconfiguration (CSPM)



Runtime Threats (CDR)



External Attack Surface (EASM)



# Contributing Factors

## With TruRisk™ Insights

## Risk Multipliers

Critical vulnerability with a known exploit found on Publicly Exposed VM

Asset with Vulnerability and C2 beaconing to malicious IP

High permission publicly exposed critical vulnerabilities

Endpoints with vulnerabilities, EOL software, and cloud secrets



# TruRisk Insight Report

Get Yours Now for Multi-Cloud Environment

1. Know your Risk of Multi-Cloud Workloads
2. Publicly exposed Cloud Application & Technologies
3. Identify Risky IAM Roles, Permissions and resource
4. Prioritize and Remediate the Risk

## Call To Action :

Reach out to local TAM team for your TruRisk Insight Report

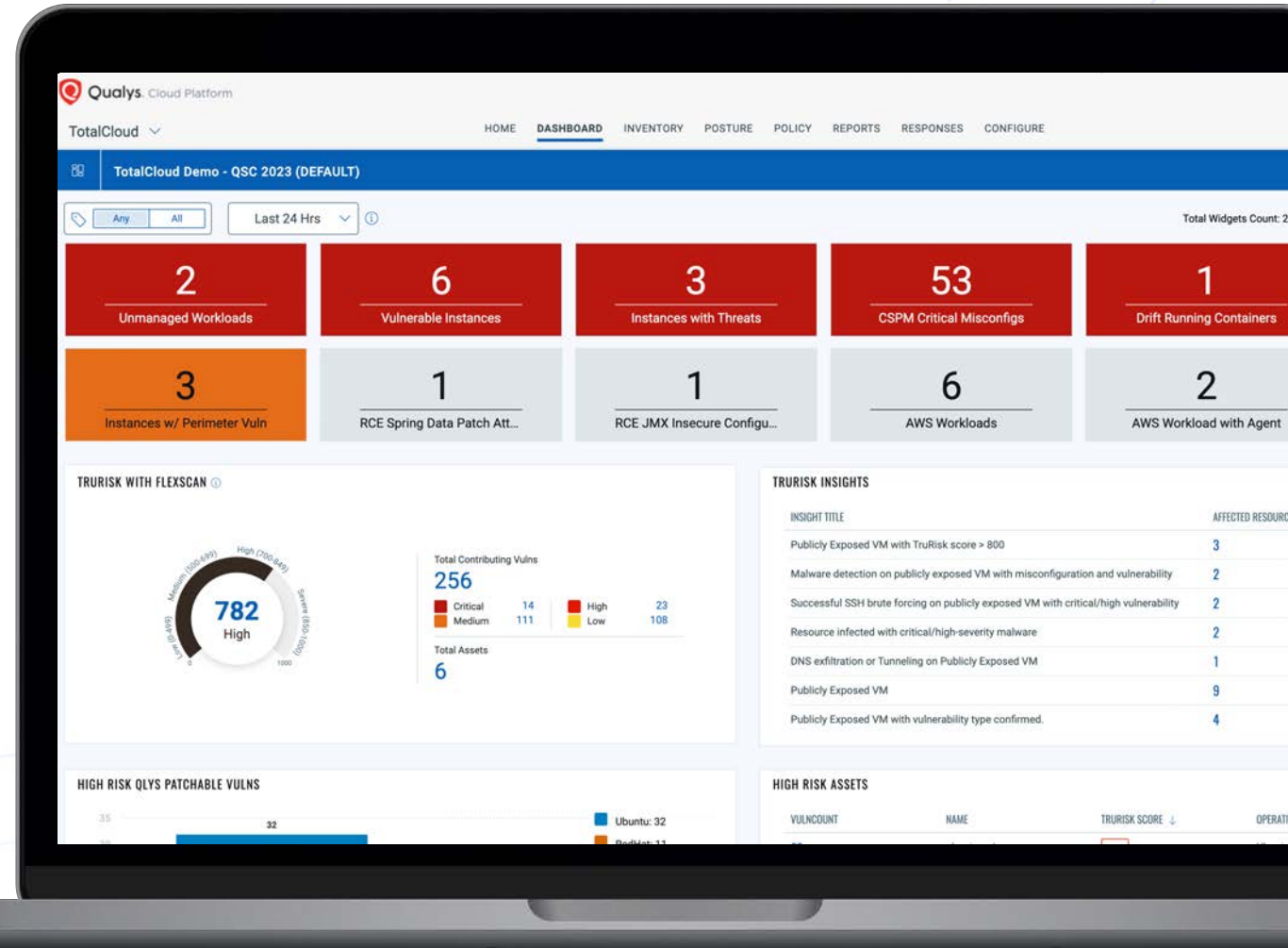


Powered by: 

