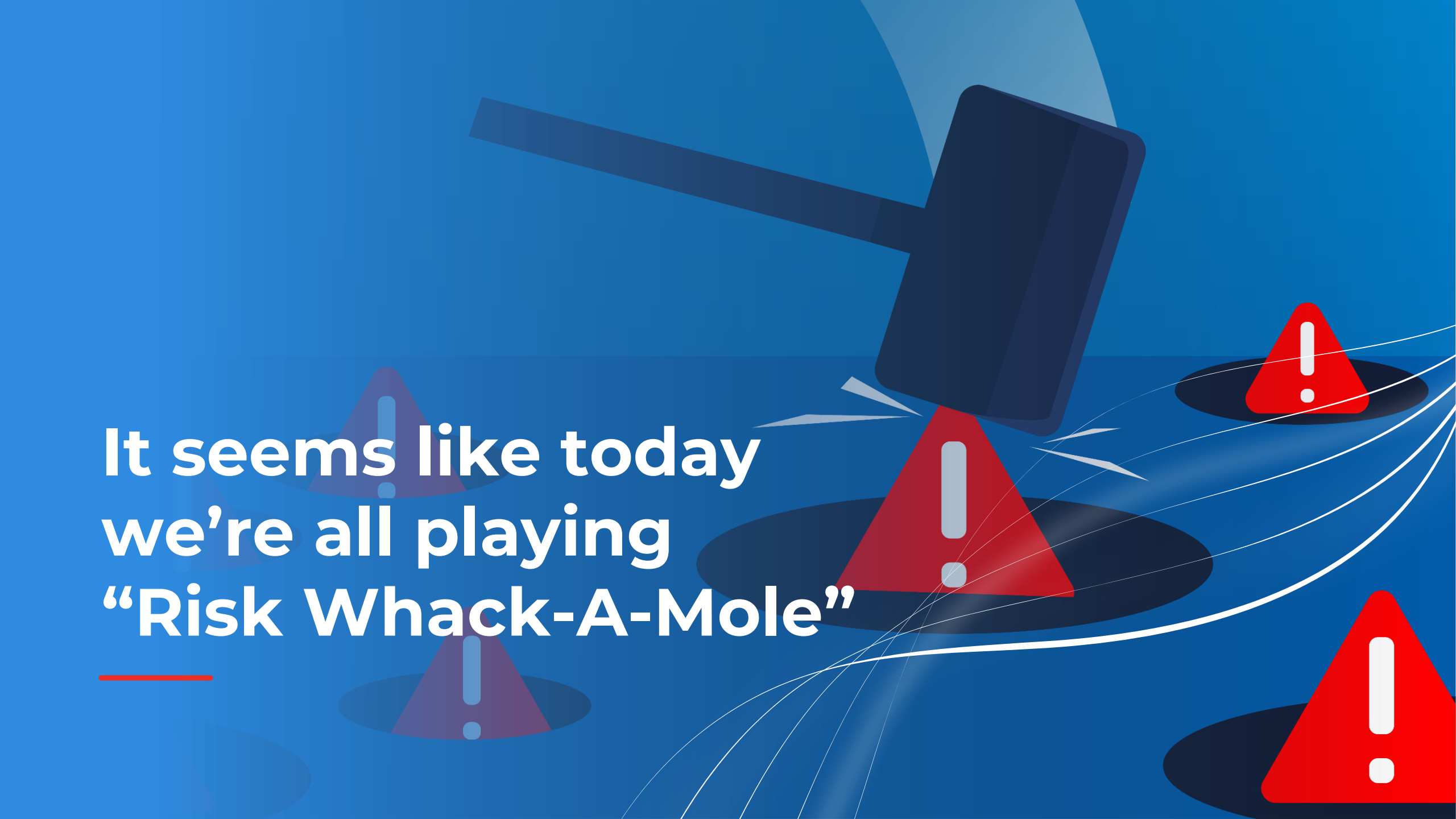
Cloud Risk Management: Breaking the Cloud Security Silos

Cloud De-Risked

Nirav Kamdar
Security Solution Architect, Cloud & DevOps APAC - Qualys Inc

Qualys®


It seems like today
we’re all playing
“Risk Whack-A-Mole”


You will never have
Zero Risk.

If everything is critical, nothing is.

Too many threats.
Too many patches.
Too many alerts.
Too many vulnerabilities.

Top 5 Cloud Risks Today

Uphill Battle for Security Team to Reduce Cloud Security Risks

Exploitable Exposure, Not Just CVEs	Contextual risk scoring based on exposure, reachability, and threat intelligence
Alert Overload and Fragmented Tools	Unified risk visibility and correlation to prioritize what matters
Code to Cloud Blind Spots	Integrated code-to-cloud visibility and runtime risk correlation
Multi-Cloud Misconfigurations at Scale	Continuous configuration monitoring and automated remediation
Identity Misuse and Over-Privileged Access	Identity risk analysis and least privilege enforcement with continuous monitoring

The Numerous Sources of Cyber Risk

New and Evolving Risk Sources

Risk Sources

- IT Assets
- Cloud Resources
- Data Center
- Installed Software
- Modules & Packages
- Workloads
- AI
- IoT
- Identities
- SaaS Apps

CISO

APPLICATIONS

workday. Office 365 SAP

OPERATING SYSTEMS

Windows Linux Apple

CLOUD / CONTAINERS / VMs

aws Google Cloud Azure

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Numerous Sources of Cyber Risk

New and Evolving Risk Factors

Risk Sources

- Data Center
- Installed Software
- AI
- Cloud Resources
- IT Assets
- Workloads
- IoT
- Identities
- SaaS Apps
- Modules & Packages

Risk Factors

Vulnerabilities	Infra/DB Misconfigurations	Unauthorized software	Missing required software
Access risks	Unauthorized File Changes	Open-source vulnerabilities	Cloud Misconfigurations
Sensitive data leakage risks	Technology debt risks	Endpoint Malicious activities	Web application risks

CISO

APPLICATIONS

workday. Office 365 SAP

OPERATING SYSTEMS

Windows Linux Apple

CLOUD / CONTAINERS / VMs

aws Google Cloud Azure

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Numerous Sources of Cyber Risk

...and New Stakeholders to Communicate With

Risk Sources

- Data Center
- Installed Software
- AI
- Cloud Resources
- IT Assets
- Workloads
- IoT
- Identities
- SaaS Apps
- Modules & Packages

Risk Factors

- Vulnerabilities
- Unauthorized software
- Infra/DB Misconfigurations
- Open-source vulnerabilities
- Access risks
- Missing required software
- Unauthorized File Changes
- Cloud Misconfigurations
- Sensitive data leakage risks
- Endpoint Malicious activities
- Technology debt risks
- Web application risks

Apps & Environments

Cloud Misconfiguration Fixes

Application, Open-source vulnerabilities

Dev Teams

SOC, Pen-test team

& many more...

