FORTINET

FORTINET XPERTS SUMMIT 2025

FortiCNAPP Recap & Guided CTF

Filippo Caliari

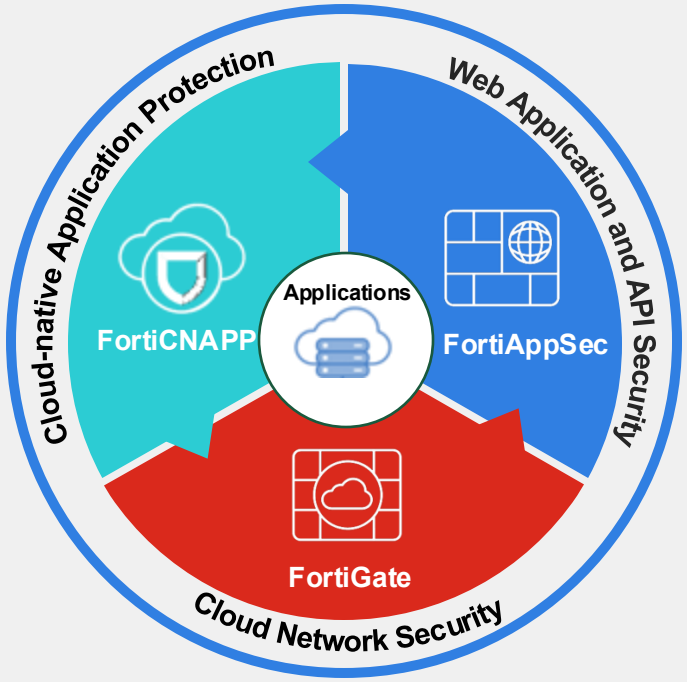
Francisco Menezes

Comprehensive Integrated Code-to-Cloud Security

360-degree cloud defense-in-depth protection against all threat and risk vectors

Secure everything from code to cloud faster with **unparalleled context and visibility with a single unified platform**.

- CSPM
- KSPM
- CWP
- CIEM
- IaC
- Code Security



Integrated AI/ML-driven platform to protect business-critical web applications and APIs from attacks that target known and unknown vulnerabilities.

- WAAP
- GSLB
- Bot Mitigation Management
- Threat Analytics
- DAST

Achieve network visibility and enforcement of **consistent security policies** across private, public, and telco clouds.

- Virtual FW
- Cloud-native FW

How to Address the Native Cloud Security Challenge

Identifying, Prioritizing and Resolving Risks and Threats in Cloud-native Applications

Minimize Attack Surface

Gain comprehensive visibility and proactively reduce vulnerabilities, misconfigurations and excessive privileges without slowing down development.

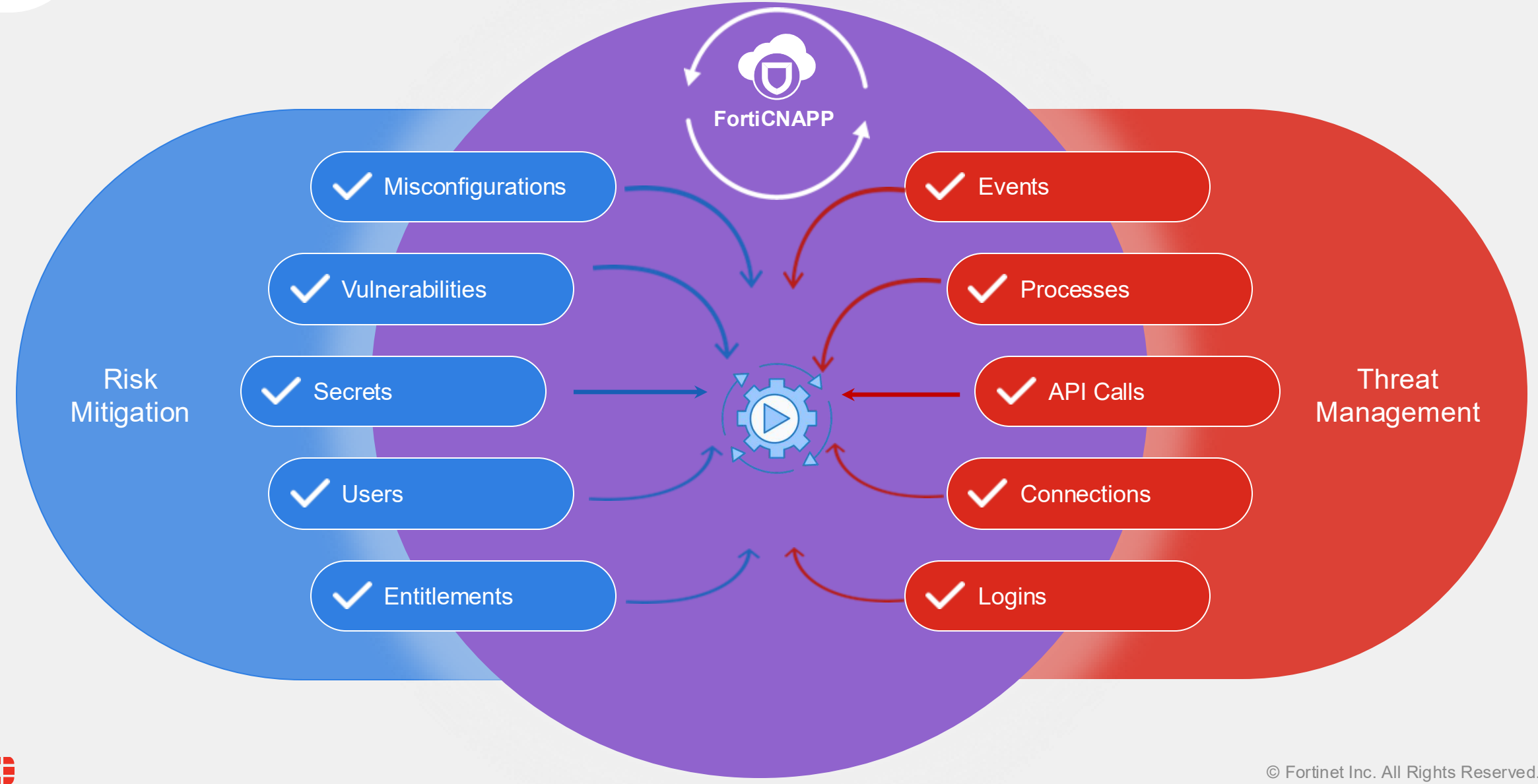
Continuously Monitor Risks

Continuously assess virtual machines, containers and Kubernetes workloads to address active risks before they are exploited.

Reduce Threat Impact

Quickly detect, investigate and respond to unusual behavior and active threats including the use of compromised credentials, cloud ransomware and cryptomining.

