
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

DEM224-S

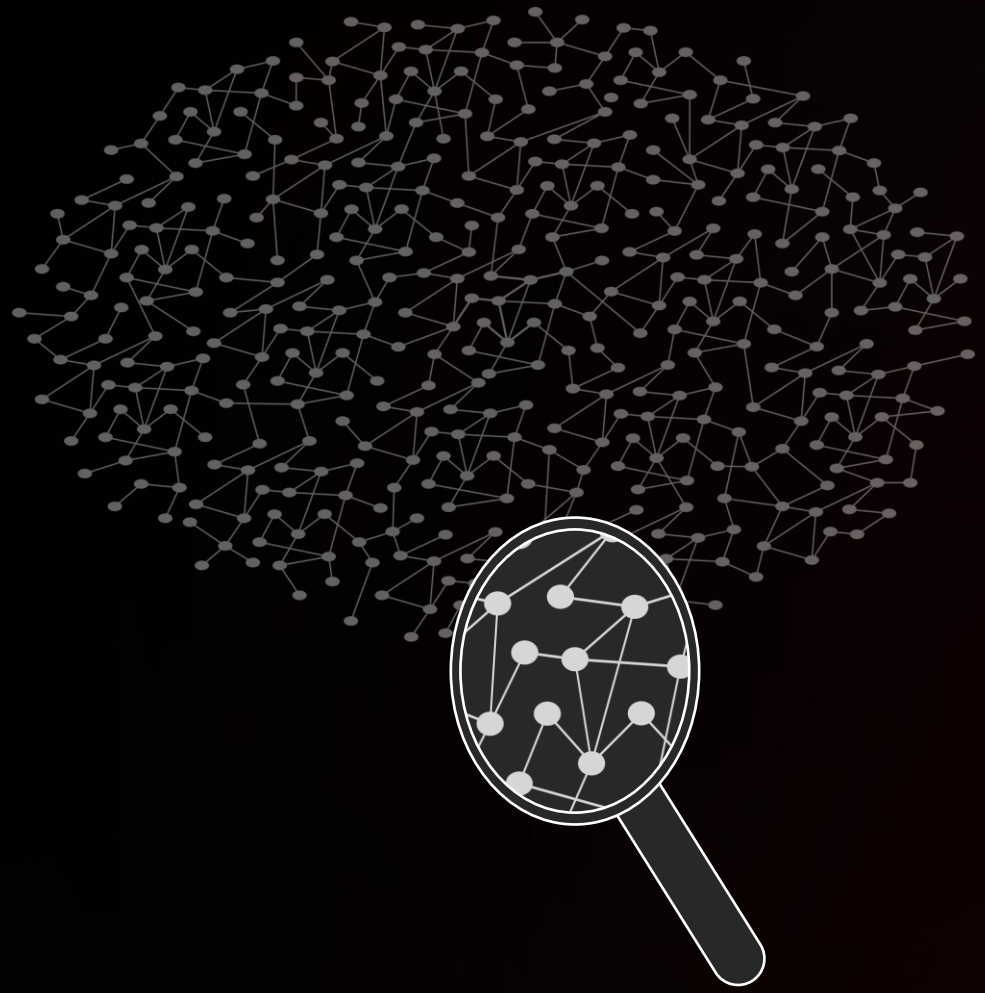
Amazon Neptune: Using graphs for security operations insights

Raaz Herzberg
VP of Product Strategy
Wiz

Brad Bebee
General Manager
Amazon Neptune

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Graphs are awesome!



1. Model data based on relationships

2. Applications explore connections and patterns in connected data

3. Processing graphs is hard due to random data access

4. Generalized graph operations require purpose-built processing

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common business applications that use graphs



Social networking



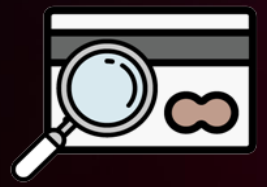
Recommendations



Knowledge graphs



Security Graph



Fraud detection



Life sciences



Network & IT operations

With connected datasets

- Where relationships between data matter just as much as the data itself
- When results are dependent on the basis of the *strength*, *weight,* or *quality* of relationships

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Neptune (Now Serverless and Global too!)

FULLY MANAGED, PURPOSE-BUILT GRAPH DATABASE IN THE CLOUD



Cost-effective



No hardware management



Instant provisioning



Security and compliance



Serverless



Global

- Optimized to **store and map billions of relationships**
- Enables **real-time navigation of connections with millisecond query** response time
- Supports **open standard query languages** openCypher, Gremlin, and SPARQL

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Every day thousands of customers use Neptune



Amazon Neptune

Customers across different verticals and use cases use Amazon Neptune in production today

WIZ · Finra · SIEMENS · AstraZeneca · JupiterOne · freshworks

amazon alexa · intuit · FACTSET · SAMSUNG · Blackfynn · Rappi

Uber ATG · HUUUGE · NBCUniversal · NETFLIX · asurion · COX AUTOMOTIVE

PaySense · zeta · Pearson · MARINUS ANALYTICS · noonum · THOMSON REUTERS

Case studies: https://aws.amazon.com/solutions/case-studies/?customer-references-cards.q=neptune