CISO

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Numerous Sources of Cyber Risk

...and New Stakeholders to Communicate With

Risk Sources

- Data Center
- Installed Software
- AI
- Cloud Resources
- IT Assets
- Workloads
- IoT
- Identities
- SaaS Apps
- Modules & Packages

Risk Factors

- Vulnerabilities
- Unauthorized software
- Infra/DB Misconfigurations
- Open-source vulnerabilities
- Access risks
- Missing required software
- Unauthorized File Changes
- Cloud Misconfigurations
- Sensitive data leakage risks
- Endpoint Malicious activities
- Technology debt risks
- Web application risks

Apps & Environments

- Cloud Misconfiguration Fixes
- Application, Open-source vulnerabilities
- Dev Teams
- SOC, Pen-test team

Continuous Cloud-Risk Operations

Risk Stakeholders

- CIO
- CEO
- IT/Ops Teams
- DevOps Teams
- Vulnerability Management
- Audit / GRC

APPLICATIONS: workday, Office 365, SAP

OPERATING SYSTEMS: Windows, Linux, Apple

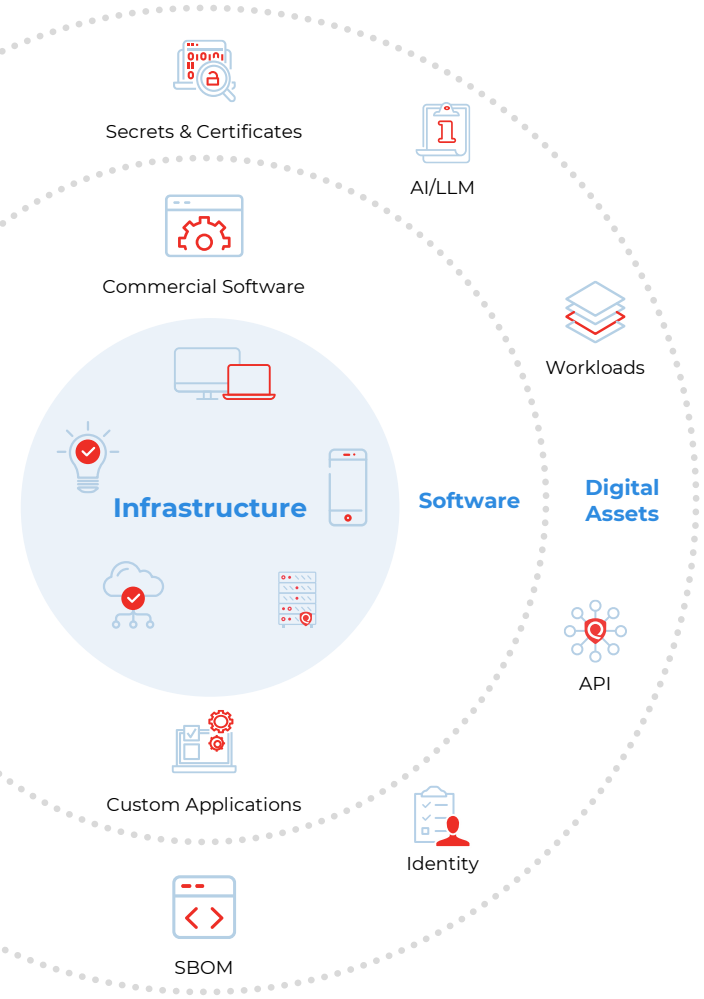
CLOUD / CONTAINERS / VMs: aws, Google Cloud, Azure

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Rapidly Expanding Attack Surface & Tool Sprawl



Accelerated cloud adoption → **Rise of specialized tools***

*Enterprise have **70+ security tools on average**

- VM
- CSPM
- ISPM
- DSPM
- SSPM
- AISPM
- ....


ALERT
ALERT
AppSec
ALERT
ALERT
ALERT
EDR
ALERT
WANNING
CSPM
CNAPP
ERROR
IAM
WARNING
SCAN

And breaches are only increasing for this vector of attack.

01

In 2025, Qualys Research Unit identified **that 70% of the Azure resources are misconfigured,** leading to a potential open attack surface.

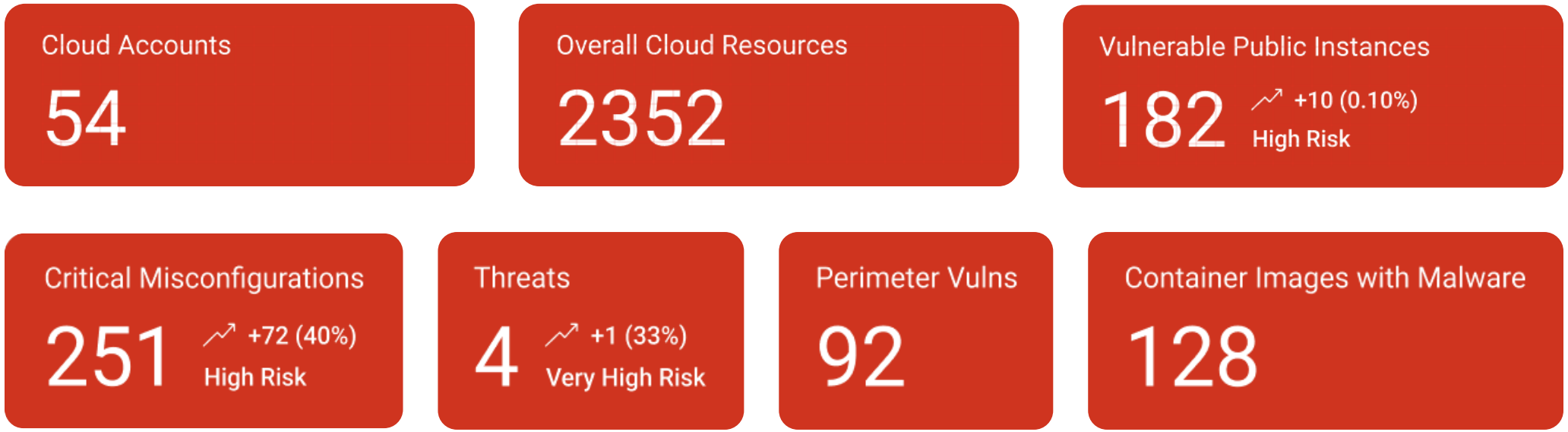
02

Attackers injected **malicious code** into 1000s of **popular container images** on public registries. 51% of Docker images scanned has a **critical security vulnerability**

03

FTC fined a consumer DNA sequencing company after determining **1000s of customer's DNA information** was stored in **public S3 buckets**

What is My Cloud Risk?