Prioritization Requires Combining Risk and Threat Context



FortiCNAPP Integration – Step 1:
Read only cloud environment

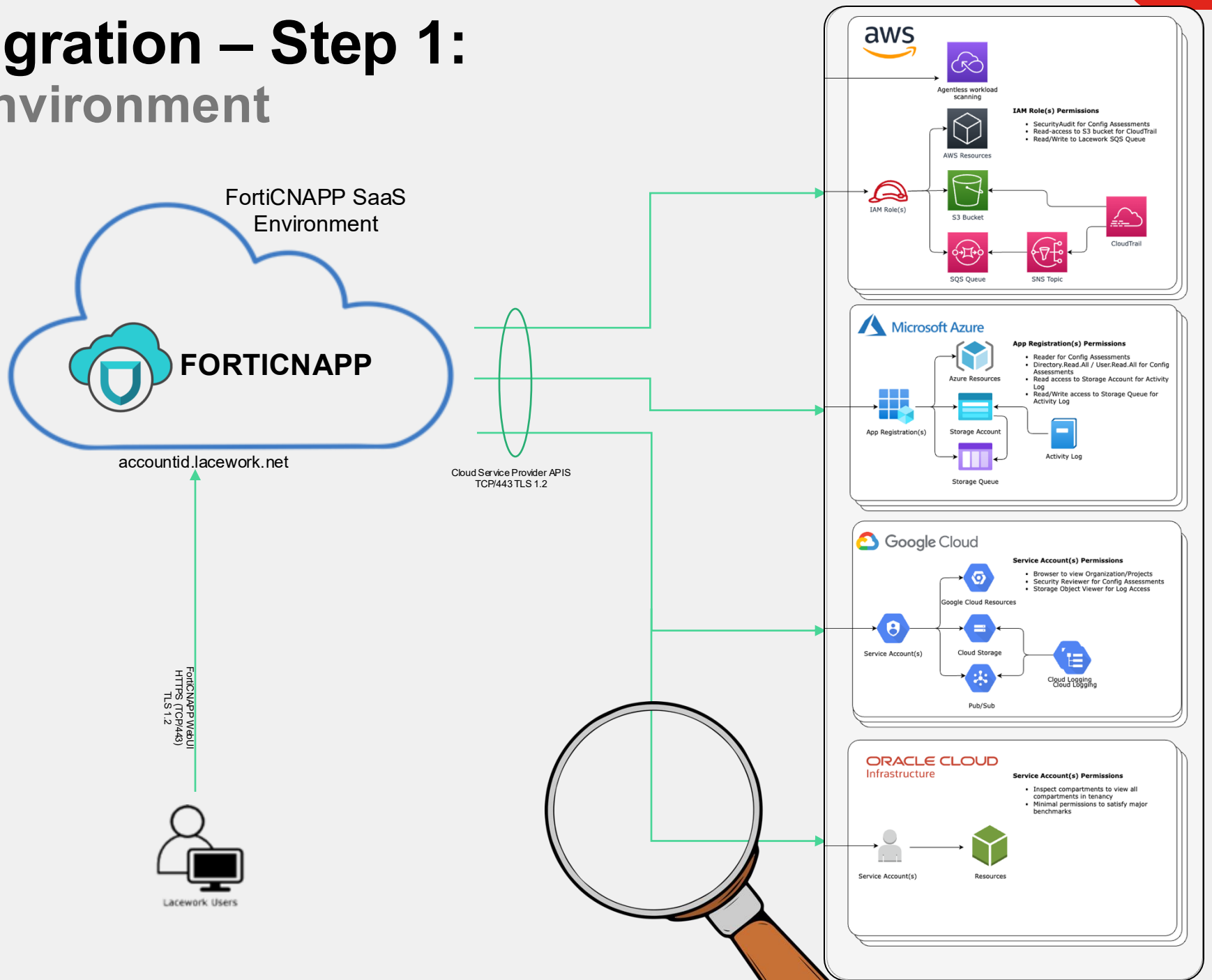
Inventory

CSPM + KSPM

CIEM

Vulnerability

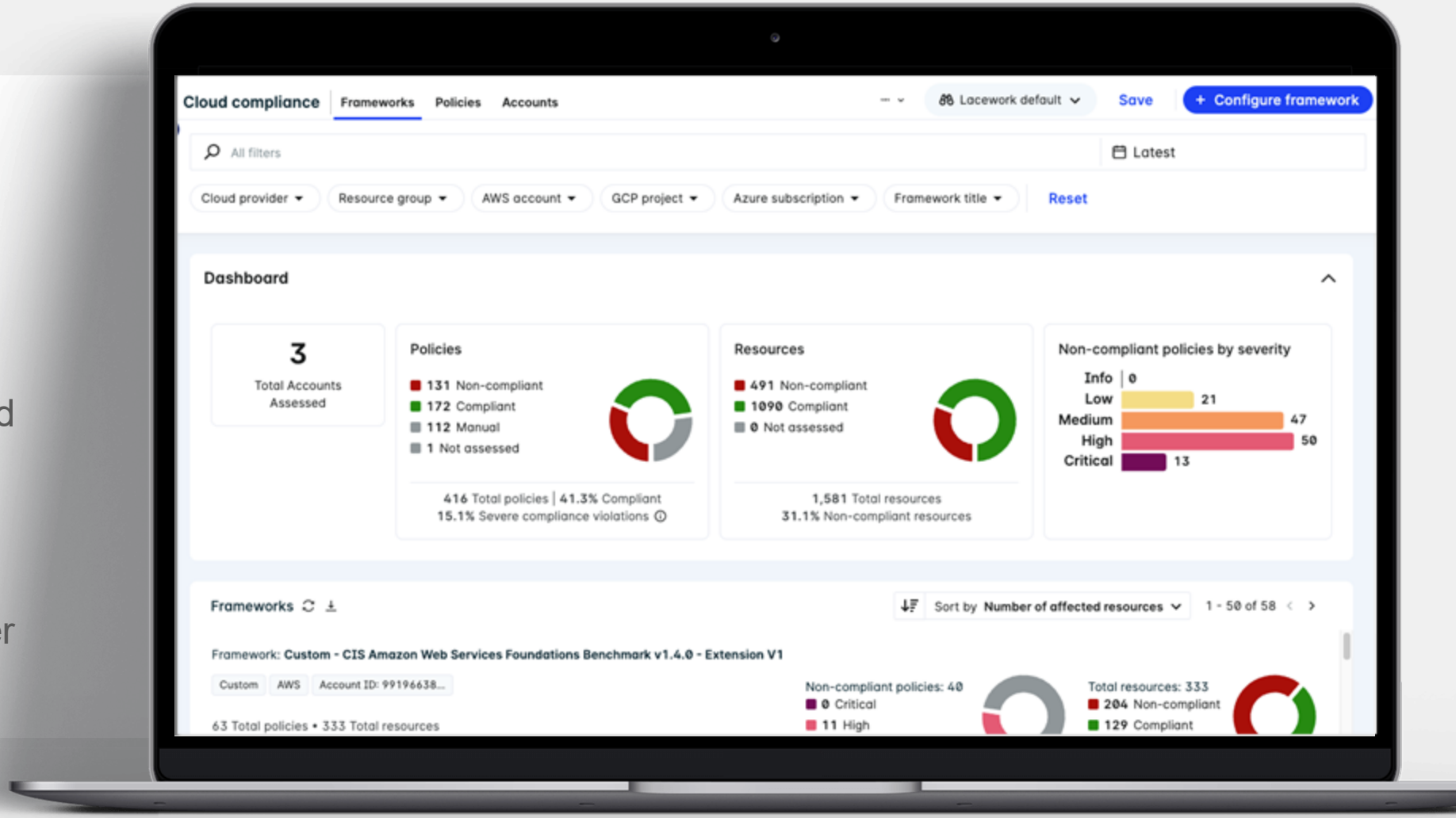
CWP agentless



Cloud Configuration

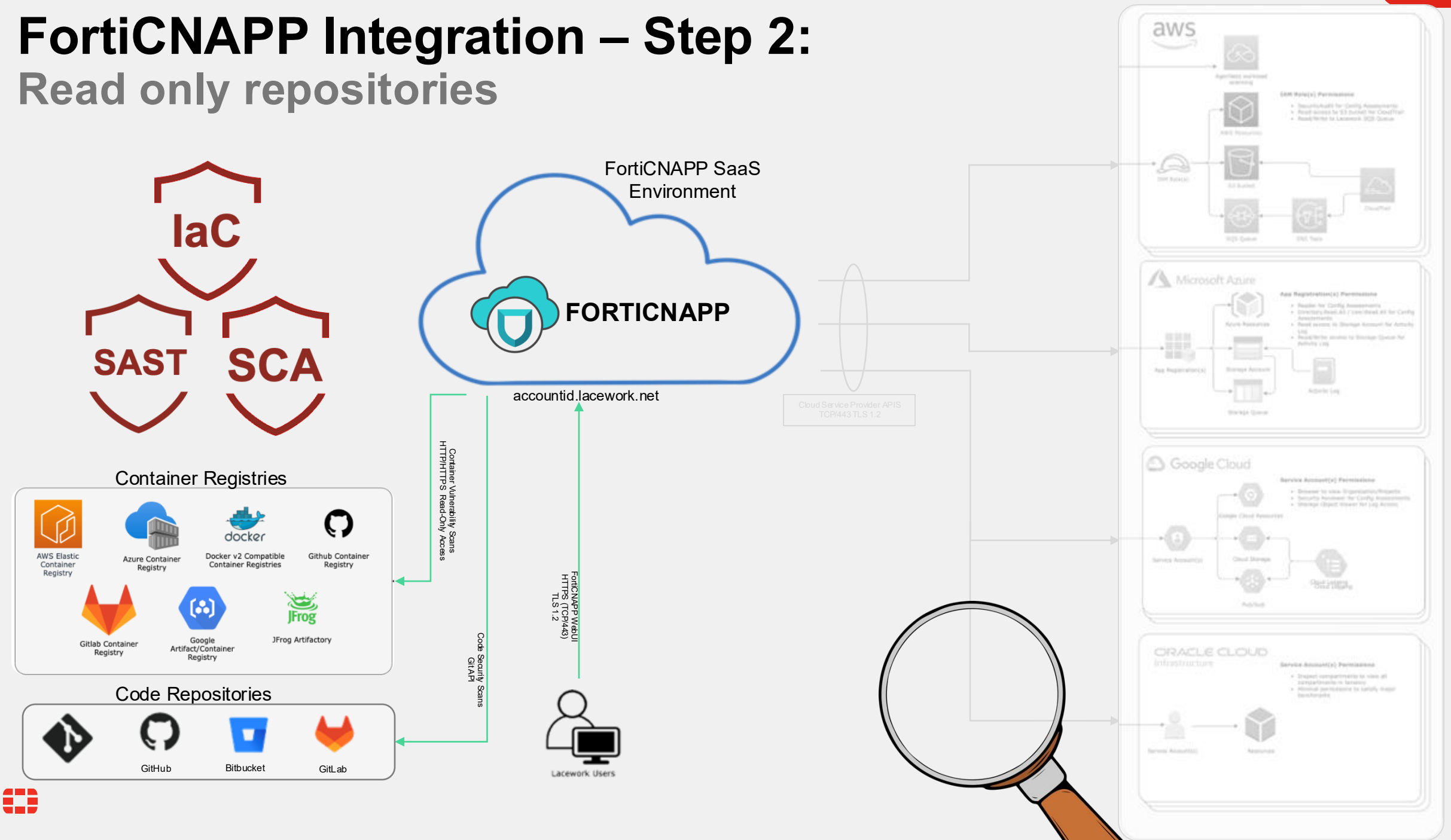
Security Posture Management CSPM and KSPM

- Gain complete visibility of continually changing cloud resources
- Continuously monitor for misconfigurations
- Achieve compliance faster



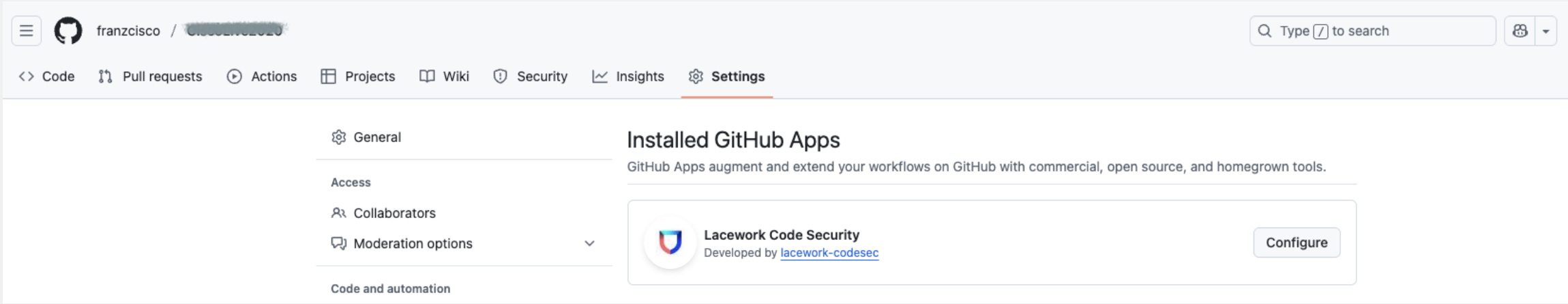
POSSIAMO VEDERE UNA DEMO?