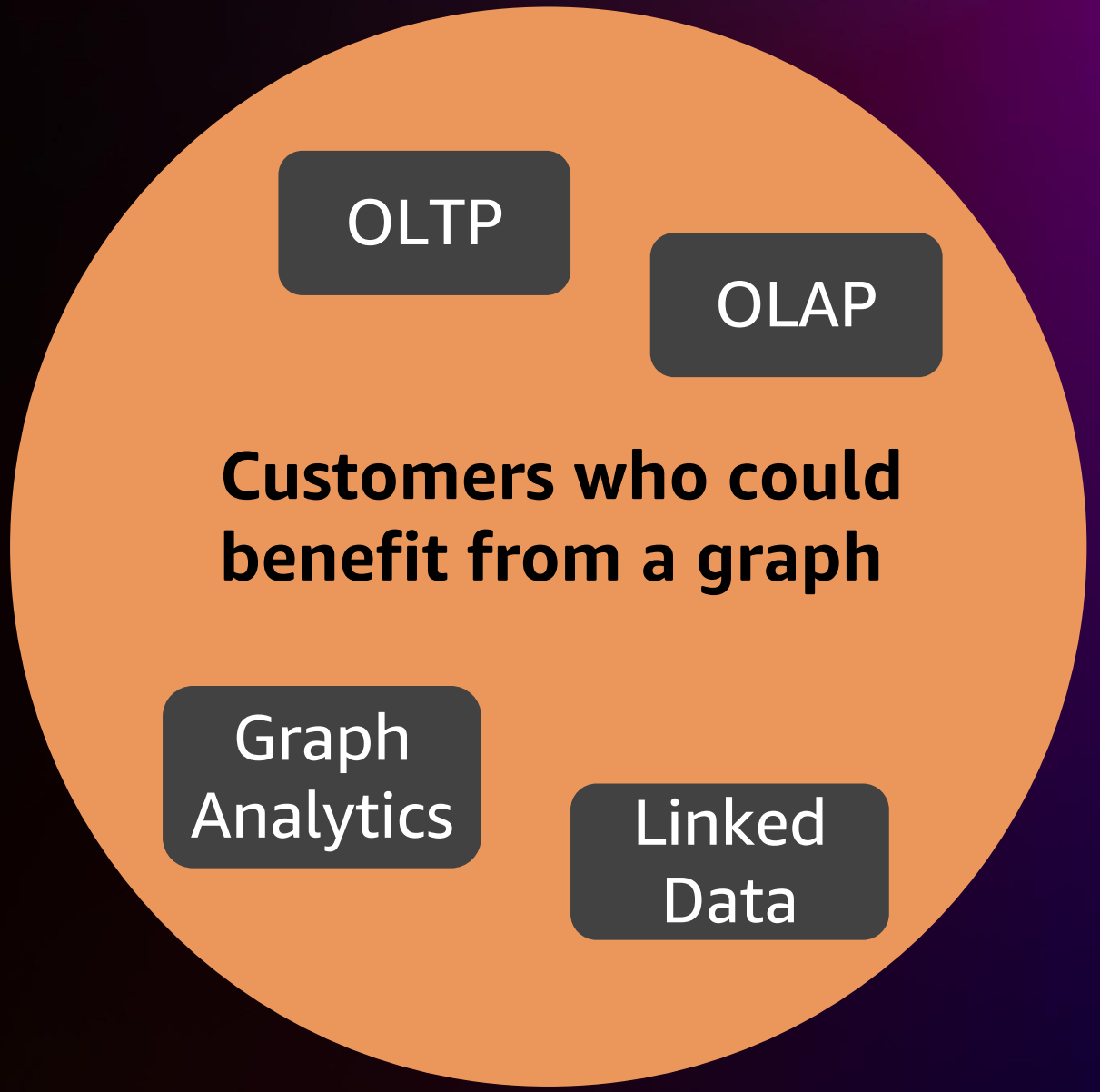
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

It’s still Day 1 for graphs



Customers who know they want a graph database



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wiz: Revolutionizing cloud security with an agentless, graph-based approach

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wiz: Redefining cloud security

One of the fastest-growing SaaS companies in history*

5M workloads

Scanned daily

Over 30%

of the Fortune 100

aws PARTNER

- Marketplace Seller
- Security Software Competency

*Forbes Article by Peter Cohan, https://www.forbes.com/sites/petercohan/2021/10/30/outpacing-palo-alto-networks-wizs-valuation-soars-11000-in-10-months/?sh=2e2a725463d2

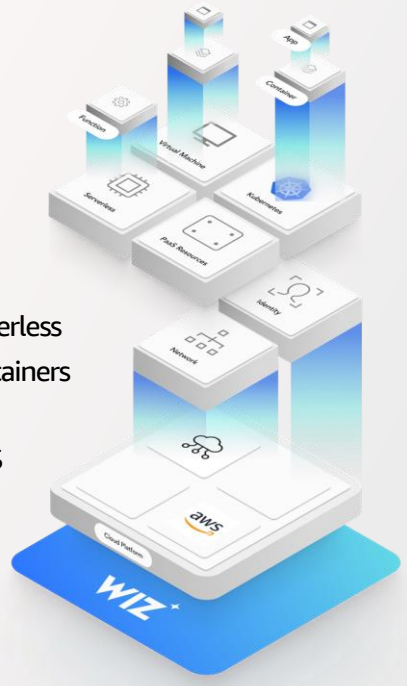
aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Industry leaders trust Wiz as their cloud security partner

MARS, COLGATE-PALMOLIVE, Takeda, salesforce, BMW, REI co-op, LVMH, priceline, FOX, Blackstone, PerkinElmer, AVERY DENNISON, ASOS, snowflake, yotpo., redis, PLAID, BRIDGEWATER, agoda, DocuSign, ManpowerGroup, THIRTY MADISON, Salesloft., UiPath™