Millions of Findings, 100s of Attack Paths, Not Risk!

Cloud Accounts
54

Overall Cloud Resources
2352

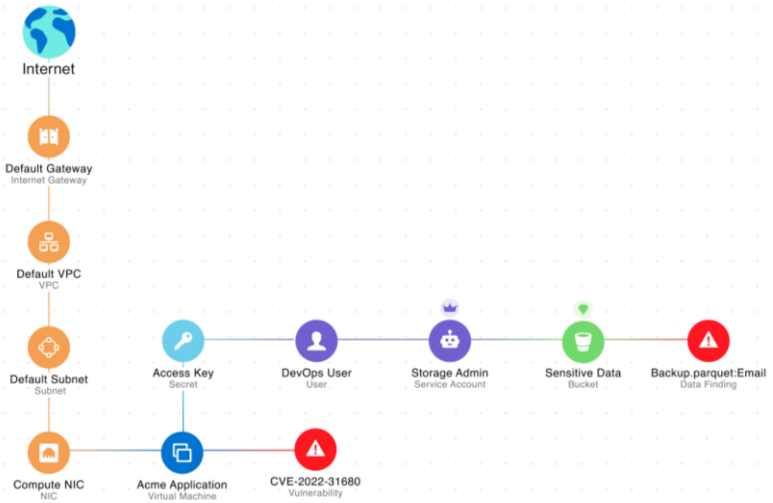
Vulnerable Public Instances
182 +10 (0.10%)
High Risk

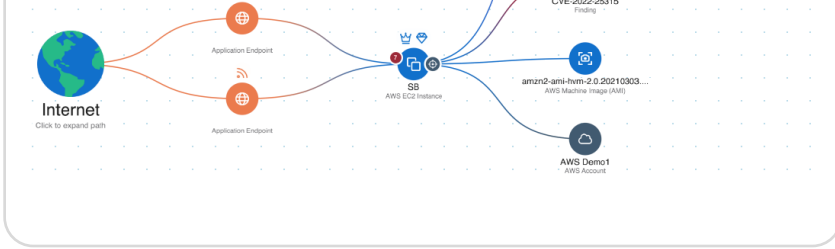
Critical Misconfigurations
251 +72 (40%)
High Risk