FortiCNAPP Integration – Step 2:
Read only repositories



Code Security

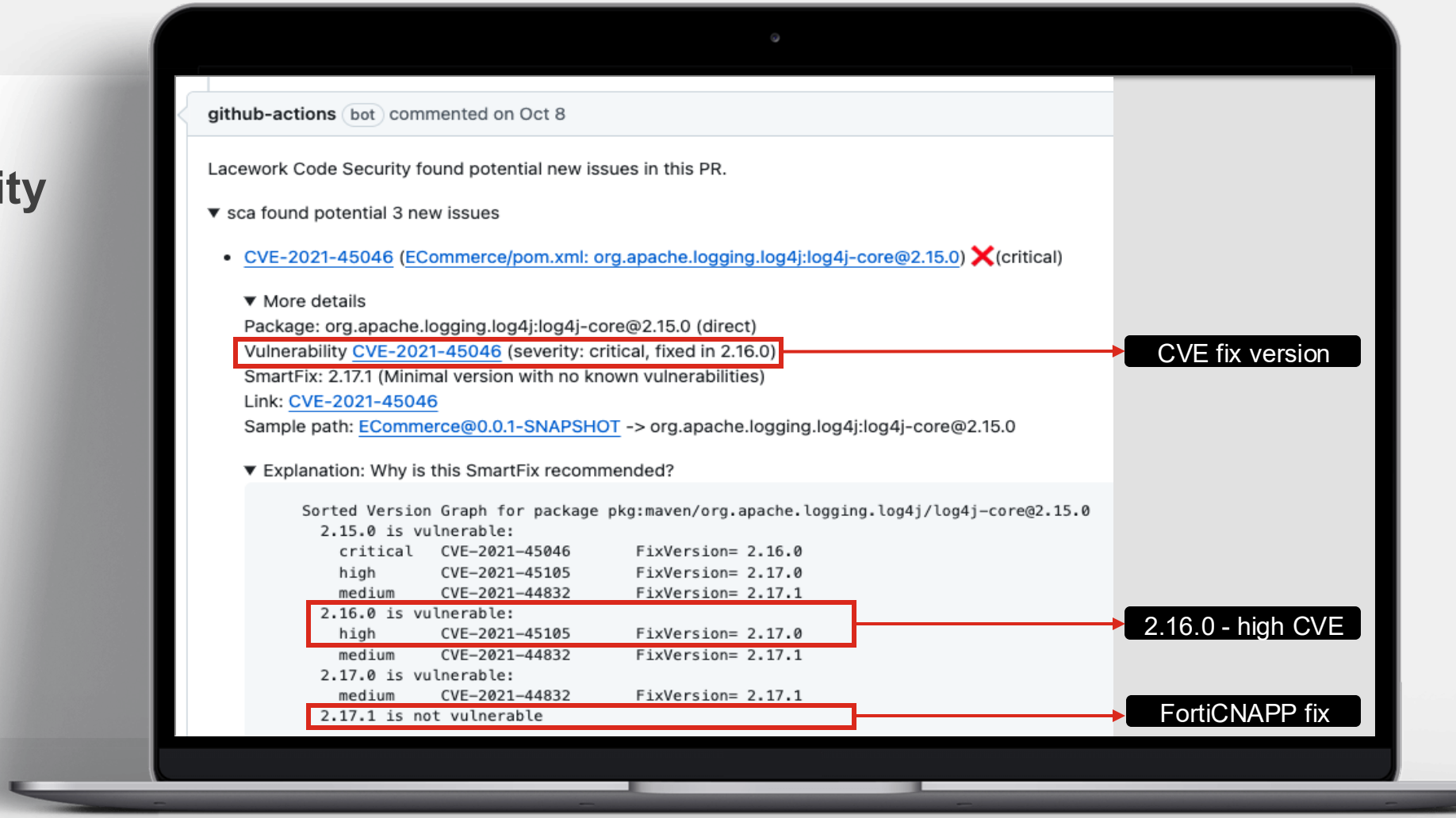
FortiCNAPP registers itself as a GitHub App.
Lacework FortiCNAPP Code Security will automatically scan the default branch of all your repositories. Once the scans are completed, you will be able to see the results in the UI.



Shift Security Left to Reduce Risk and Remediation Costs

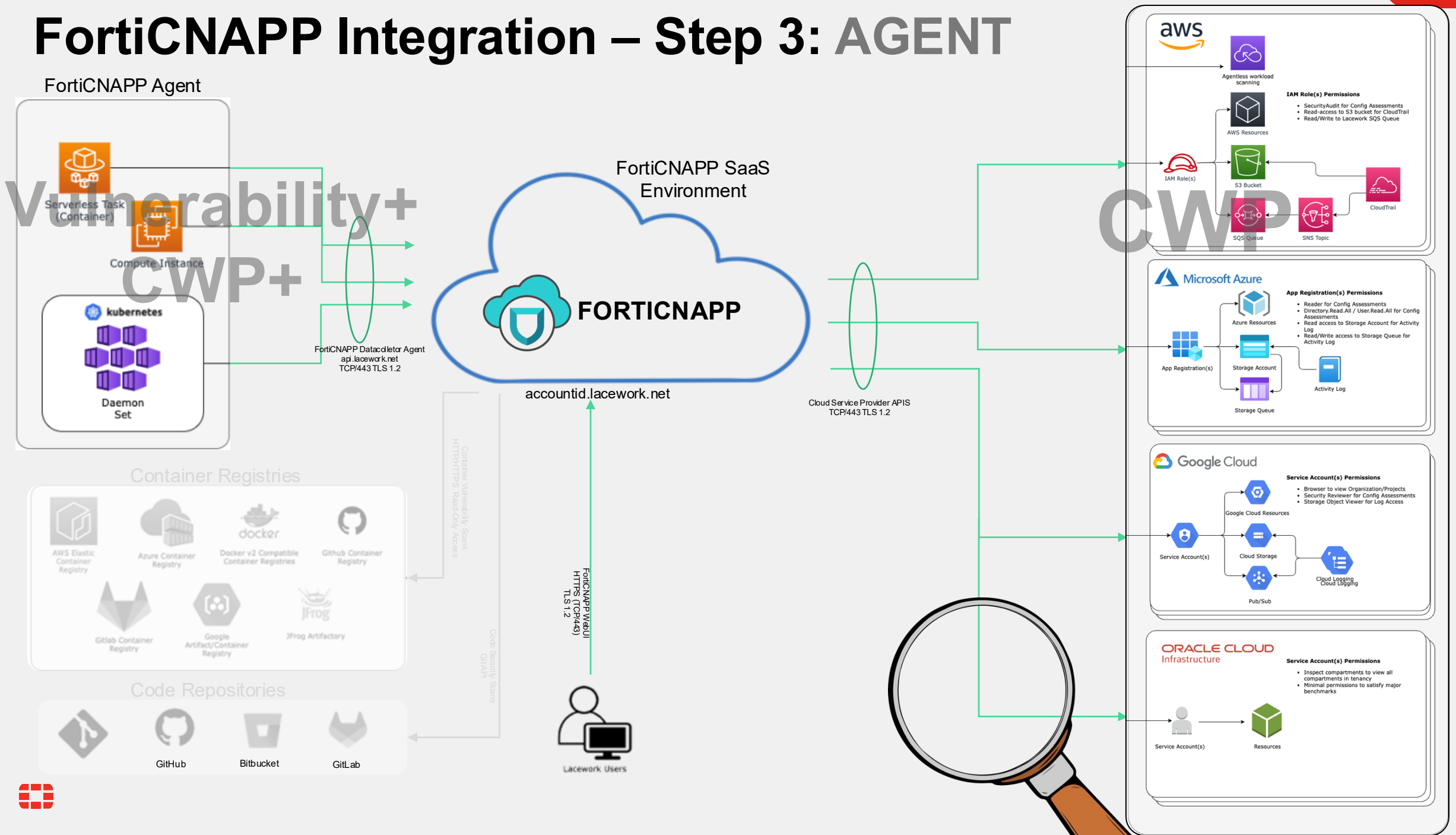
Application and Infrastructure Security

- Gain visibility of software supply chain (SBOM)
- Identify third-party code CVEs (SCA)
- Detect first-party code weaknesses (SAST)
- Secrets detection
- Verify cloud infrastructure configuration (IaC)

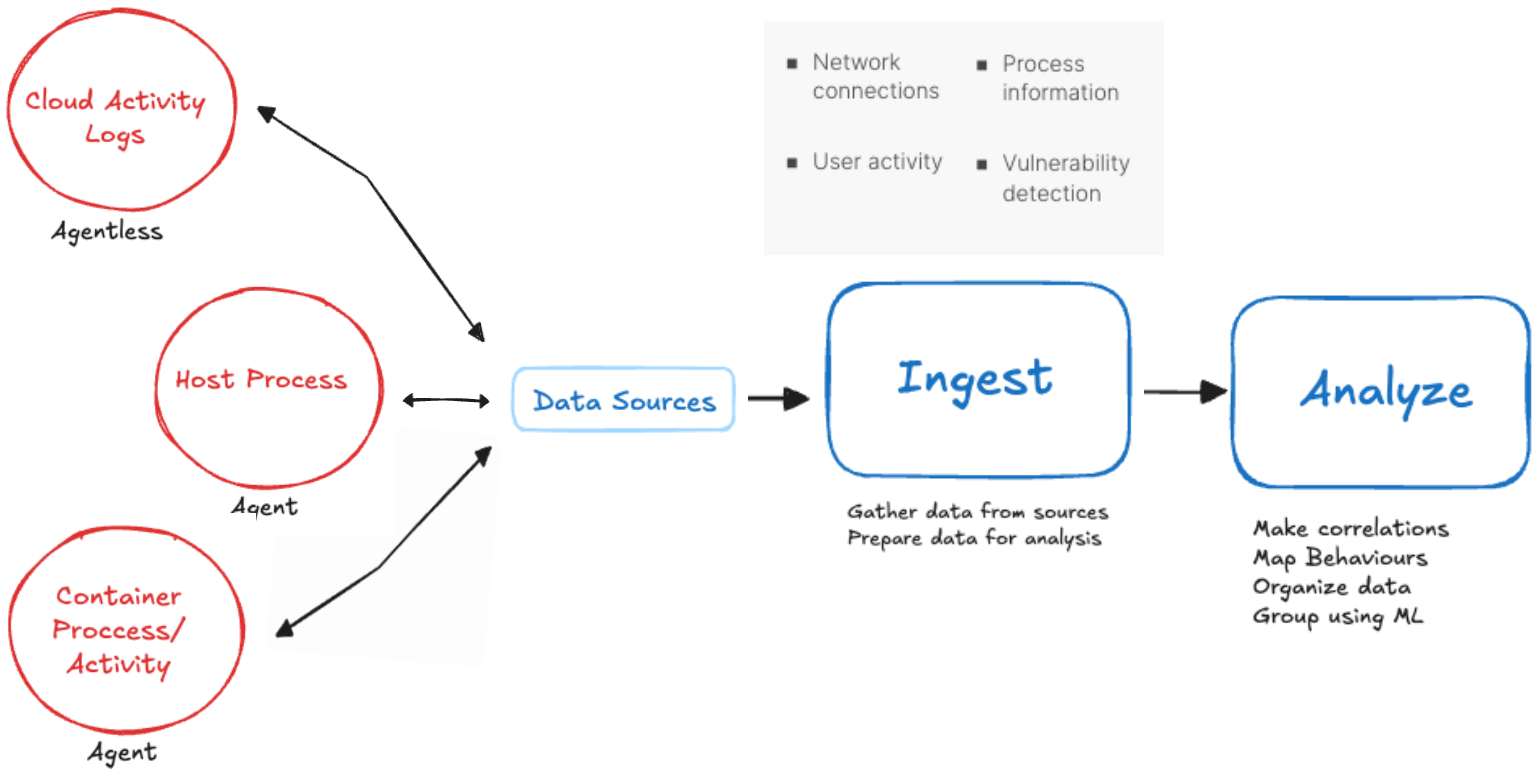


POSSIAMO VEDERE UNA DEMO?