A new approach to cloud security

1 Agentless scan of cloud metadata and workloads



2 Perform a deep cloud assessment

Traditional scanning

Vulnerabilities and missing patches

Misconfigurations

Malware

Cloud risk engine

External exposure

Excessive permissions

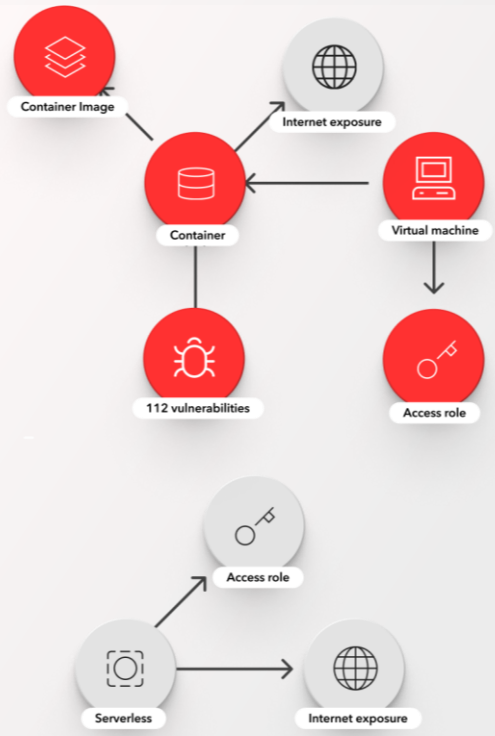
Exposed secrets

Lateral movement paths

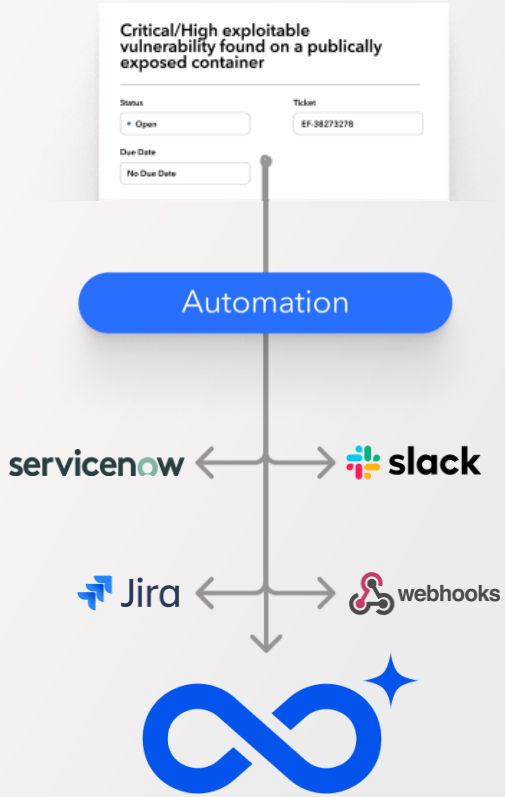
Wiz threat research

Novel cloud vulnerabilities and attacks

3 Identify the most critical risks



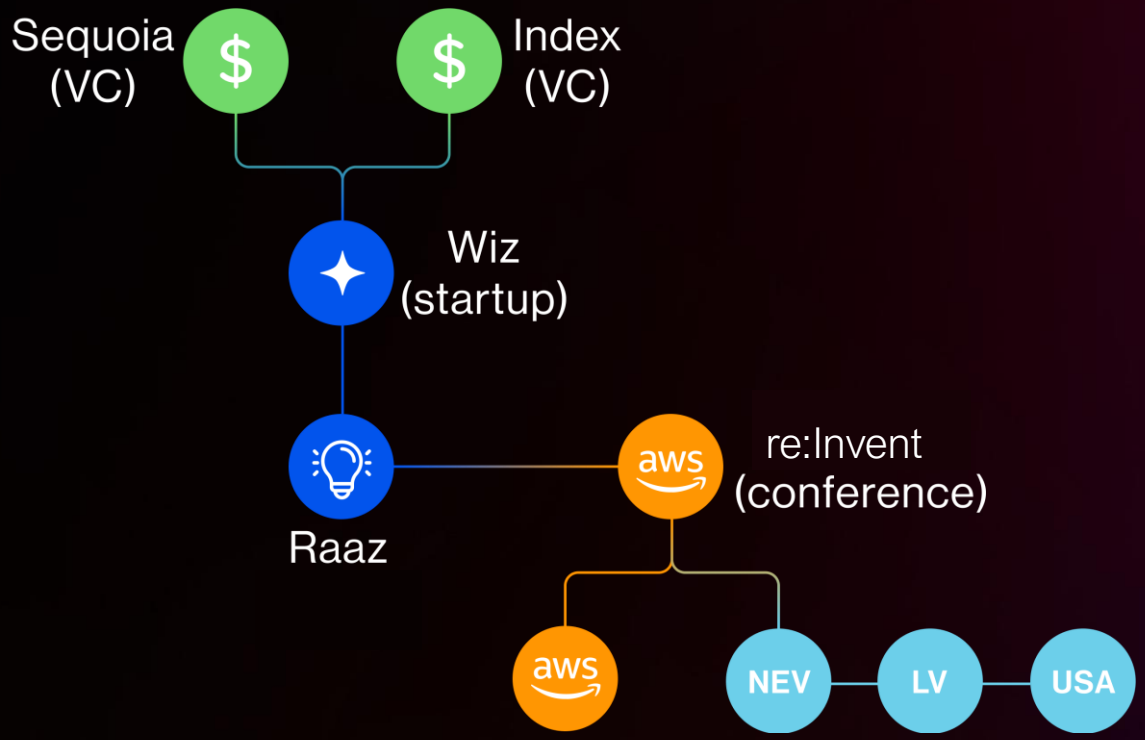
4 Proactively harden your cloud



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why graphs?
The world is a graph

Asking complex questions about the world requires a graph model



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is the most critical risk in my cloud?

Finding critical risks in the cloud is a complex graph question

Breakdown of an attack path:

> **Step #1:** finding an exposed VM

> **Step #2:** detecting a critical vulnerability

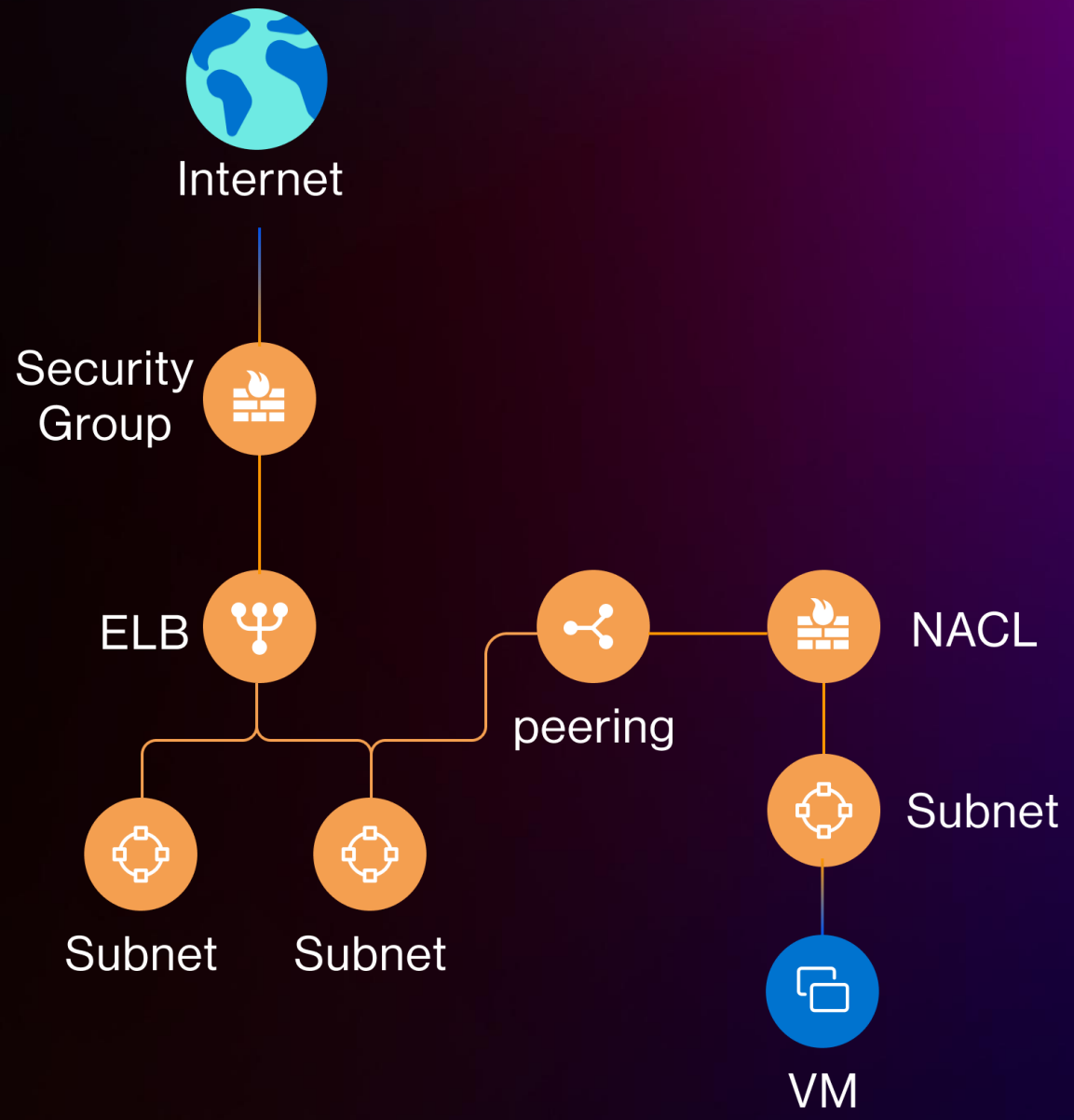
> **Step #3:** escalating to a sensitive database