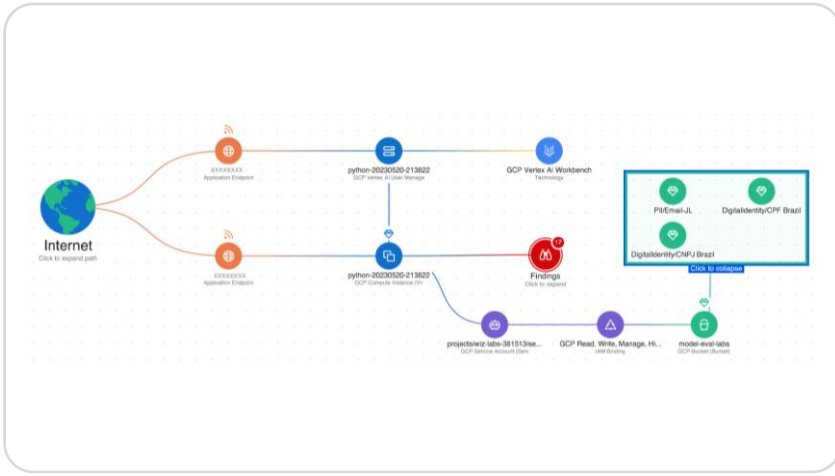
Container Images with Malware
128

Threats
4 +1 (33%)
Very High Risk

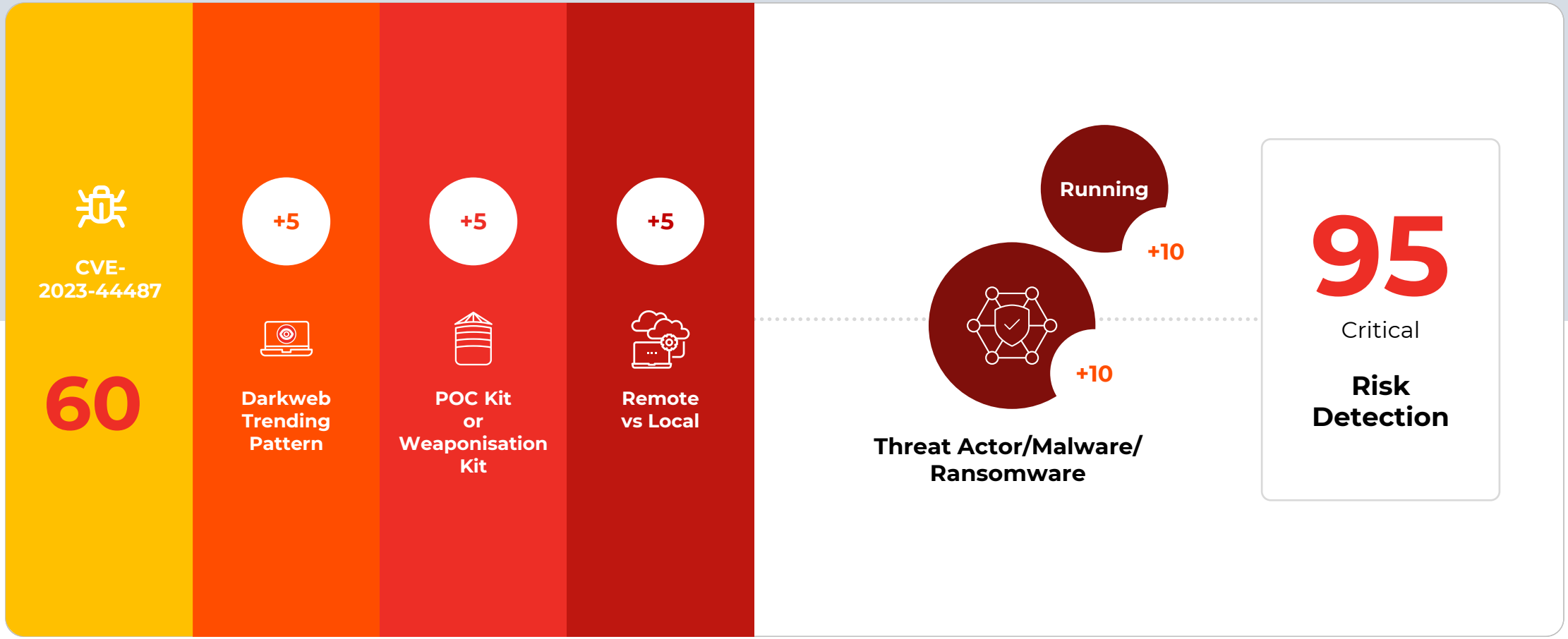
Perimeter Vulns
92







Step 1 Risk Based Vulnerability Prioritization



Risk Exposures

Combines Asset Environmental Factors Considers Only

- Active Service/Process
- Attack Path
- Public Exploit
- Public Asset Exposure

Threat DB of 25+ Threat Intel Sources | Researchers | Vulnerability Environmental

Vendor 1

Medium	CVE-2023-44487
High	CVE-2020-1147
Critical	CVE-2021-41303
Low	CVE-2023-42282
High	CVE-2025-0411
Medium	CVE-2020-11023

Vendor 2

Medium	CVE-2023-44487
Low	CVE-2023-42282
High	CVE-2020-1147
High	CVE-2025-0411
Medium	CVE-2020-11023
Critical	CVE-2021-41303

McAfee, FireEye, packet storm, GitHub, CISA, MISP Threat Sharing, Canadian Centre for Cyber Security, VDE, Reversing Labs, metasploit, Greynoise, MITRE ATT&CK, Kaspersky Industrial CyberSecurity, Talos, Google, EPSS

- Dark web chatter
- Trending patterns
- POC vs Weaponization
- Easy vs complex exploitation (remote vs local)
- Threat actors associated
- Exploited by Malware, Ransomware?
- Celebrity

100 | 95 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10

CVE-2023-44487

- POC of Exploit Exists
- Unattributed Threat Actors
- Trending In Mar & Apr 2025
- CISA Known Exploited Vulnerabilities
- CVSS – **7.5** & EPSS – **0.94437**

CVE-2020-1147

- POC Exists and Weaponized
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **7.8** & EPSS – **0.92695**

CVE-2020-11203

- POC of Exploit Exists
- Threat Actors – **Emissary Panda, Comment Panda**
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **6.1** & EPSS – **0.11526**

CVE-2021-41303

- Last Trending in Mar 2025
- CVSS – **9.8** & EPSS – **0.65449**
- CVE Is Not Exploited and No
- Other Significant Contributing Factors Observed

Comprehensive Risk Scoring is Critical

- Vulnerabilities (CVSS / EPSS)
- Malware
- Exploit Type
  Real Threat Indicator
- Certificates
- Unauthorized Software
- CISA KEV
- Exploited by malware threat actors
- Asset Critically
- Unauthorized Ports
- EoL & EoS SW, OS, HW
- Trending – Chatter, Dark Web
- Exploit Code maturity
- Location of the Asset
- Required SW Missing
- Custom Rule-based Risk factor

IMMUNITY · REVERSING LABS · GREYNOISE INTELLIGENCE · CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY · McAfee · VDE · MITRE ATT&CK · GitHub · MISP Threat Sharing · PROJECT ZERO · CANADIAN CENTRE FOR CYBER SECURITY · Square Security · metasploit · Kaspersky Industrial CyberSecurity · Google · EPSS · TALOS · packet storm · FIREEYE