FortiCNAPP Integration – Step 3: AGENT



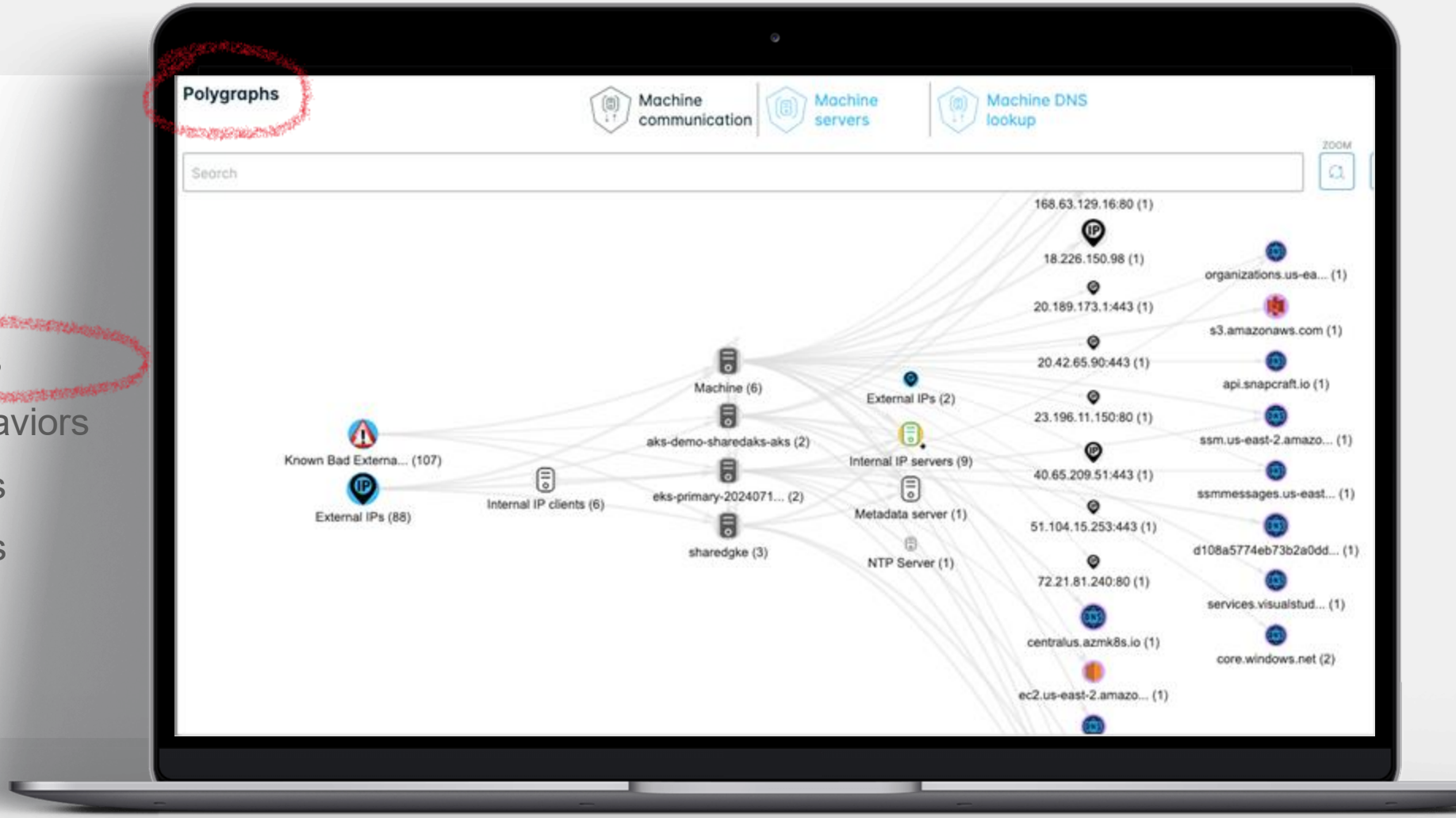
Runtime Protection



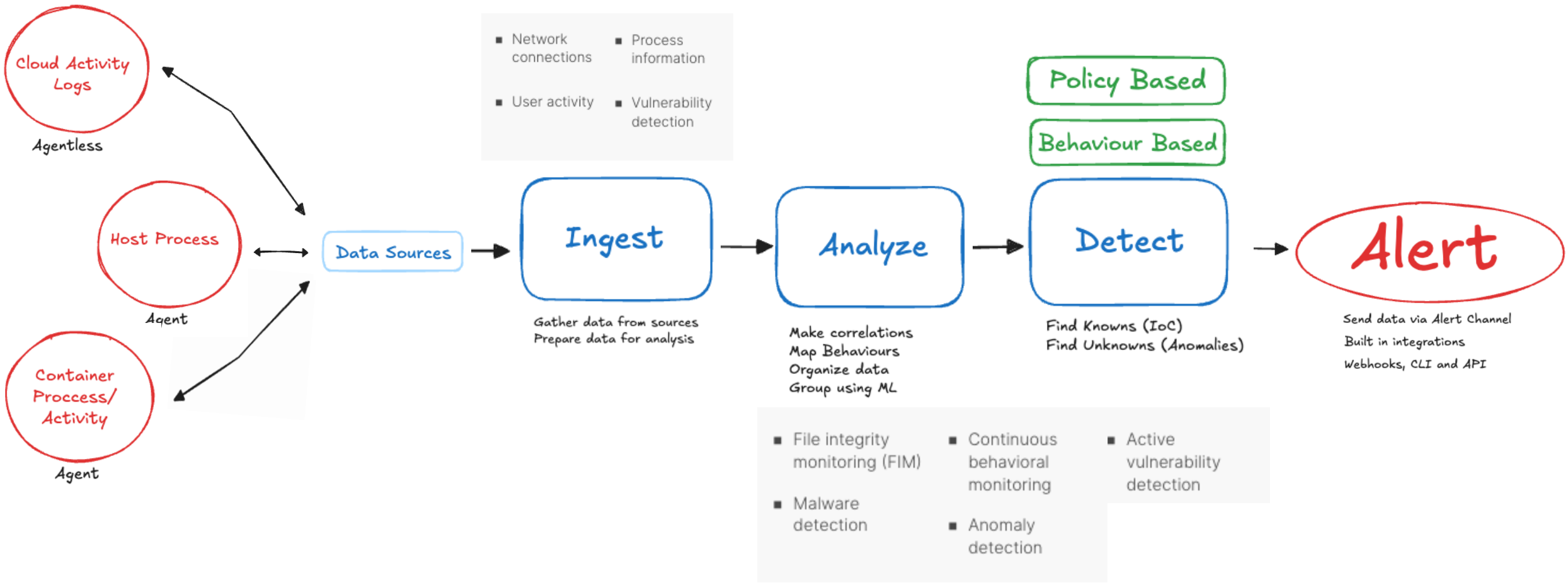
Runtime Protection

Cloud Workload Protection Platform (CWP)

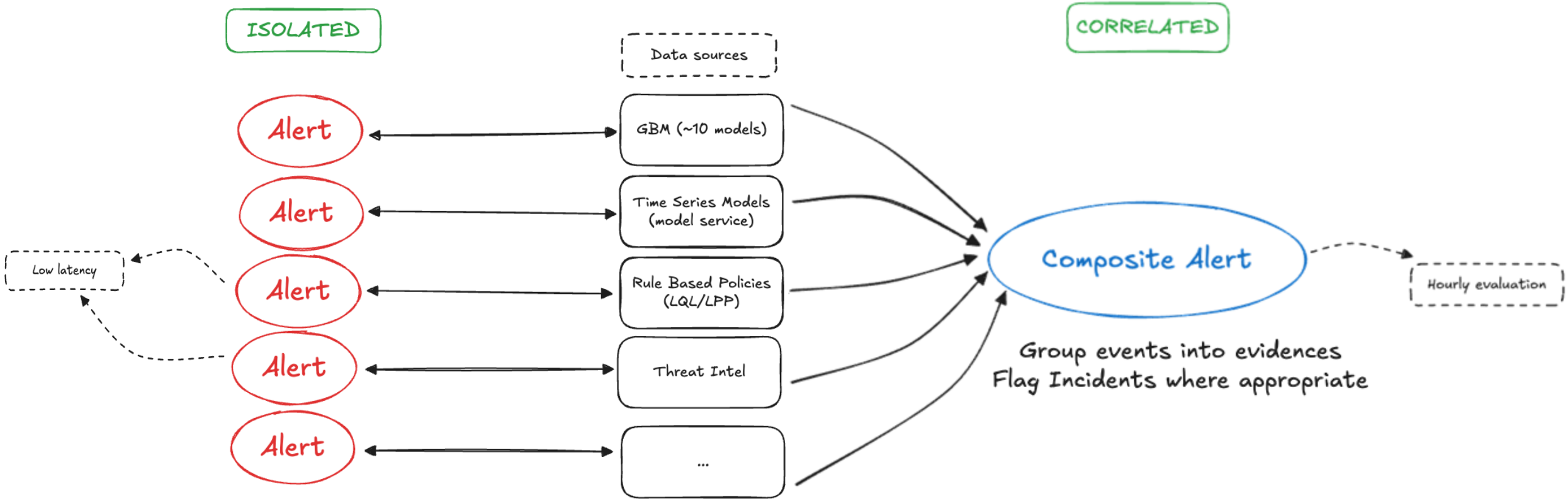
- Map network connections
- Discover anomalous behaviors
- Detect in-progress threats
- Find vulnerabilities across hosts, containers and Kubernetes (K8s)