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security graph use case: Network exposure

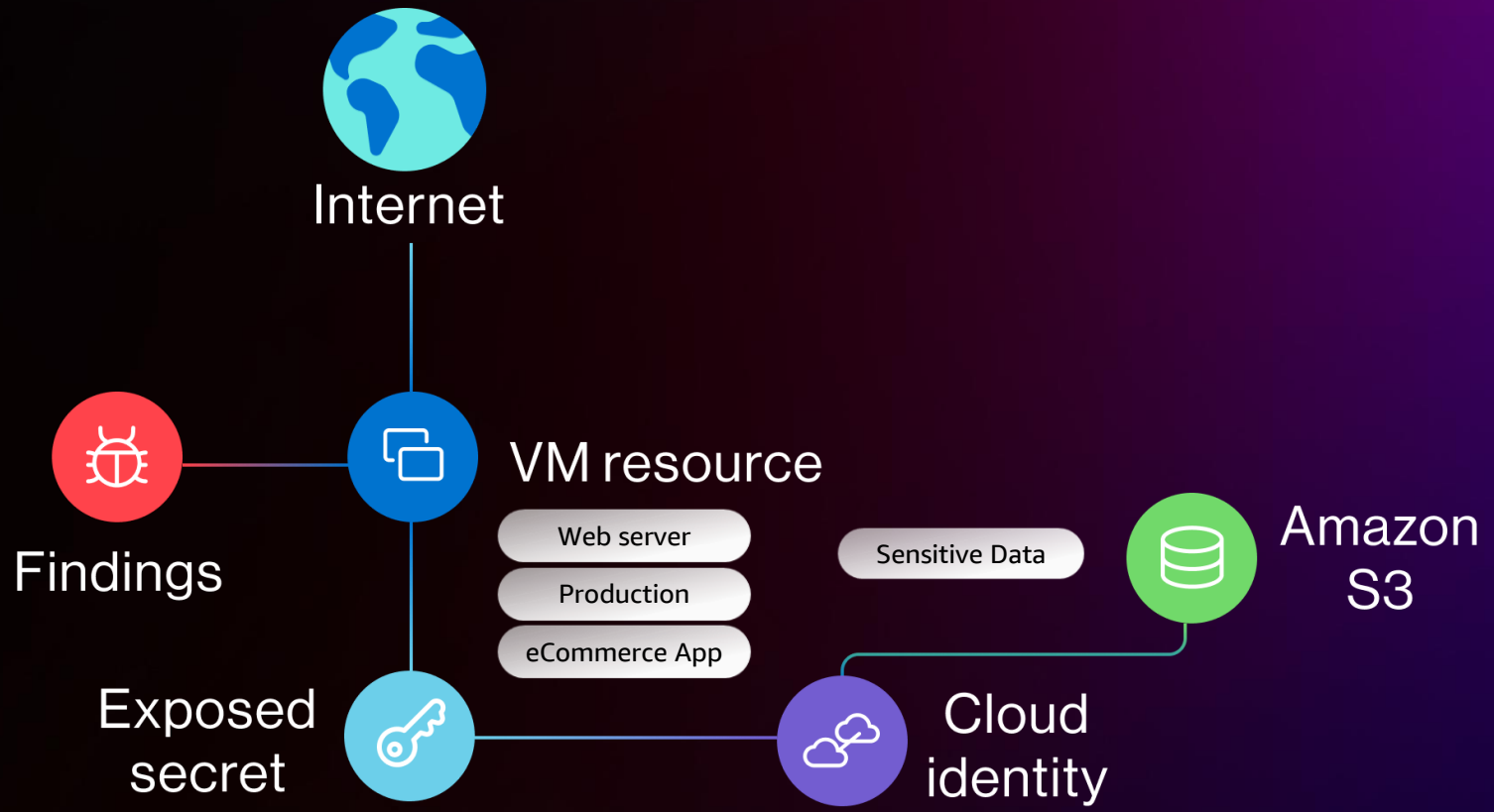
- Legacy tools failed to analyze exposure
- Graphs allow to detect effective exposure
  - Load balancers
  - Network peering
  - Cloud firewalls
  - Kubernetes networking components
  - And more!



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security graph use case: Prioritize vulnerabilities