TruRisk™ Score

Total Assets
110K

Total Findings
1.5M

Top Risk Factors

CISA/NCSC Vulnerabilities
143.2K

Internet Exposed Assets
20.4K

Misconfigurations
92.4K

Incidents
19

Step 2 : AI/ML-Threat Detections

Leverage AI/ML to detect & prioritize critical risk with maximum efficiency

AI-Powered Threat Detection

Identify threats in real-time with deep learning AI-based detection

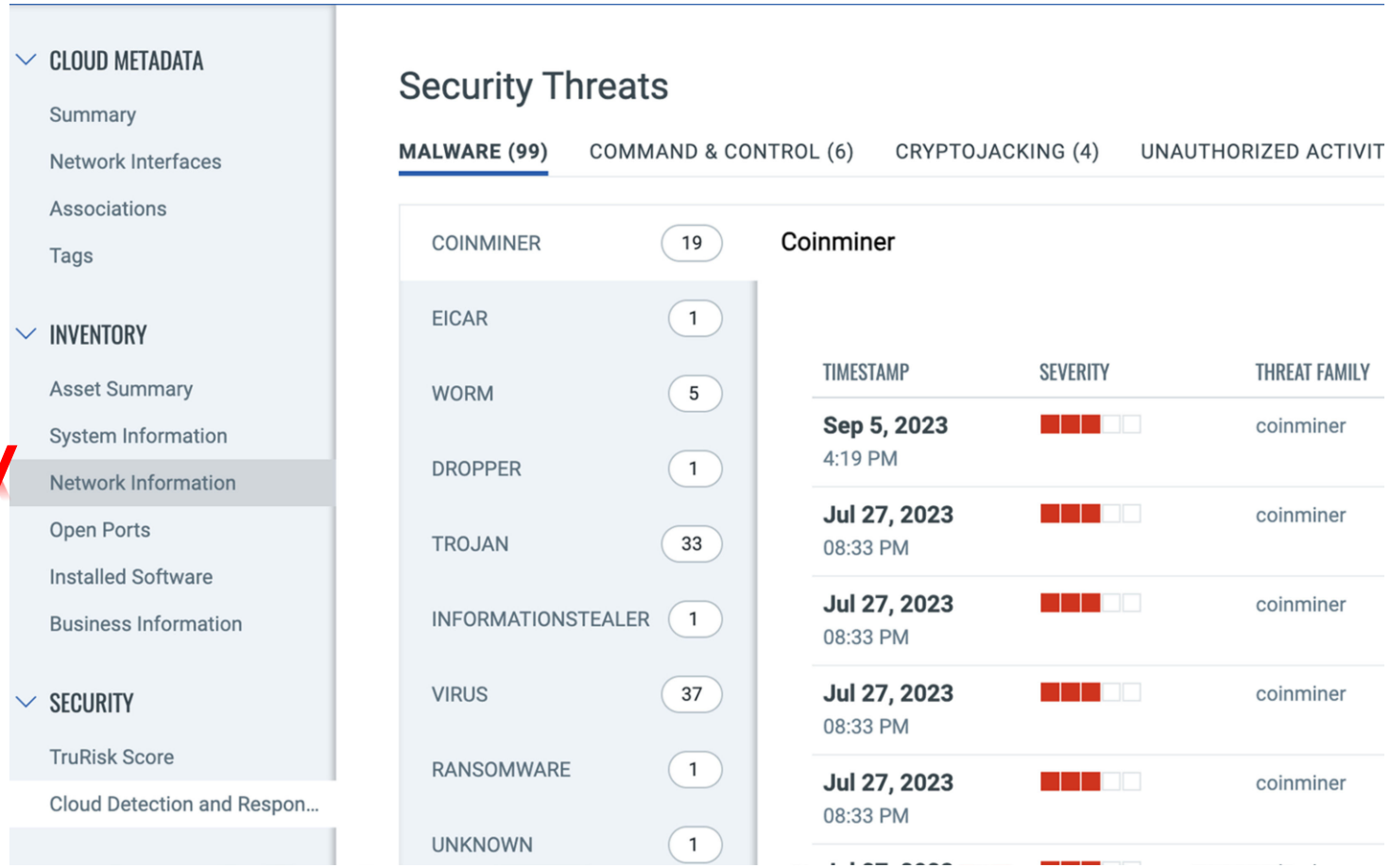
Malware

C2

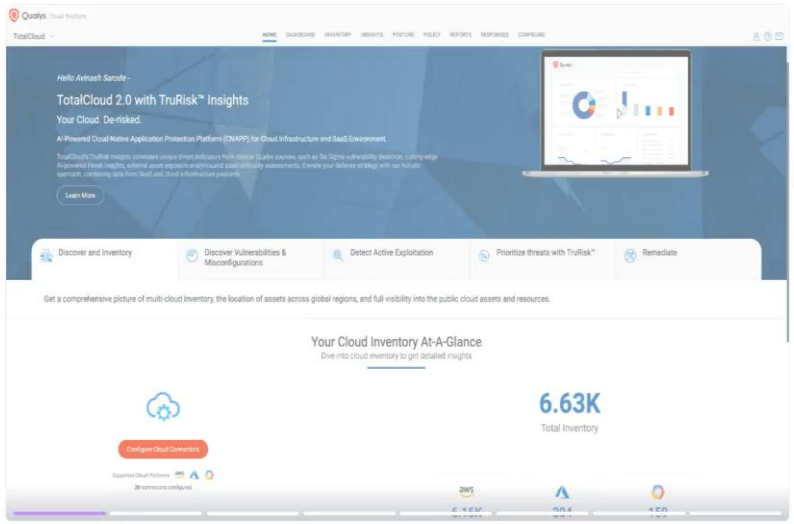
Unauthorized Activity

Cryptomining

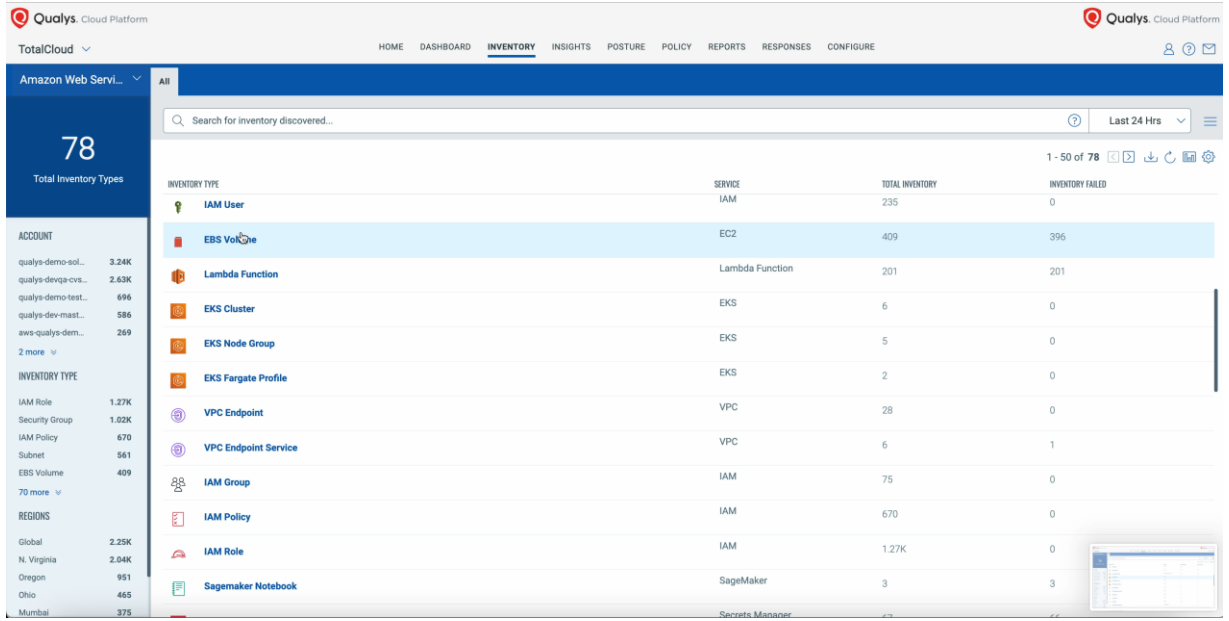
Suspicious Communications



Step 3
CSPM



Step 4
CIEM



Continuous Compliance Monitoring

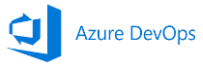
Step 5 Kubernetes and Container Security (KCS)

Containers Never Rest. Neither Should Your Risk Strategy

Build
Scan Your Dev Builds





CI/CD Scanning

Vulnerability & Secrets Scanning

Shift-Left Policy Controls

Release
Scan Your Repositories







Registry Scanning

Vulnerabilities

Zero-Day Malware

Secrets Detection

Deploy
Scan Your Production Environments

Cluster




Host



Serverless

VMDR for Containers With Attack Path Analysis

Policy Audit (CIS for Kubernetes, PCI 4.0)