Runtime Protection

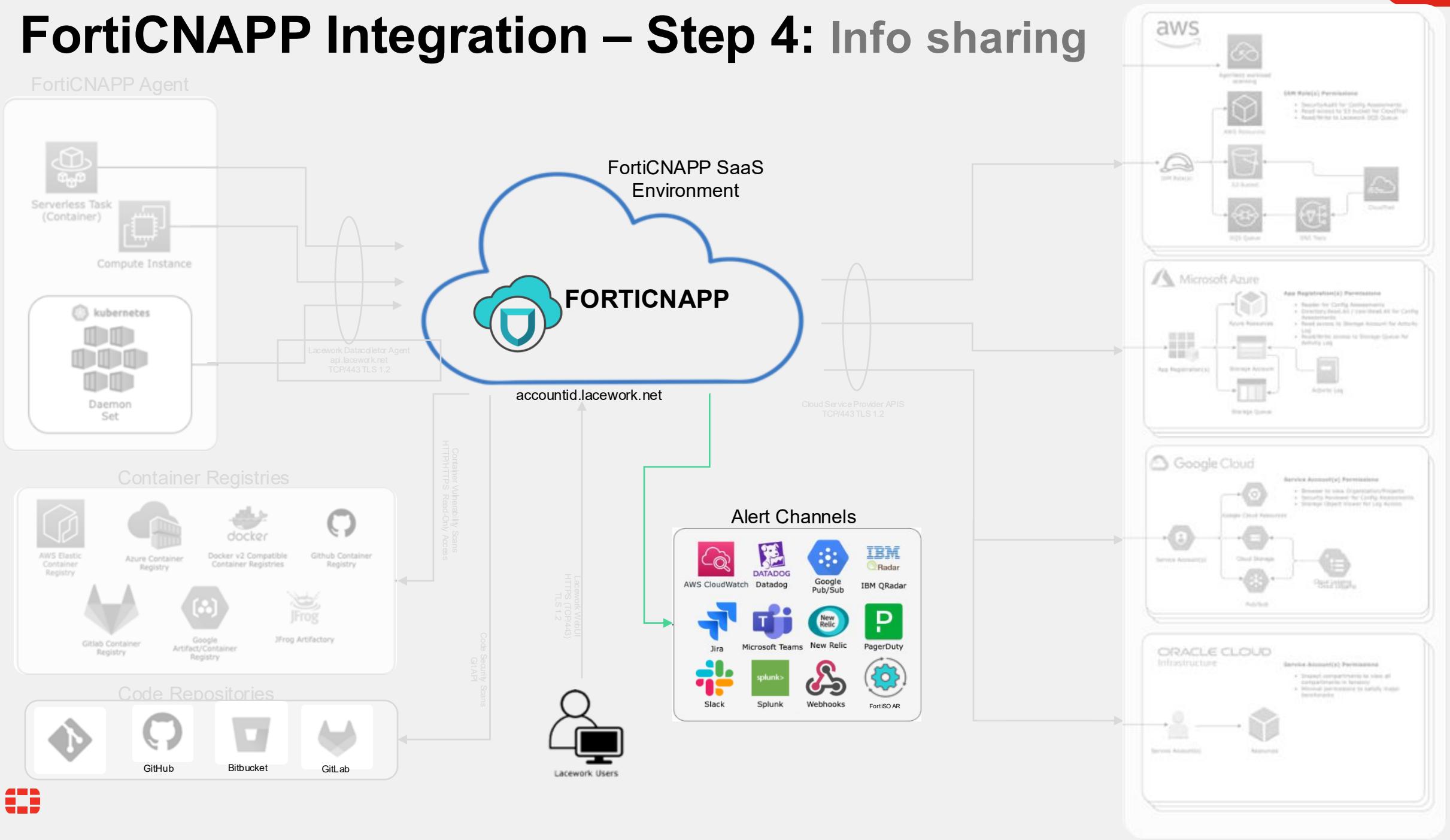


Alerting



POSSIAMO VEDERE UNA DEMO?

FortiCNAPP Integration – Step 4: Info sharing



FortiSOAR Automated Response

Automated threat investigation and response

Composite Alert

High fidelity low volume **actionable alerts**.

Respond

Automated response in AWS, Google Cloud and Azure

Google Cloud

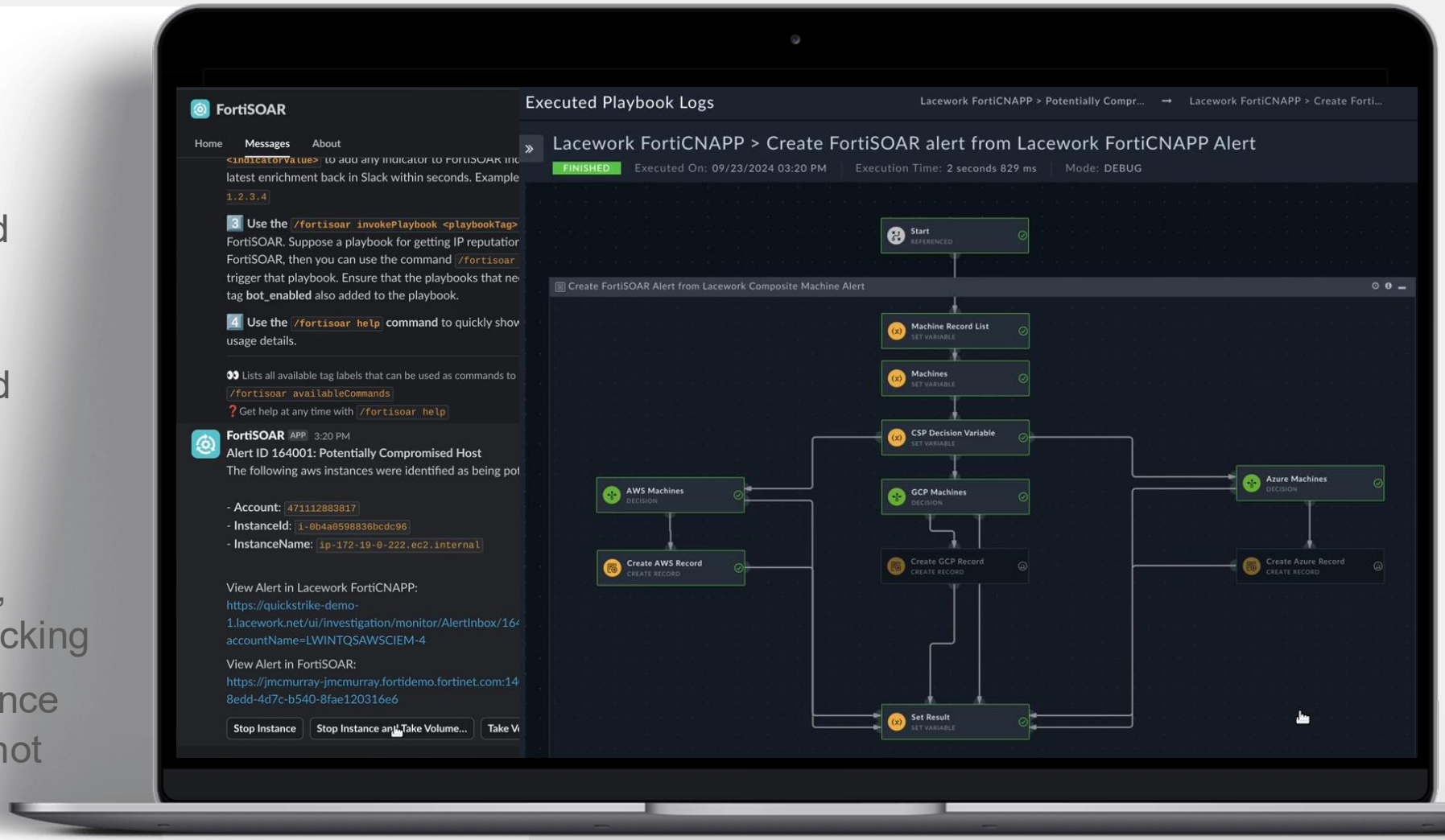
aws

Azure

Automate Threat Response

Accelerate Alert Response Times

- Automate remediation and blocking of active runtime threats
- Easily customize and build granular playbooks for FortiCNAPP alerts
- Quickly respond to compromised credentials, ransomware and cryptojacking
- Stop Instance, Stop Instance & Snapshot, Take Snapshot