# Communicate Risk Effectively

## Cloud Security it Hard. Why Make it Harder?

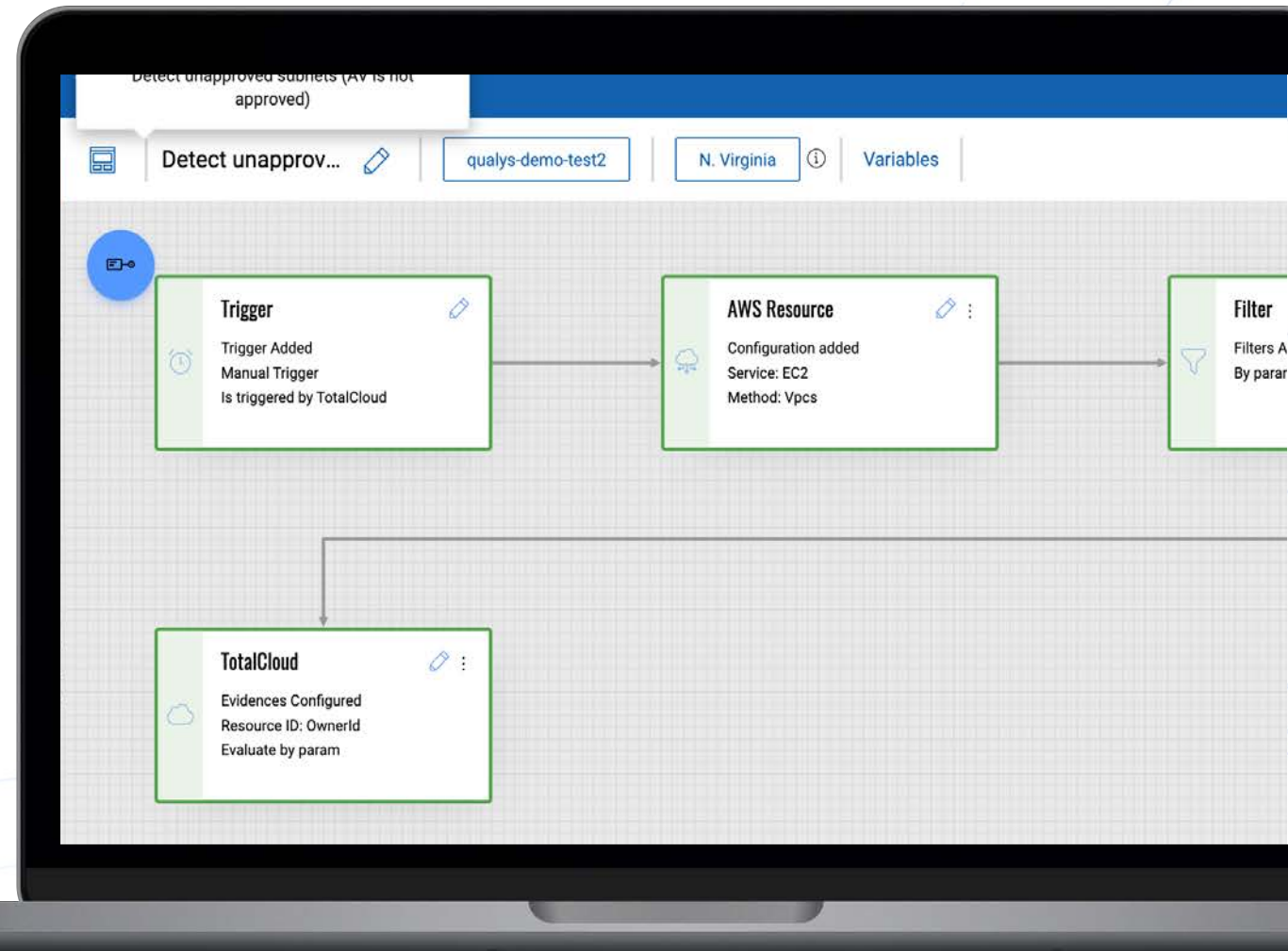
- ✓ **View persona-based dashboards** that aggregate risks from all the public clouds
- ✓ **Integration with IDEs, Git repositories, CI/CD tools, Container Registries, ITSM tools (ServiceNow, JIRA)**
- ✓ **Generate reports for 30+ industry compliance mandates**