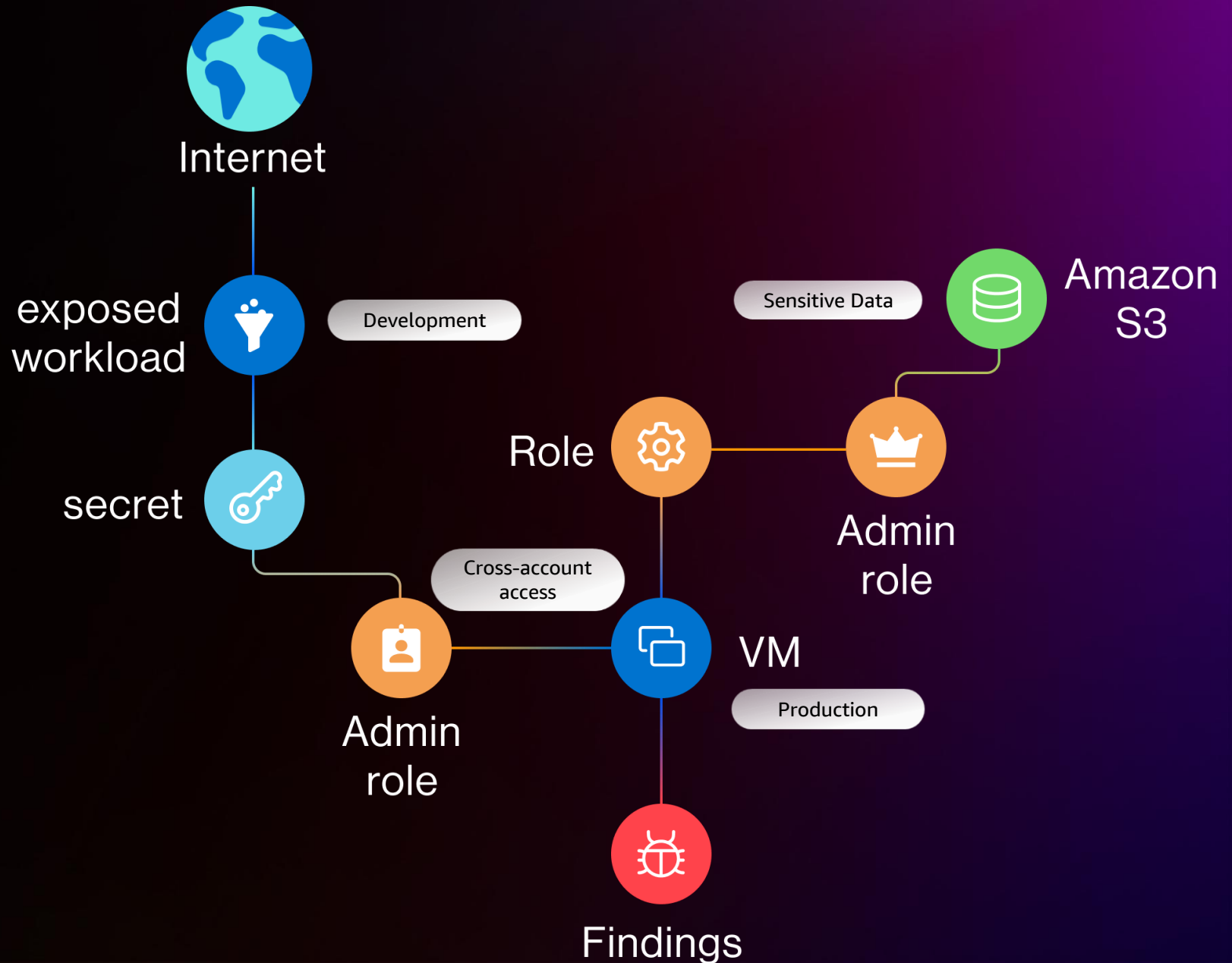
- It's more than CVE score
- Context across workloads, cloud, and business layers is crucial
- Security Graphs show you all the context



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security graph use case: Escalation path

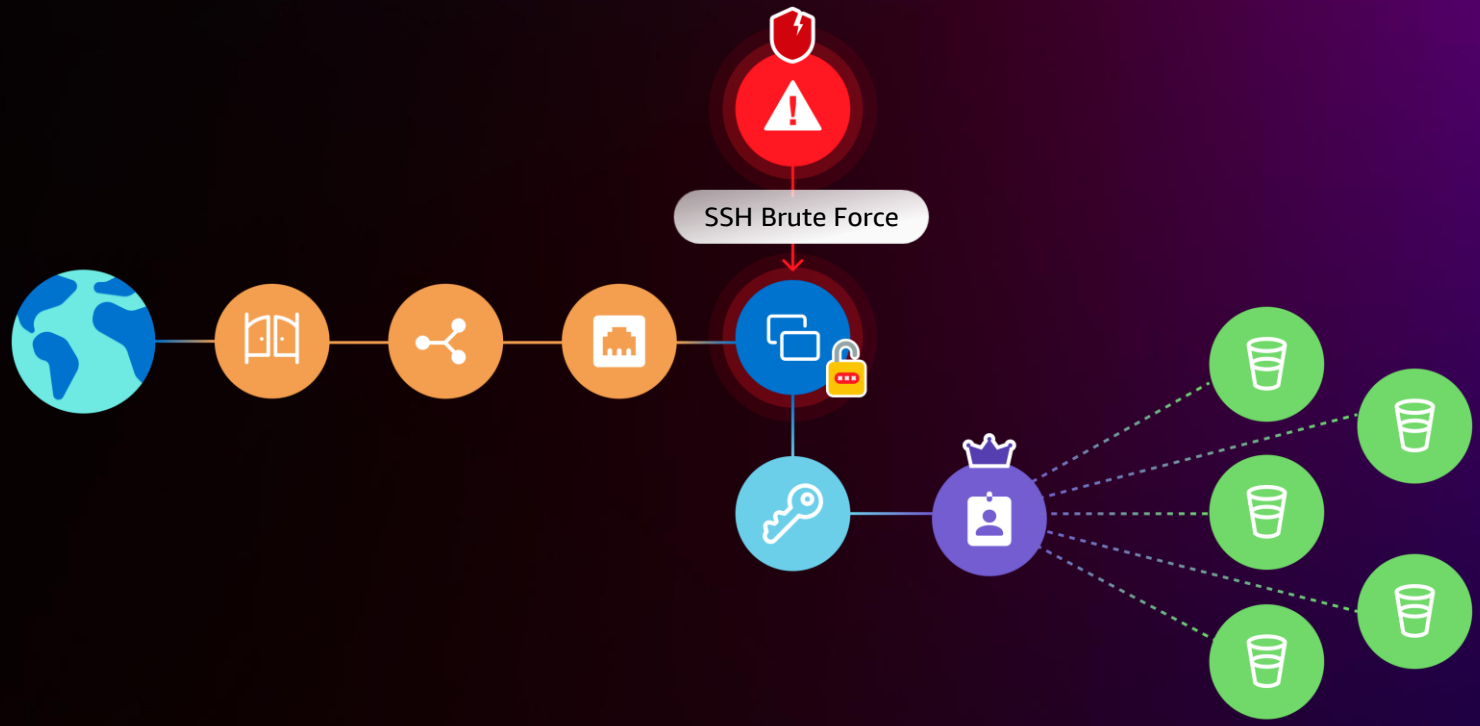
- Identify lateral movement and escalation paths using graph analysis
- Correlate exposed secrets, permissions and the resources they can access



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security graph use case: Amazon GuardDuty integration