Admission Controls – Zero-Trust Deployments

Runtime Security – Threat Detection & Response

Remediate with


Risk Insights

One prioritized view of risk, so you can fix what matters most...FIRST

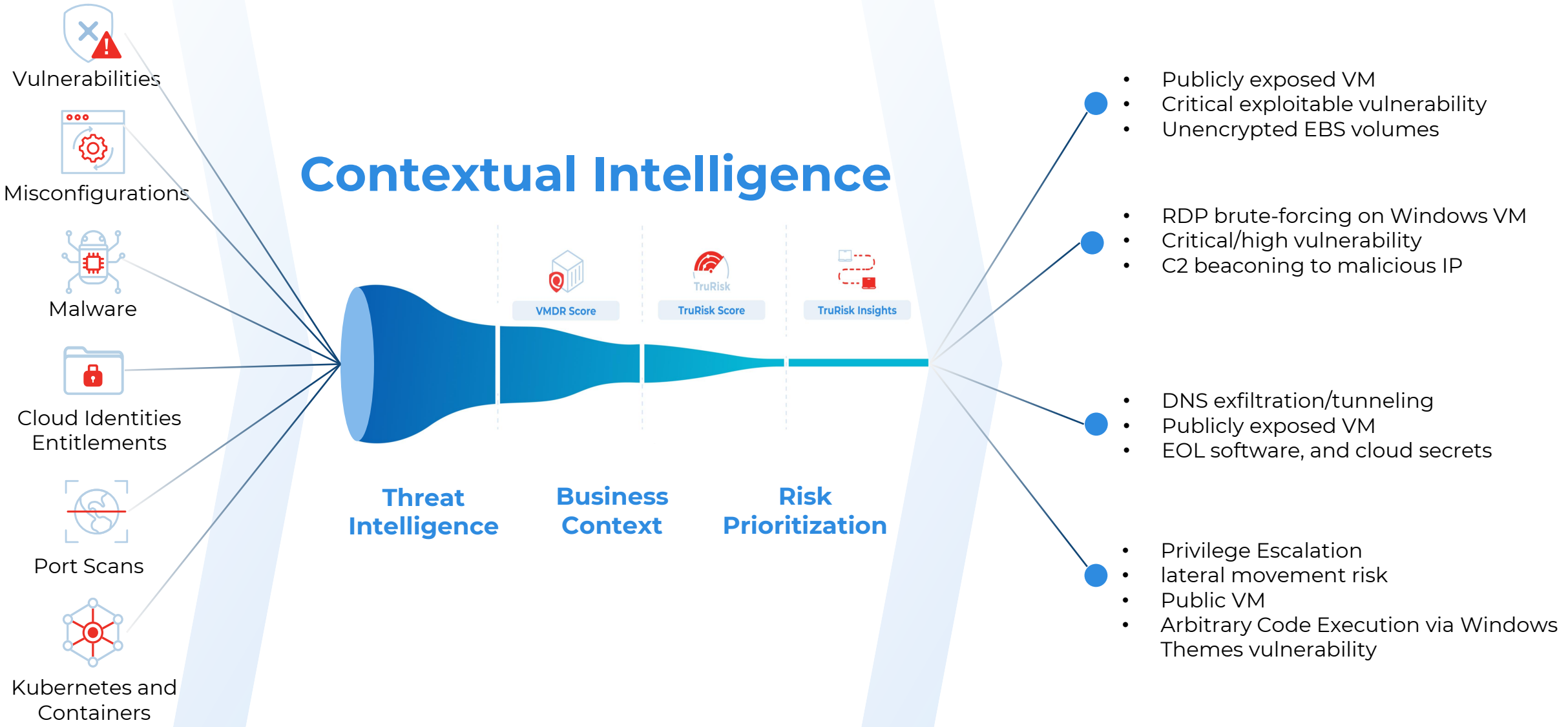
Risk Multipliers

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


Vulnerabilities
Misconfigurations
Malware
Cloud Identities Entitlements
Port Scans
Kubernetes and Containers
Contextual Intelligence
VMDR Score
TruRisk
TruRisk Score
TruRisk Insights
Threat Intelligence
Business Context
Risk Prioritization
Publicly exposed VM
Critical exploitable vulnerability
Unencrypted EBS volumes
RDP brute-forcing on Windows VM
Critical/high vulnerability
C2 beaconing to malicious IP
DNS exfiltration/tunneling
Publicly exposed VM
EOL software, and cloud secrets
Privilege Escalation
lateral movement risk
Public VM
Arbitrary Code Execution via Windows Themes vulnerability

Focus On The Findings That *Actually Matter*

From Attack Surface to Risk Surface

Operationalize Container Risk to Reduce Noise, Cost, and Time

Contextualize Your Attack Surface

5M Images Scanned

3M images Blocked in CI/CD

2M secure images deployed

Focus on what's actually running—not just what's scanned

Prioritize Risk With Multi-Dimensional Context

Burn down the noise. Focus on the few risks that lead to real impact.