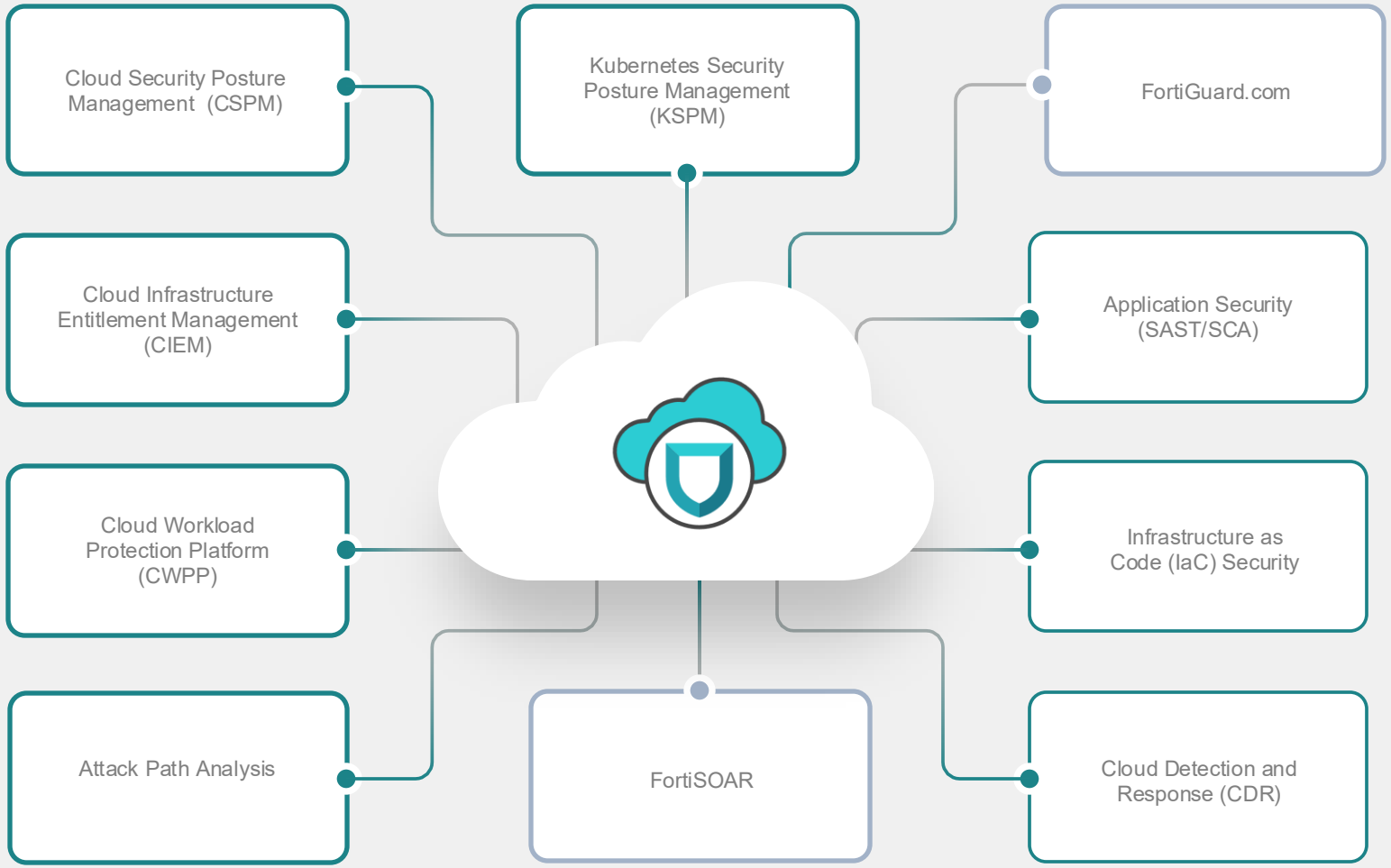
FortiCNAPP Wrap-Up

The Most Complete AI-driven Cloud-Native Application Protection Platform

Single vendor for all cloud security and secure CI/CD application development needs.

See AND protect everything from coding, deploying, and running applications across hybrid and multi-clouds.

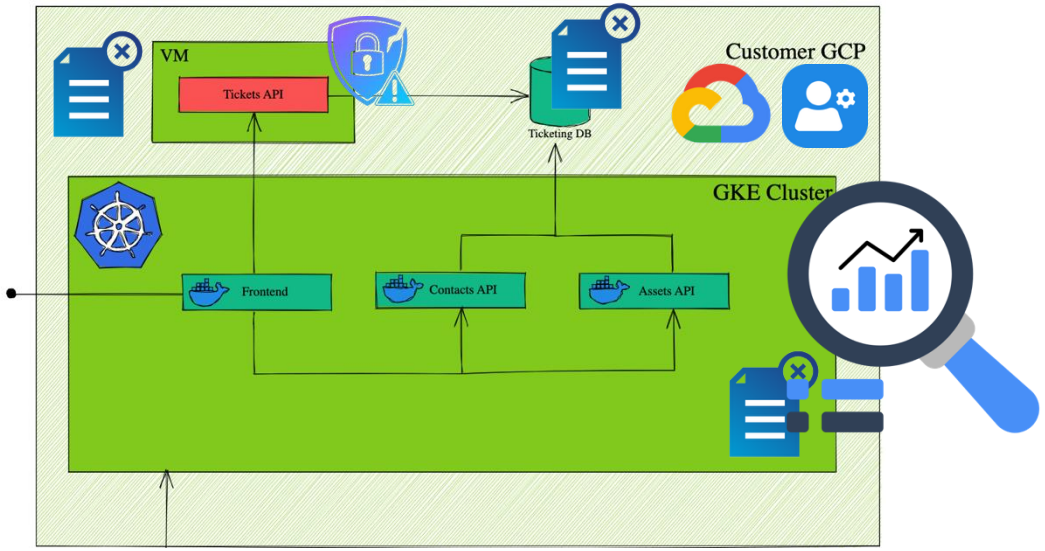
Simplify security with AI-driven platforms.