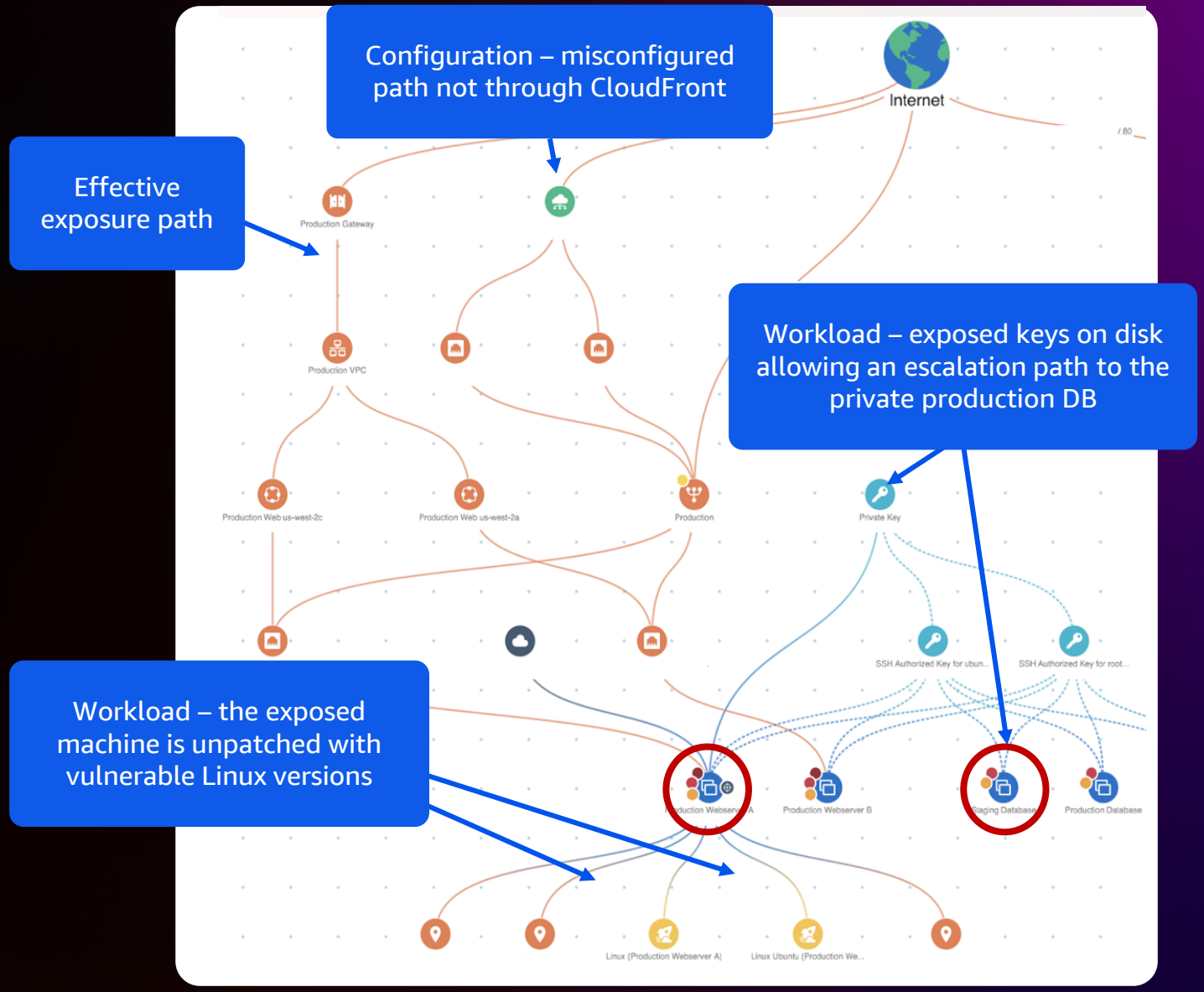
- Cloud alerts lack context
- Contextualize and prioritize threat-detection with the graph
- Example use case:
  - GuardDuty alert for SSH brute force
  - Correlated to a high-risk machine:
    - User with a weak password
    - Exposure to the internet
    - Lateral movement path



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bringing it all together

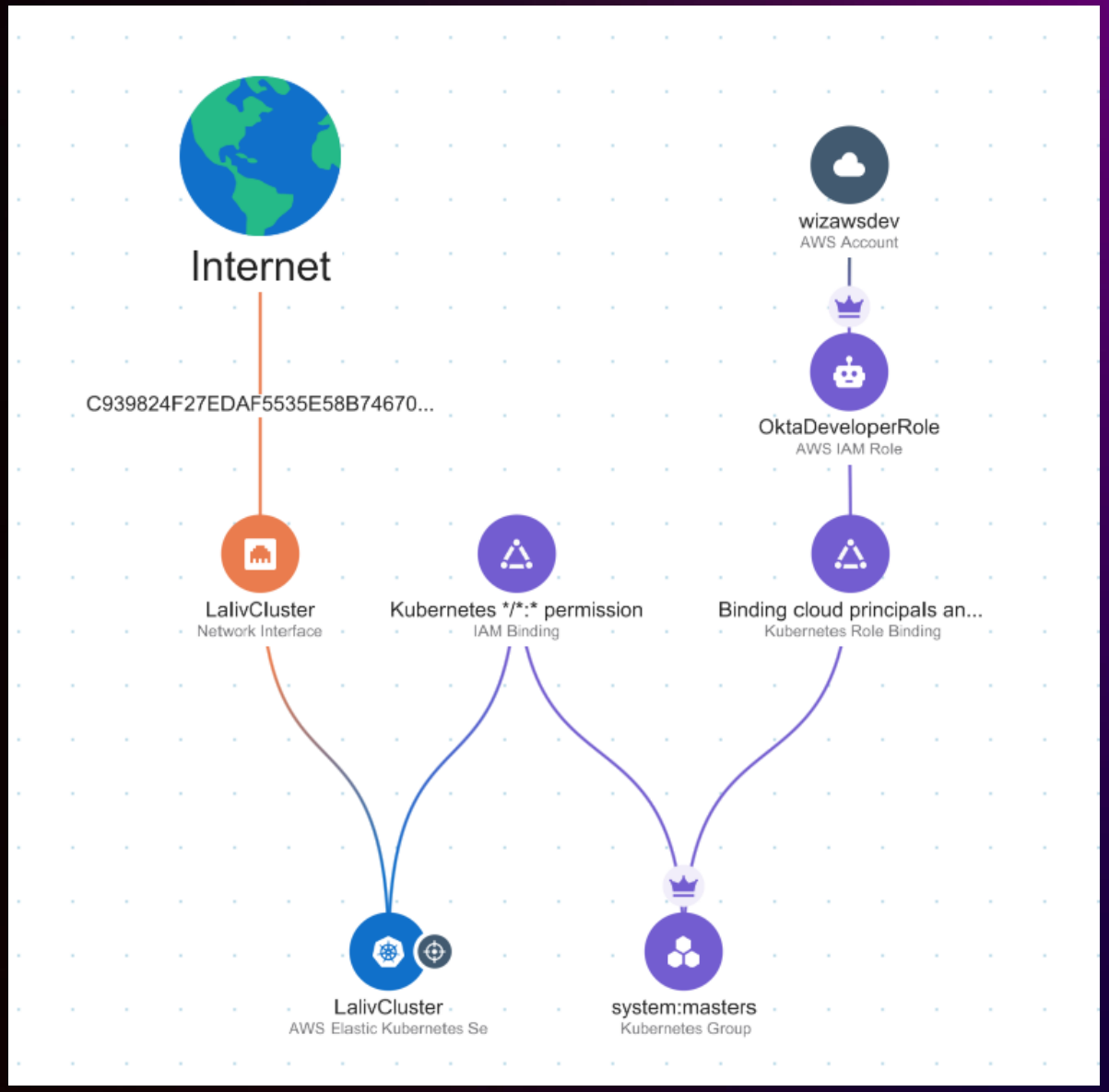
- Visualize and correlate the relationships between cloud objects with a Security Graph
- Uncover toxic combinations across layers to identify and prioritize critical risks