Shift-Left With Runtime Intelligence

Vulnerability Response

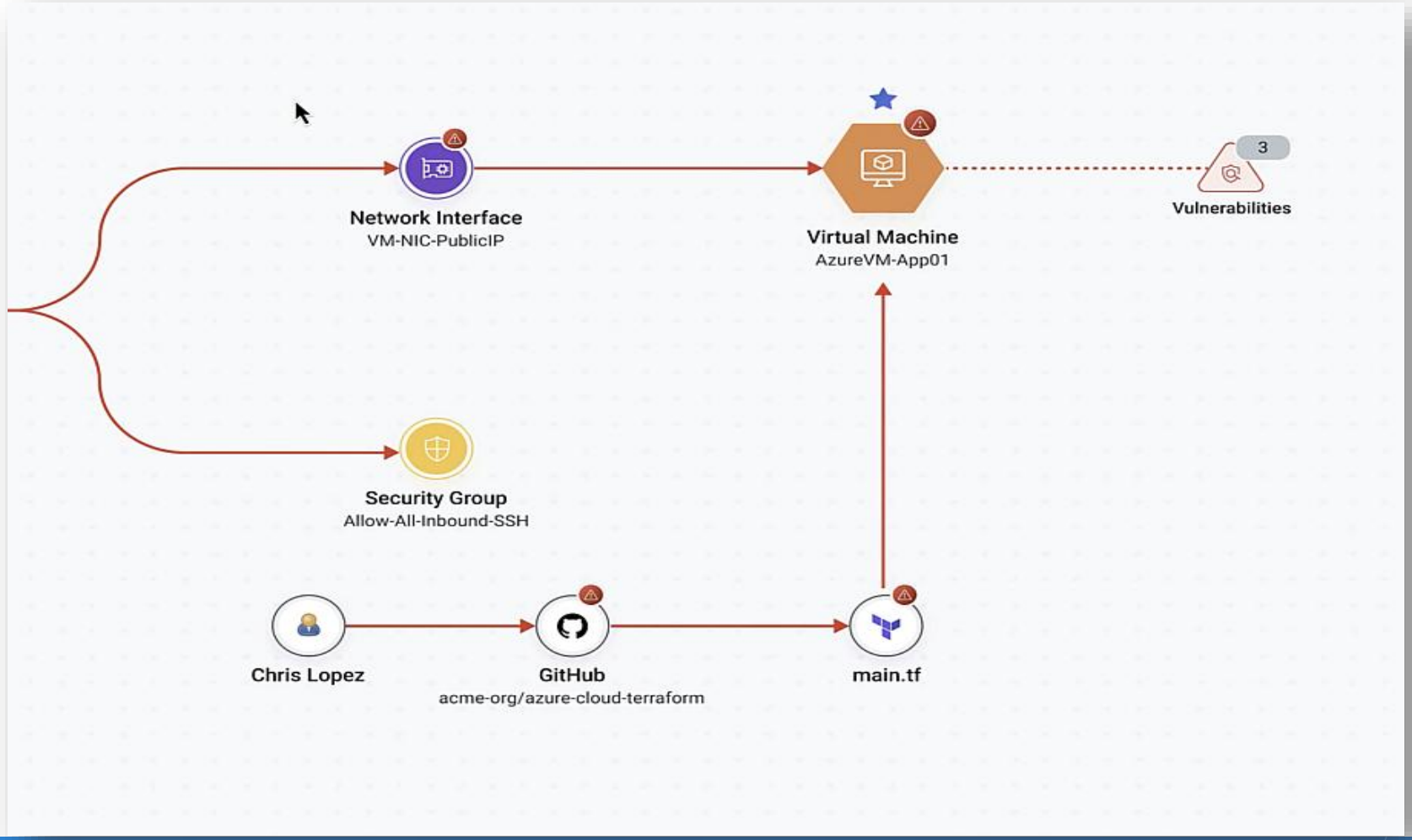
Reduce MTTR < 48 hr

Threat Response

Reduce MTTD < 10 min

Enforce Zero Trust by turning runtime learnings into compliant guardrails.

Prioritizes Risk, Leveraging Attack Paths...



Auto-Remediations

Cloud Risk Remediations

Patch

- Automatic Playbooks For CISA KEVs
- Fully automate patch deployment based on attack paths
- Full support for any host, on-prem or cloud

Mitigate

- Leverage Playbooks to apply compensating controls while waiting for patch
- Includes ability to limit privileges, restrict network access, and any API supported by your CSP
- Apply Admission Control Policies in Kubernetes

Isolate

- Isolate hosts/VMs to ensure vulns cannot be exploited
- Allow exceptions to ensure workloads and images can be patched and managed

Cloud Workflow Automation

Cloud Workflow Automation

- **Workflow** automation enables the creation of automation workflows to enable custom controls, enrichment and remediations.
- The workflow system should be no code low code system, that allows rapid creation for workflows through a visual interface.

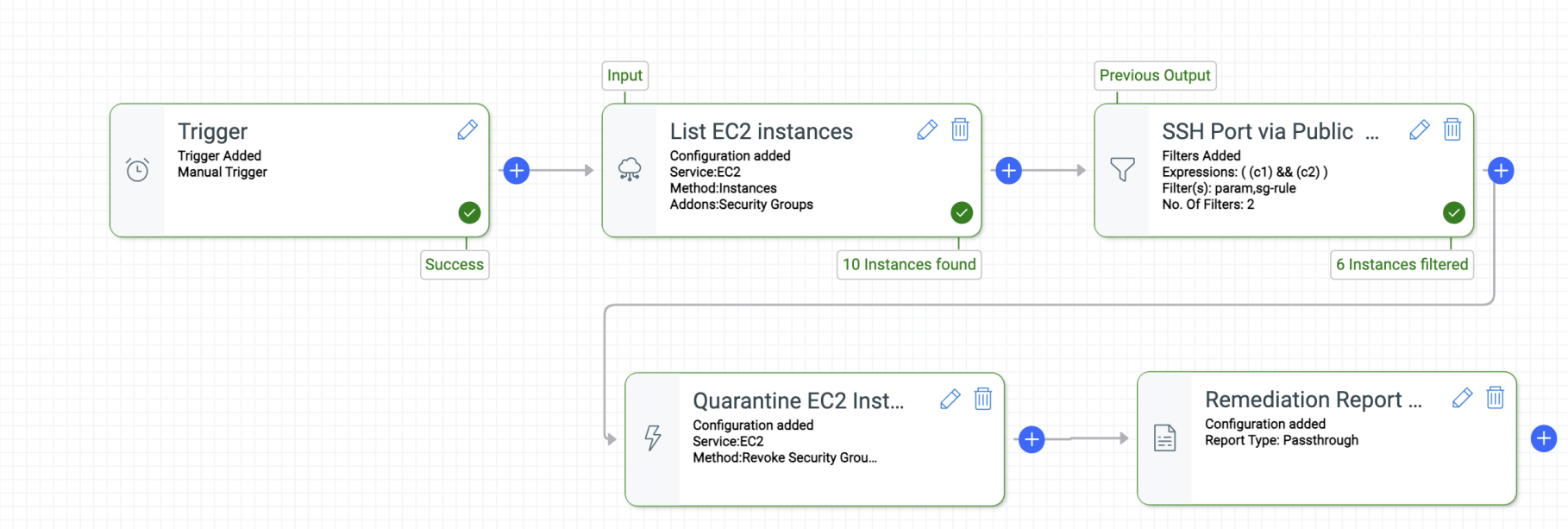
No Code / Low Code Workflow Automation Through Visual Interfaces

Remediation Workflow To FIX A Misconfiguration

Fix A Failed CIS 3.0 Recommendation 5.2/5.3 Benchmark Control

Problem – EC2 Instances Exposed to Public on SSH Port

Workflow Actions – Automatically Quarantine without impacting running applications and report the findings.