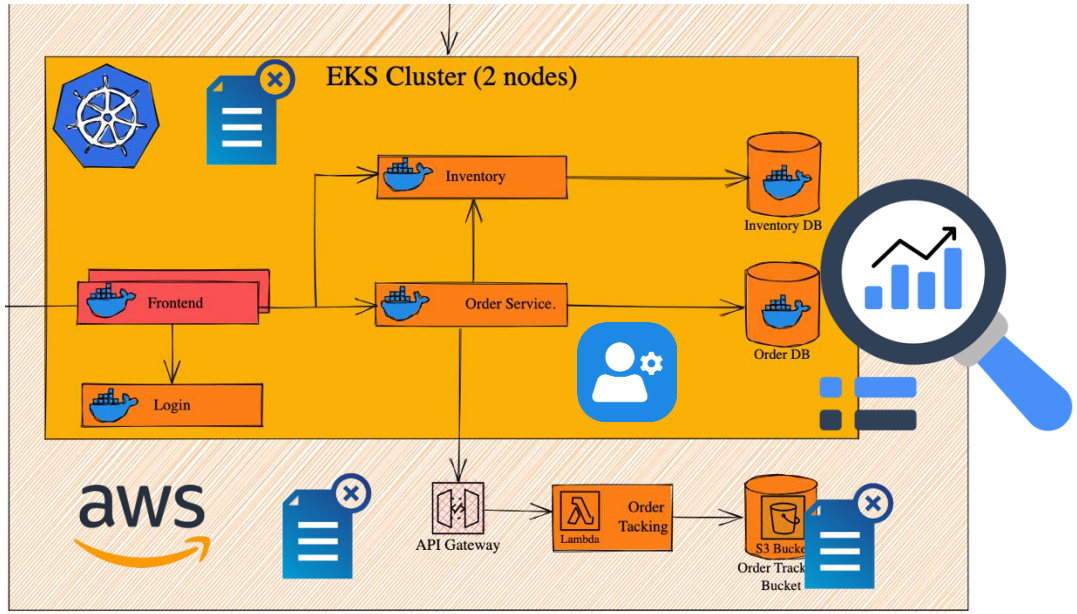


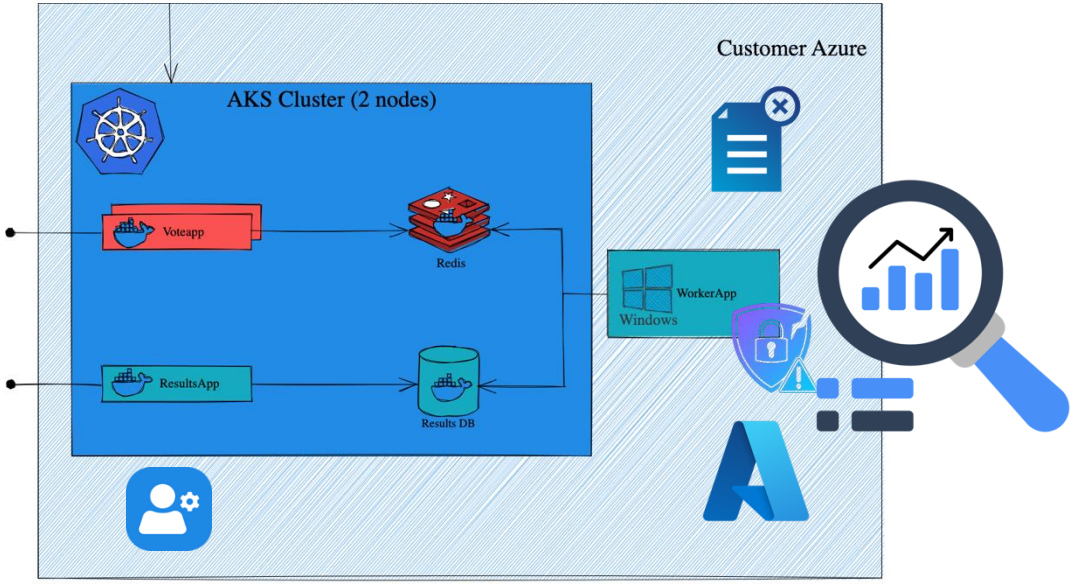
FortiCNAPP

Guided Capture the Flag

The Demo Environment







GUIDED CAPTURE THE FLAG – FortiCNAPP

The Rules

Ambiente Demo accessibile su https://lucca25.lwctf.com/

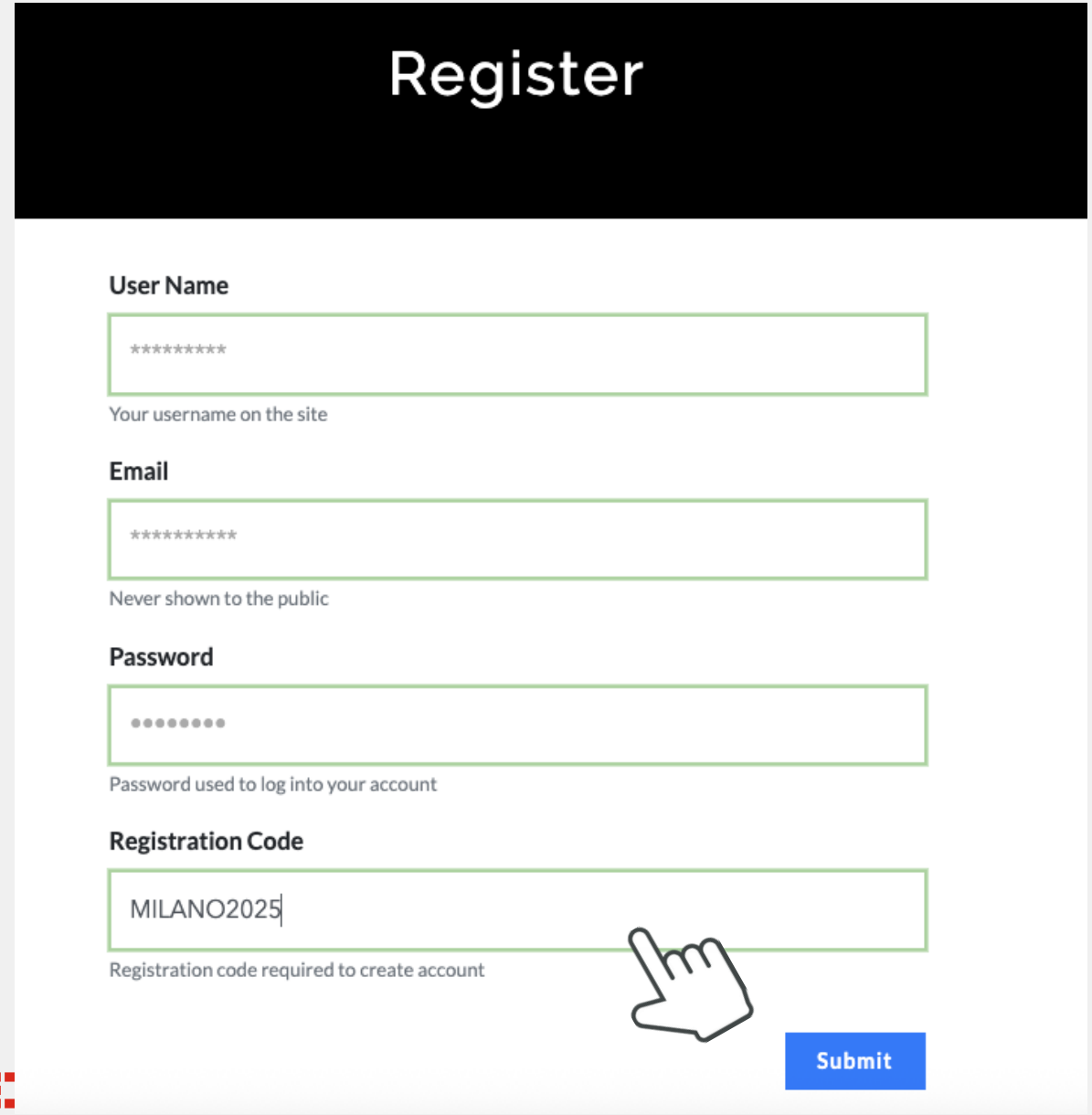
Registration Code: LUCCA2025

GUIDED CAPTURE THE FLAG – FortiCNAPP

Register to the CTF site

GUIDED CAPTURE THE FLAG – FortiCNAPP

Register to the CTF site



-> Your nickname, how you will be seen on the dashboard

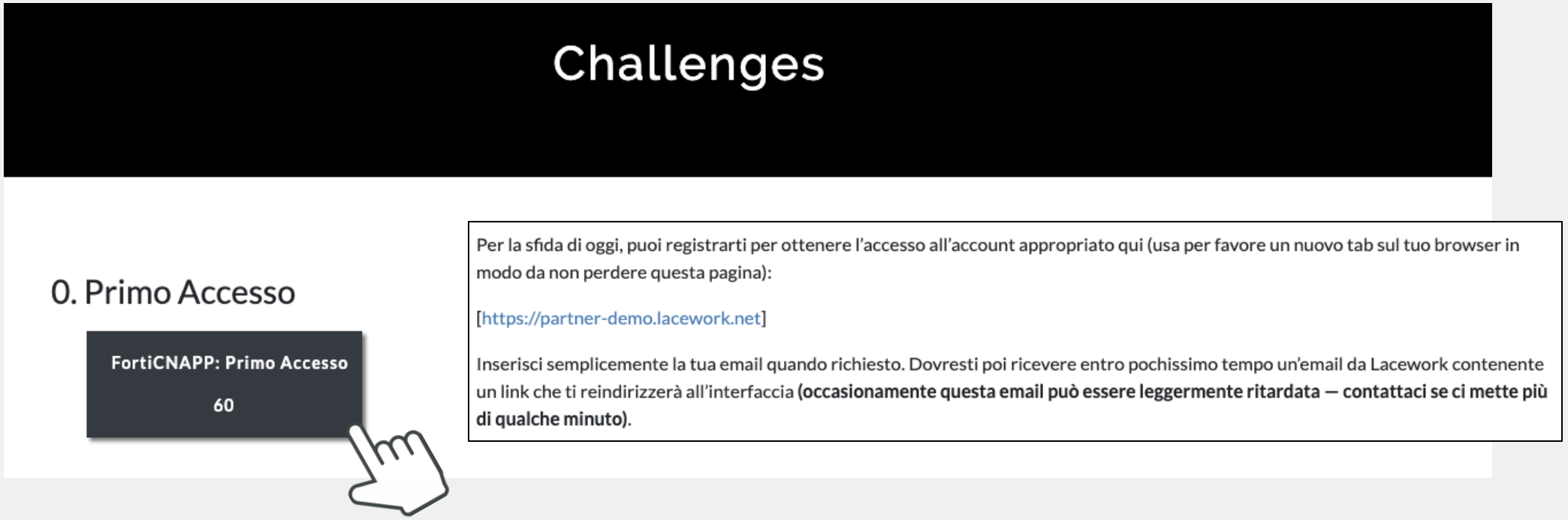
-> Your email

-> Just in case you loose your session

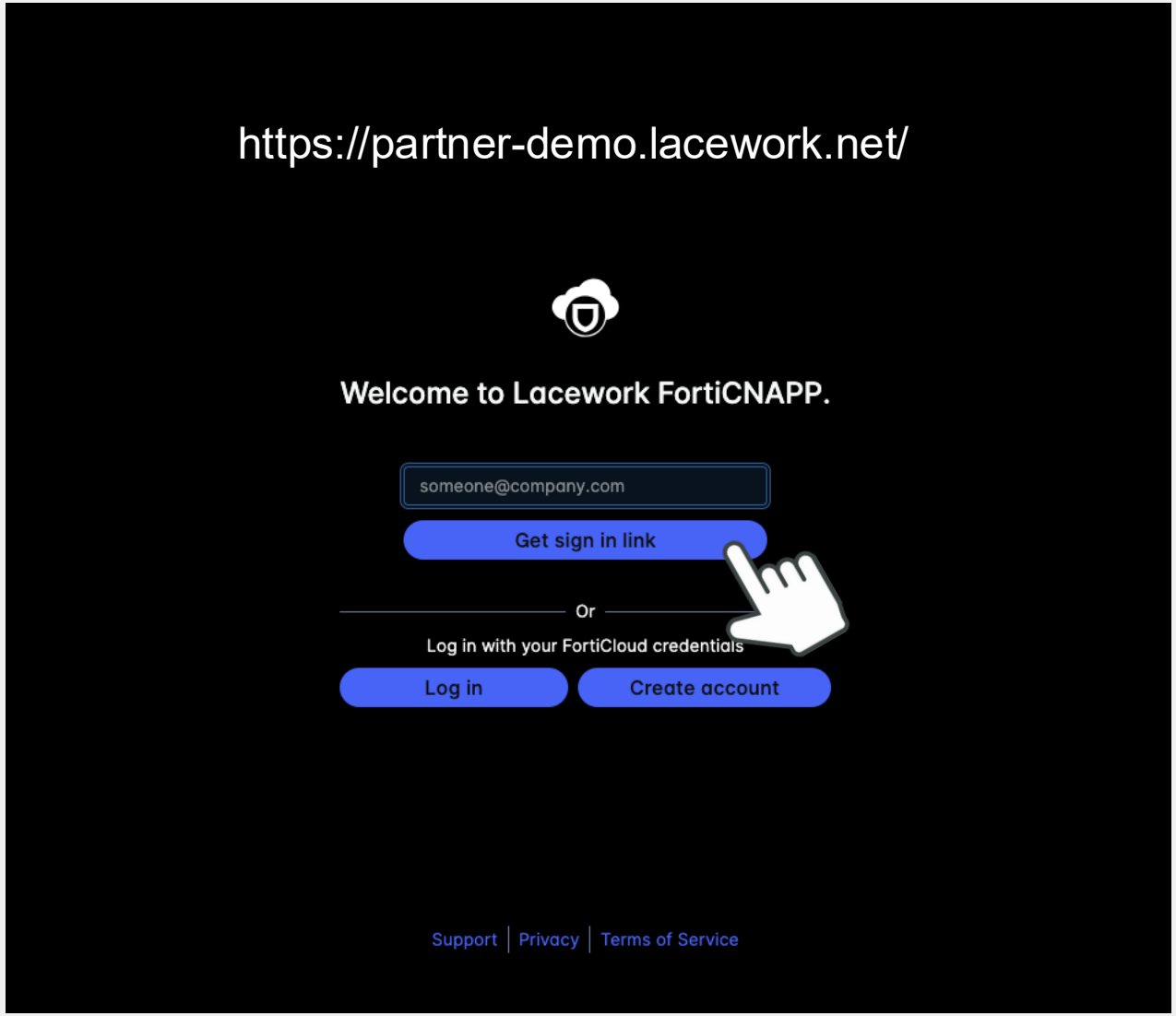
-> Insert «LUCCA2025»