# Eliminate Risk Faster

## Action Vulnerabilities – Wherever they are

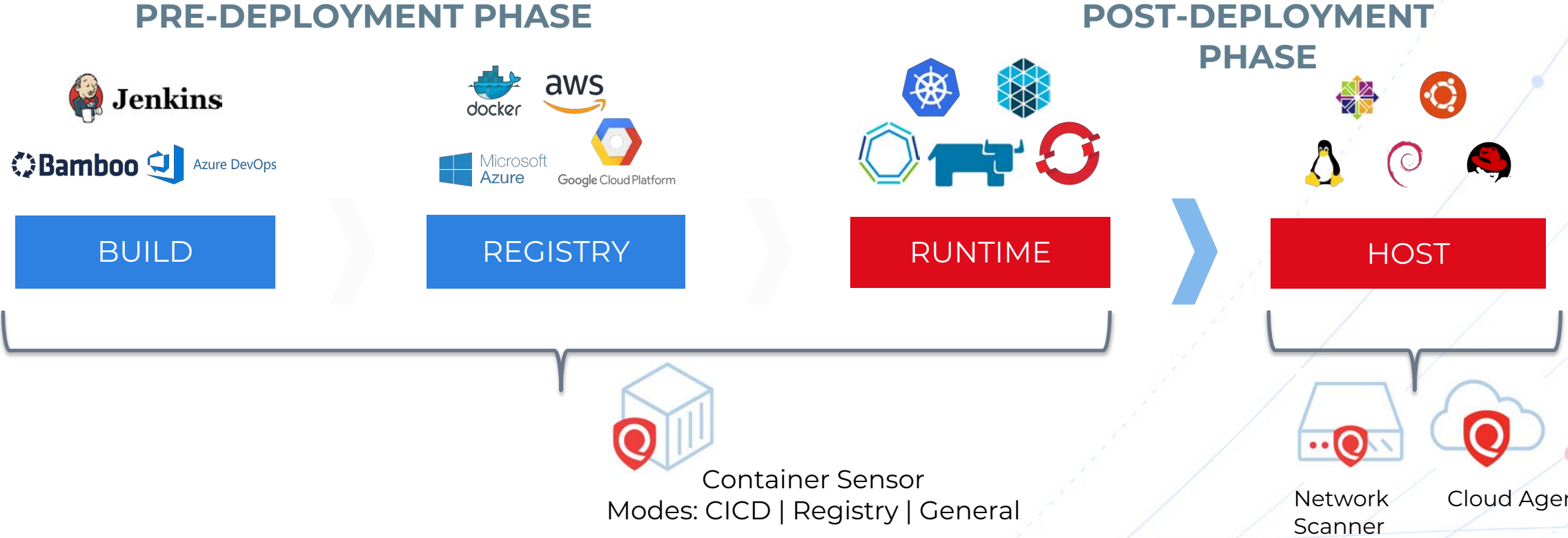
- ✓ **Use 1-click out-of-box remediations** for instant remediations
- ✓ **Automated remediation with no-code/low-code, workflow** to mitigate and remediate risk
- ✓ **ITSM tool integration** for ticket assignment



# Container Security



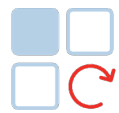
# Measure: Shift-left Security Across the DevOps Pipeline



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

# Flexible Subscription Using **QuaLys Units (QLU)**

Select what you want to deploy and when with QLUs



Ability to select different features (CWPP, CDR, CS, CSPM, SSPM) as part of the same subscription