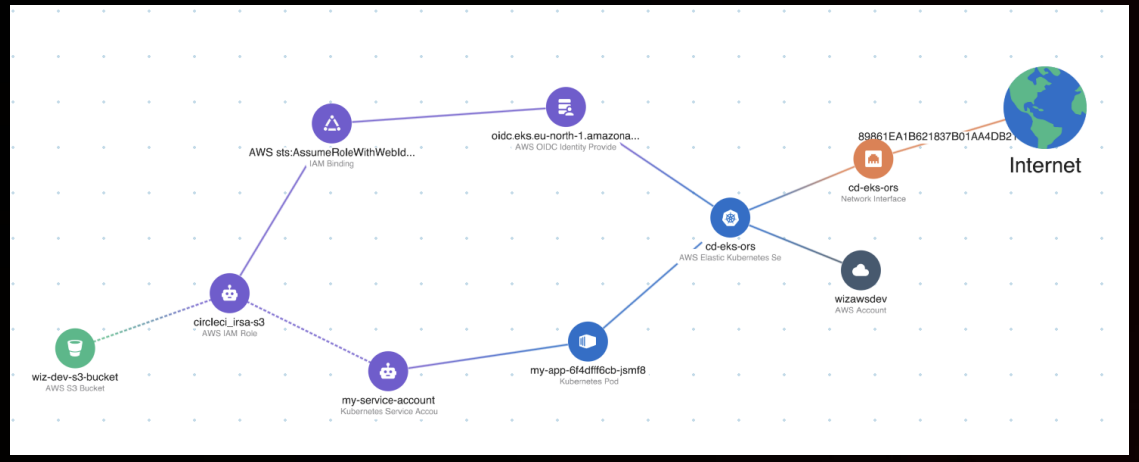


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bringing it all together

Visualize and correlate the relationships between complex cloud identities





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Graph in Wiz: Detecting critical risks in the cloud

Workload context

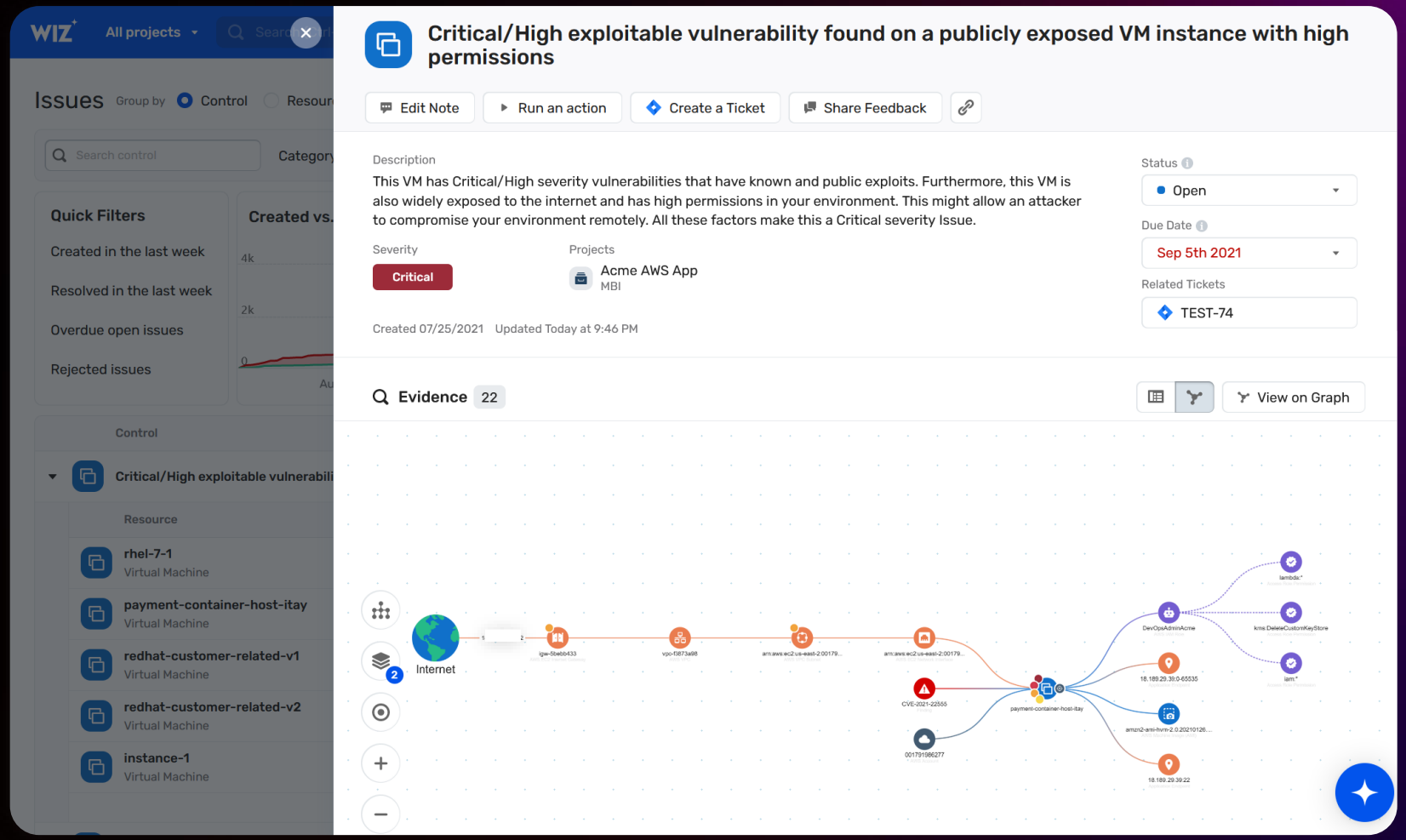
- Vulnerabilities
- Inventory
- Exposed secrets

Cloud context

- Resource configuration
- Networking
- Identities

Business context

- Tags
- Environment
- Business team



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Issue Type (Control)

Publicly exposed VM instance/serverless

Issue

dapl-jd-wiz-backend-mongo
Compute Instance

amz-linux-it-regional
EC2 Instance

gwen-GCP-transfer-vm
Compute Virtual Machine

inf-prod-access-vm
Compute Instance

View 4 issues...