GUIDED CAPTURE THE FLAG – FortiCNAPP

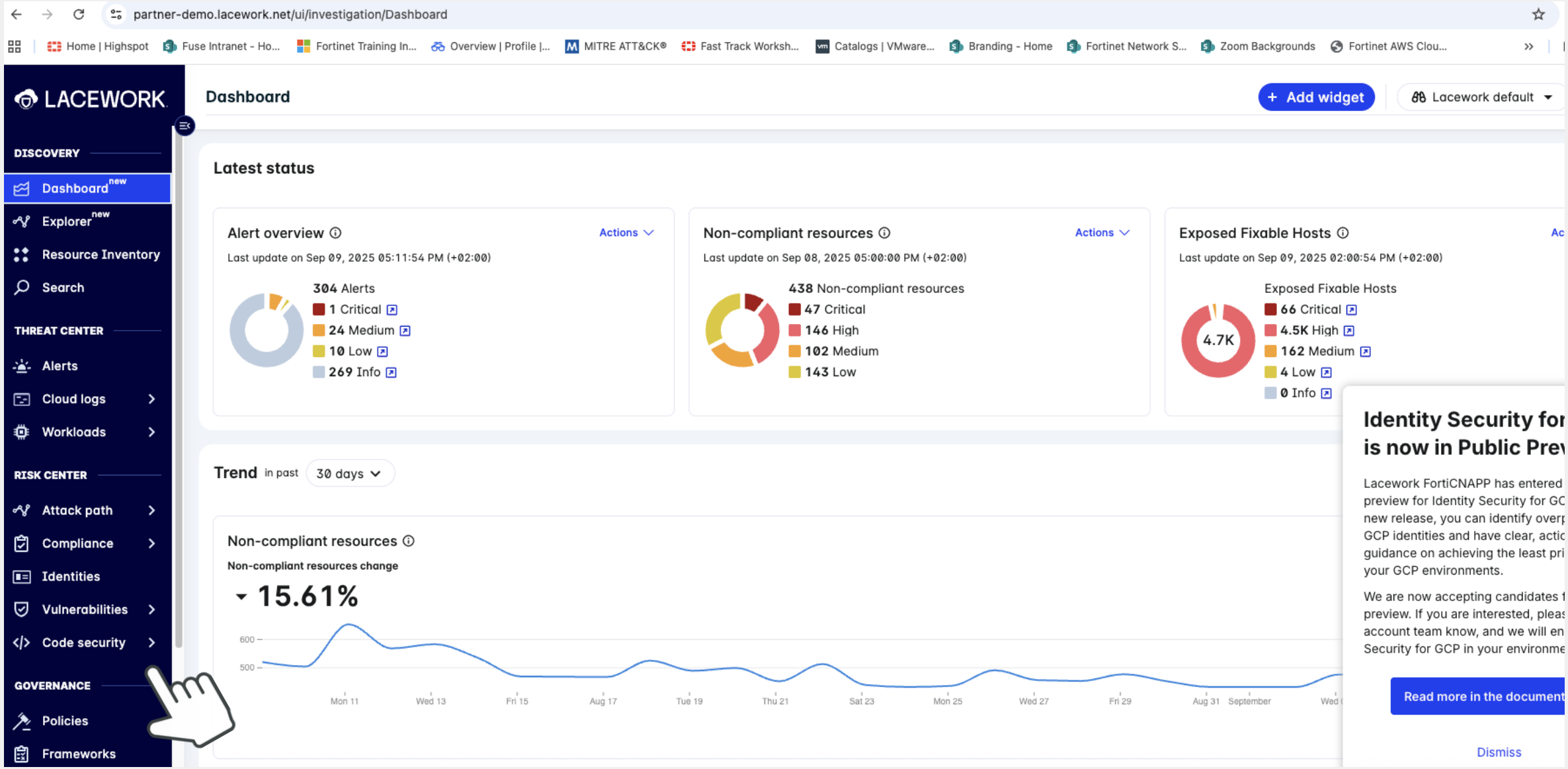
Start Capturing!



GUIDED CAPTURE THE FLAG – FortiCNAPP

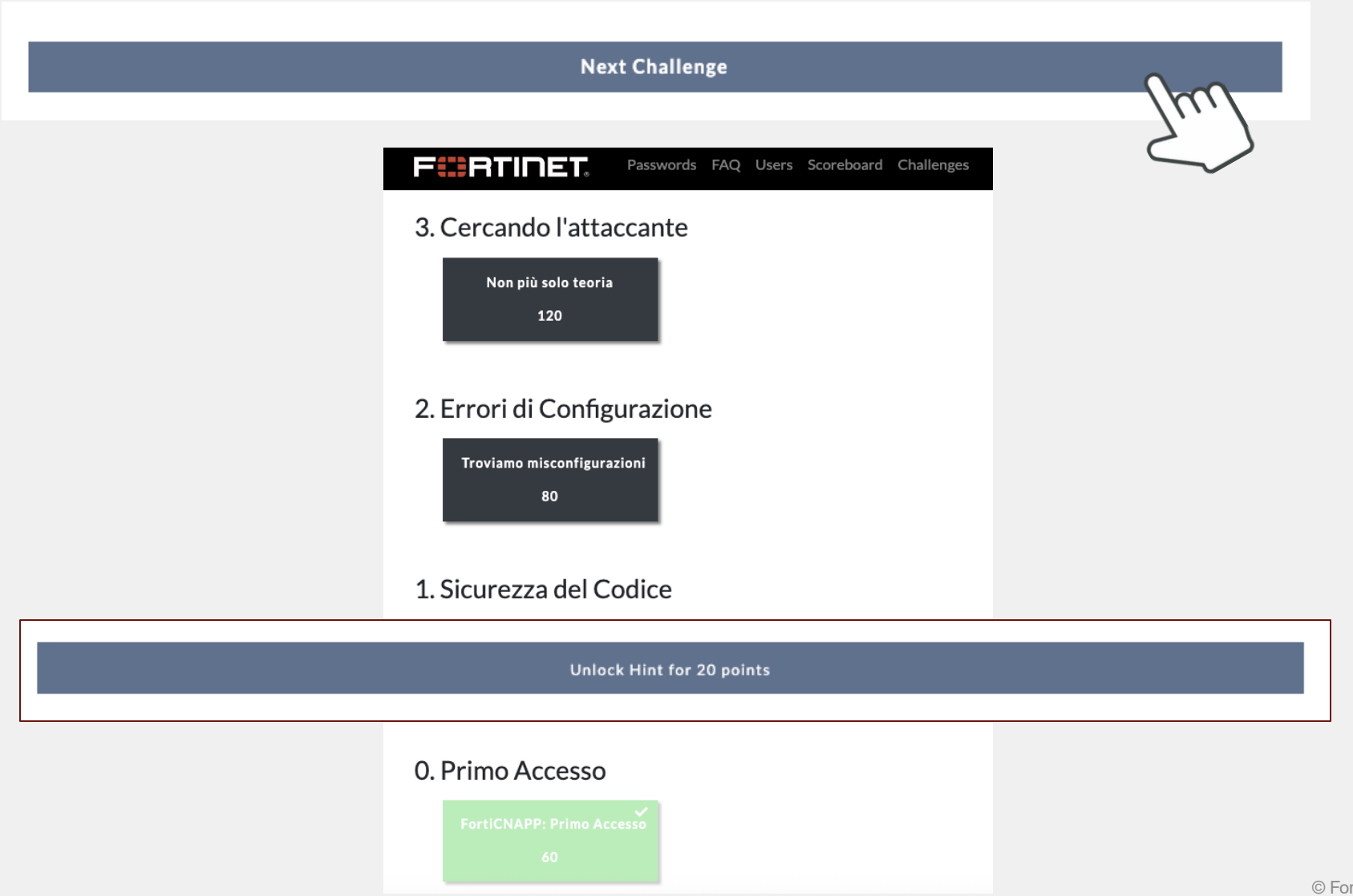


GUIDED CAPTURE THE FLAG – FortiCNAPP

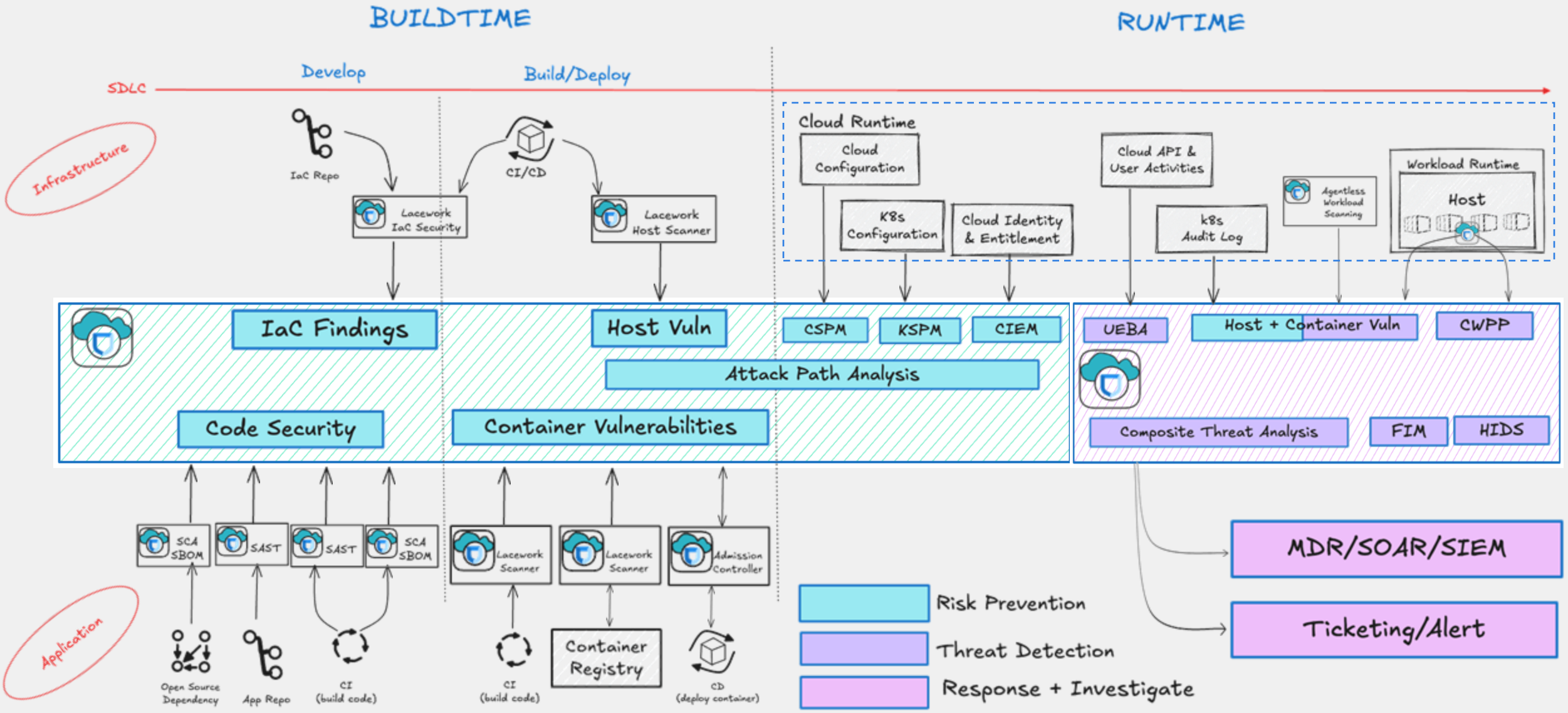


GUIDED CAPTURE THE FLAG – FortiCNAPP

Keep Capturing Flags!



FortiCNAPP in a nutshell



LINK PRESENTAZIONE

https://github.com/caliaf/XPERTS2025/forticnapp.pdf


FORTINET