No need to re-license to select different features



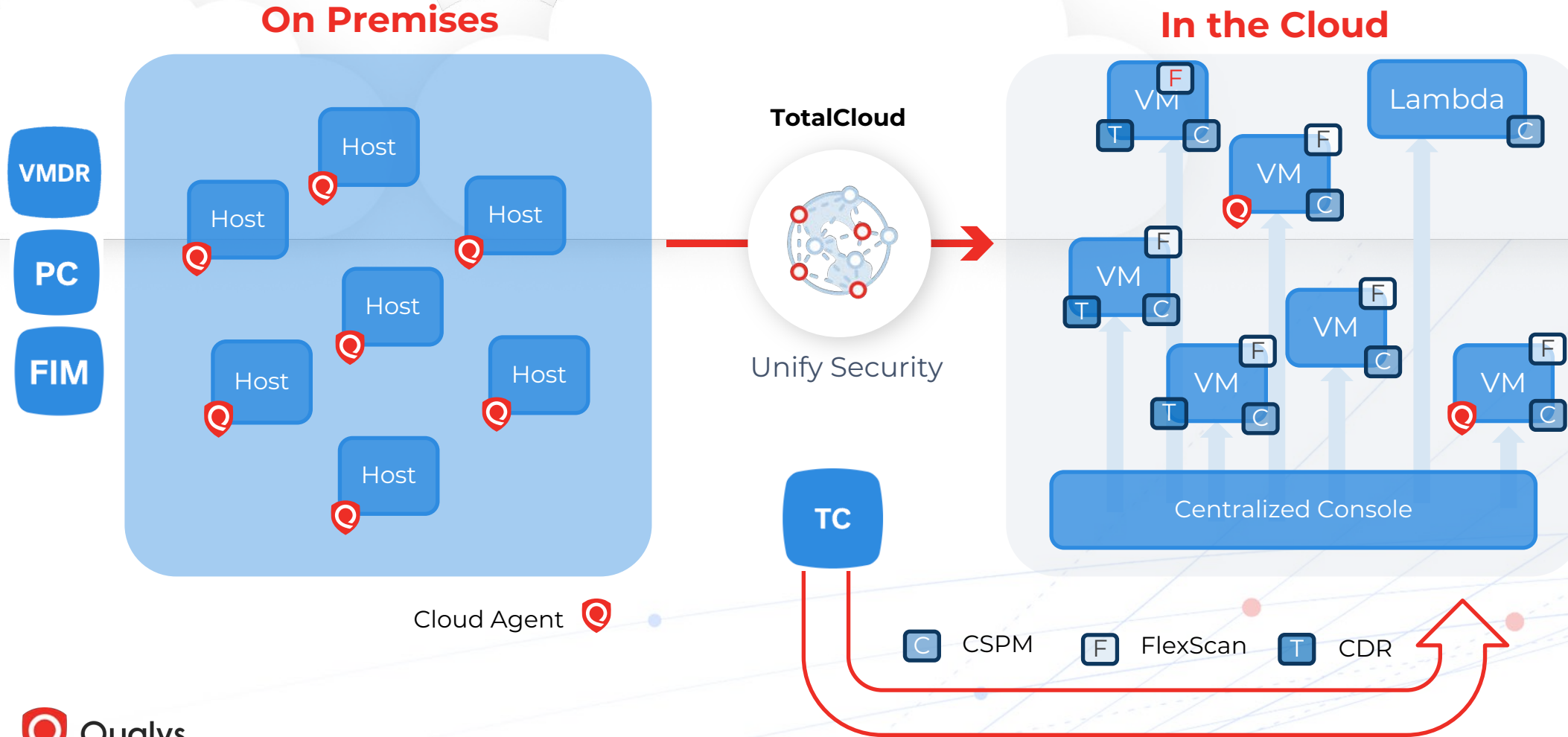
Qualys Units (QLU) are reallocated to enable preference



One QLU == One VMMDR – Move Unused VMMDR licenses to TotalCloud

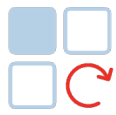
# On-Prem & Multi-Cloud

## Bringing Together On-Prem and Multi-Cloud



# Let's Get Started With TotalCloud

## Use VMDR unused Licenses towards TotalCloud QLU



Quickly onboard the connectors and see the dashboard in 30 mins!