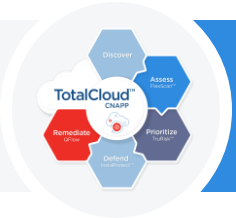
Keep Library of Cloud Playbooks

Automate to Reduce MTTR (Meant Time to Remediate)

Shift Left in Cloud and Supply Chain Security

Evaluate Code before deploying to the Cloud

Shift-Left Security
Proactive Approach



Runtime Security
Reactive Approach

Pre-Deployment

Infrastructure as Code (IaC)

Terraform
Cloud Formation
ARM Template

Repository and Registries

GitHub
Bitbucket
Gitlab

AMI Scanning

CI/CD

Jenkin
Bamboo

Pipeline Composition Analysis

Post-Deployment

Cloud

AWS
Azure

Instance/Containers/ Serverless/WebApp

Resources

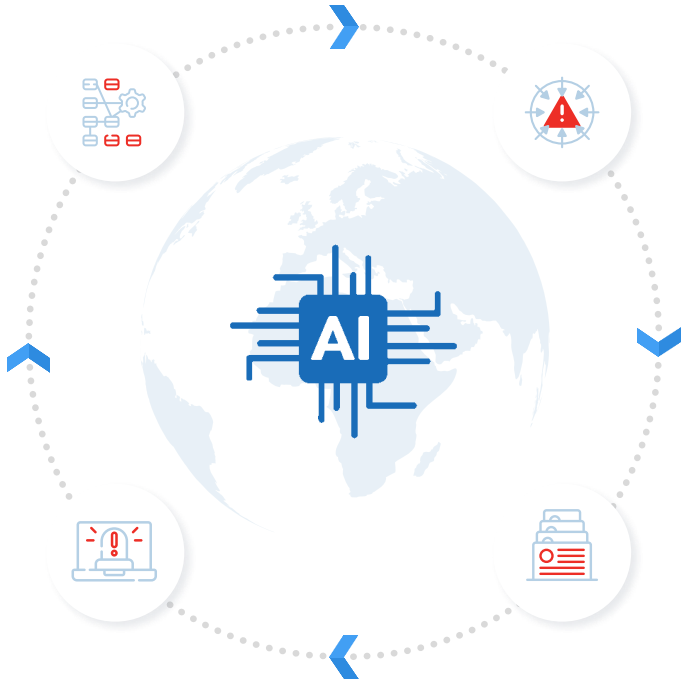
Identities

What about AI Risks

Single platform for a unified view of LLM risk, AI-Workloads, and AI-vulnerabilities

Know where AI is running

- Discover all your AI-Workloads
- Get inventory of AI packages, AI-software and AI-hardware (GPUs)
- Risk and Business context



Know the risk of AI Infra vulns

- 1000+ AI-specific vuln detections correlated with threats for TruRisk
- Patch vuln risks to harden Infra from model and data theft
- Monitor latest AI threats & Threats to AI, LLMs

Know the risk of Model and Data Thefts

- Scan LLM and Application endpoints
- Prompt your LLMs for OWASP TOP 10 to ensure they are not leaking data, showing bias, or can be jailbreak.

Be Audit-ready for using AI

- Prevent fines due to compliance violations (e.g., GDPR, PCI)
- LLM security report for management

Leverages existing Agent and Scanner

Supply Chain Risk from Open Source

... And OSS Packages are Ubiquitous in First-Party and Third-Party Software

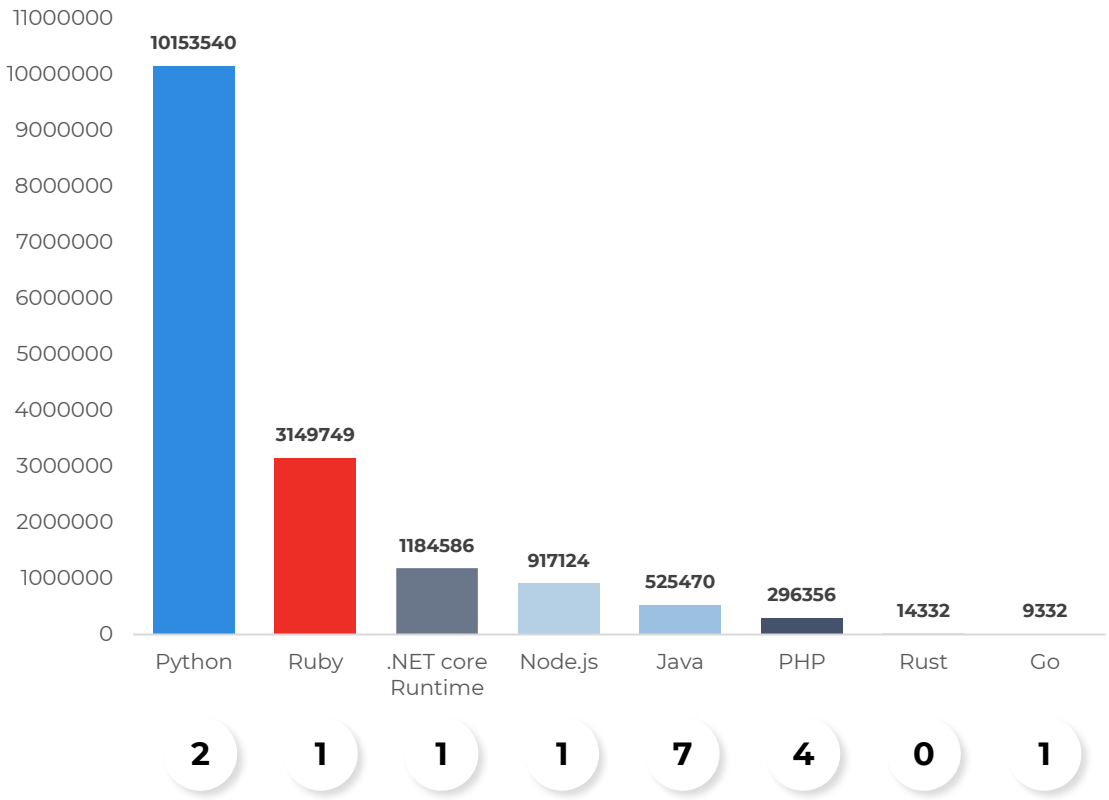
96%
Codebases contains OSS

90%
Organizations use OSS Software

48%
Codebases have high-risk OSS vulnerabilities

56
Average Vulnerable OSS packages per asset

Installation Numbers



Contextual Cloud Risk Framework

1. **Plug-in the Risks**
2. **Contextual Intelligence**
3. **Act on Attack Insights**

Steer Clear of : Cyber Tourism, Gamification or Shiny Object Syndrome

Qualys.

Bring your cloud into focus with one prioritized view of risk.

TotalCloud 2.0

with **TruRisk Insights**

Your Cloud. **De-risked.**

Start your Free Trial

Speak to an Expert

Schedule a Demo

DE-RISK YOUR **BUSINESS**

Qualys.


25
YEARS OF
REDUCING
CYBER RISK

Corinium
connected thinking

Thank you

Connect on LinkedIn

Scan me!

Nirav Kamdar
Security Solution Architect, APAC, Qualys Inc
E: **nkamdar@qualys.com**

Qualys®

Qualys®