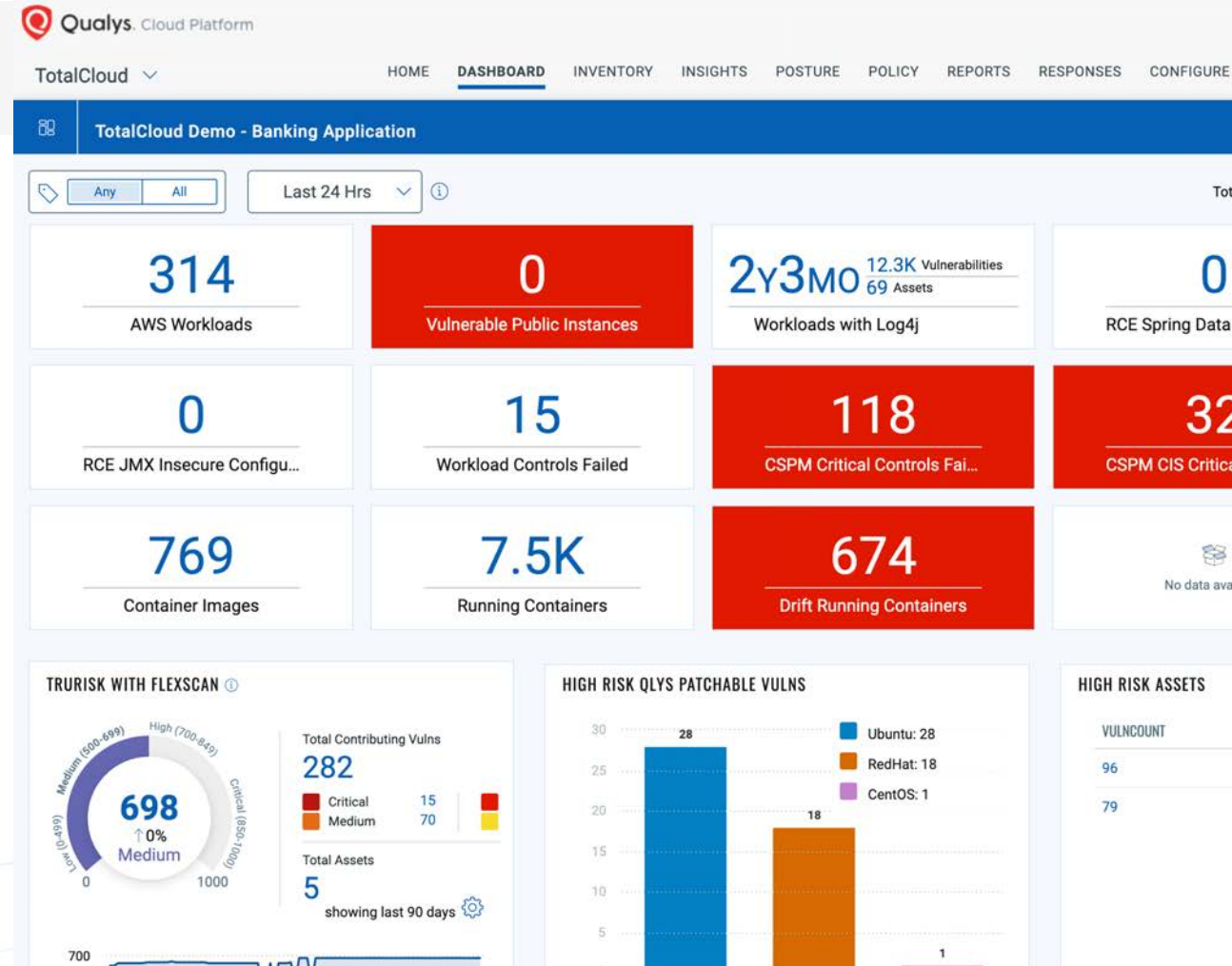
Select different features (CWPP, CDR, CS, CSPM, SSPM, SaaS DR) as part of the same subscription



See the Unified Cyber Risk across multi-cloud and on-prem environment



Prioritize and Remediation Risk with TruRisk Insights





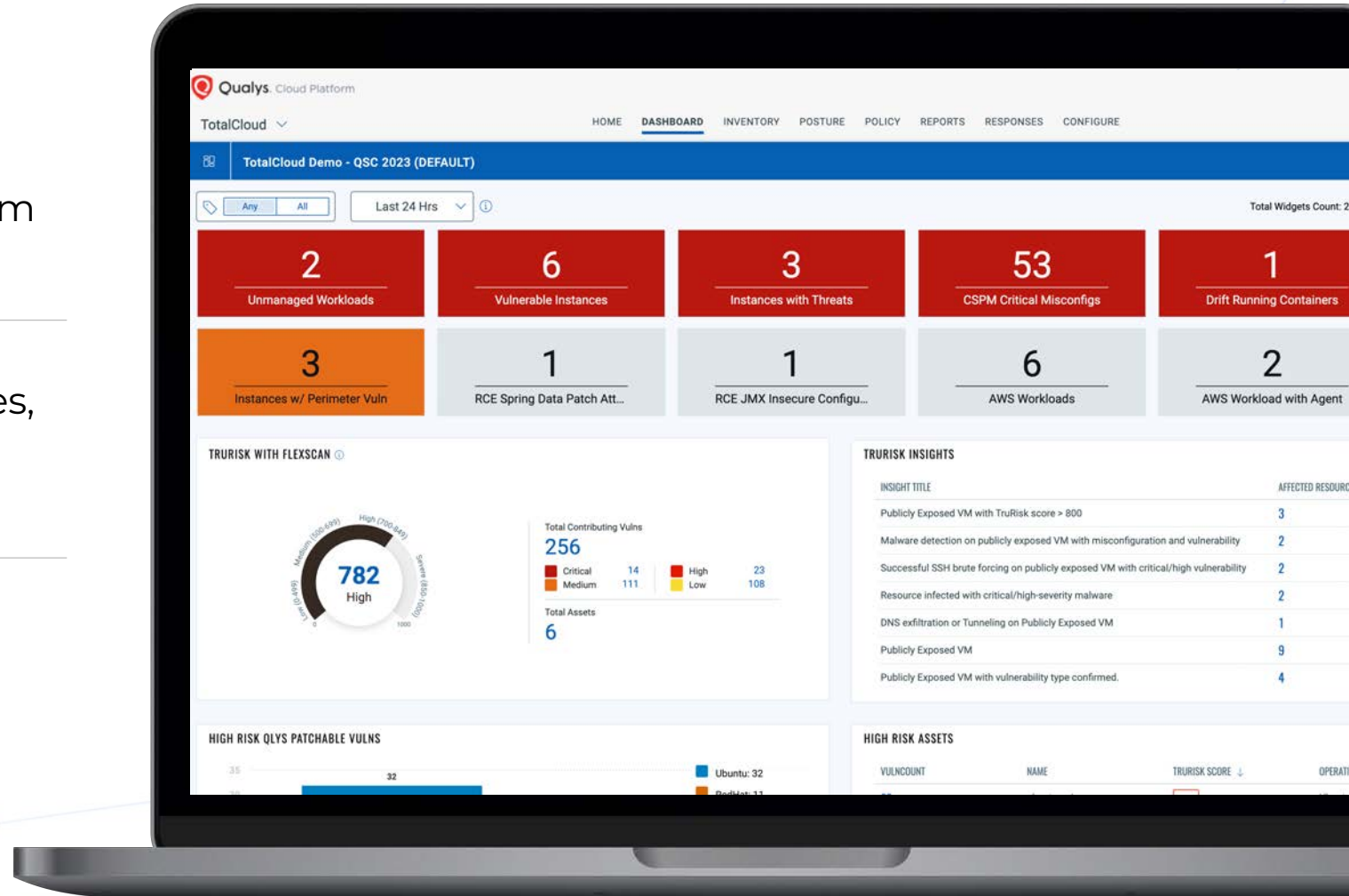
# DEMO





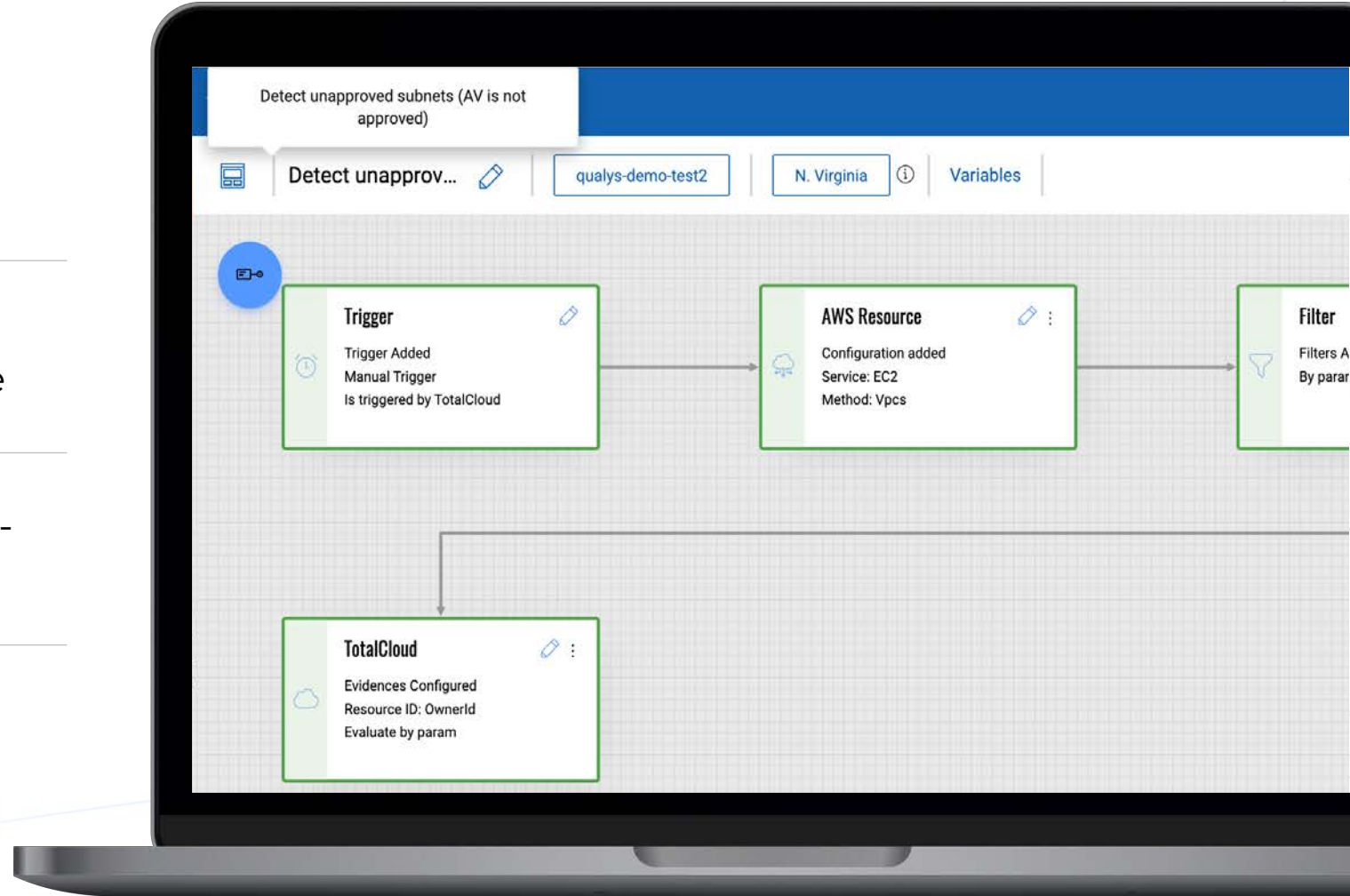
# Communicate: Risk Effectively

- ✓ View persona-based out-of-box dashboards that aggregate risks from all the public clouds
- ✓ Integration with IDEs, Git repositories, CI/CD tools, Container Registries, ITSM tools (ServiceNow, JIRA)
- ✓ Generate reports for 30+ industry compliance mandates



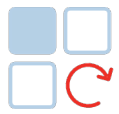
# Eliminate: Risk with Cloud-Native Workflows

- ✔ Use 1-click remediations for instant remediations
- ✔ Design with QFlow to complex workflow to mitigate and remediate
- ✔ Remediate at the source using Shift-left workflows
- ✔ Eliminate Attack Paths with MITRE ATT&CK Context



# Flexible Subscription Using Qualys Units

## Select what you want with Qualys Units (QLUs)



Ability to select different features (CWPP, CDR, CS, CSPM, SSPM, SaaS DR) as part of the same subscription



No need to re-license to select different features



Qualys Units (QLU) are reallocated to enable preference



One QLU == One VMDR