Publicly exposed VM instance with cleart

Issue

amz-linux-it-regional
EC2 Instance

inf-prod-access-vm
Compute Instance

gwen-GCP-transfer-vm
Compute Virtual Machine

View 3 issues...

VM/serverless with cross-cloud lateral m

Publicly exposed VM instance with cleartext cloud keys allowing highly privileged cross-account access

Add Note | Run an action | Create a Ticket | Share Feedback

Description

The indicated VM instance group is publicly exposed and contains a cloud key saved in cleartext. If the resource is compromised, an attacker can gain access to the key and gain high permissions to an additional subscription.

Severity

Critical

Compliance Frameworks

Risks

Subscription

ACME-PROD-ENV
us-central1

Projects

2 Projects

Related Tickets

0 Tickets

Status

Open

Due

Nov 8th 2022

Created

Aug 26, 2022 at 1:23 PM

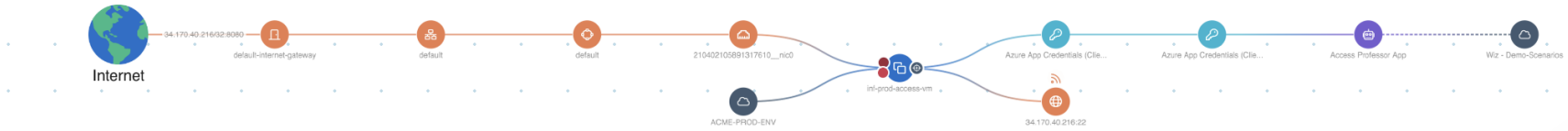
Updated

Nov 28, 2022 at 7:39 AM

Evidence

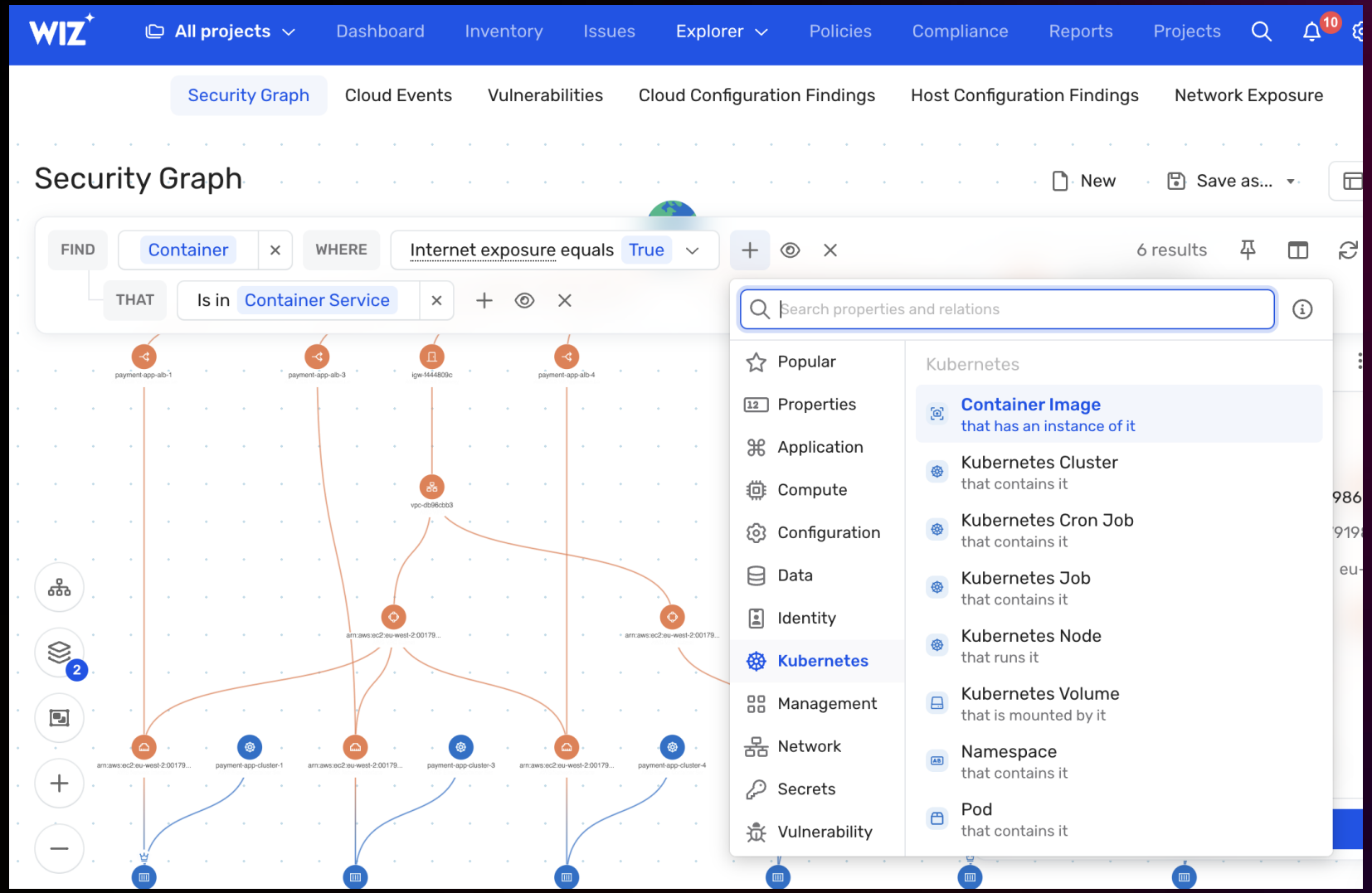
Overview

View on Graph



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security Graph in Wiz: understand your graph



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wiz & Amazon Neptune

- Great partnership with the Neptune team

- Working with us to support our scale & customers
  - Ingestion at scale – optimized keywords
  - Query optimizations – Data Flow Engine (DFE)
  - openCypher
  - Compliance – AWS GovCloud and FedRAMP (Medium and High)

- Graph technology is ready for mainstream!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enabling unique capabilities in Wiz with Amazon Neptune

- Flexibility to add additional security layers to the graph
  - Identity
  - Secrets
  - Data
  - Network

- RBAC on top of the graph
  - Graph view of your own graph

- Integrating Amazon RDS, Amazon Aurora, & Amazon Neptune
  - Combining the power of multiple types of databases

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Graphs are revolutionizing cloud security

> “One of the reasons I'm excited about [Wiz] is I believe that the same impact that the social graph had on a bunch of industries, likewise Security Graph is going to have a huge impact on the world.”

Igor Tsyganskiy
CTO, Bridgewater

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Raaz Herzberg
raaz@wiz.io
raaz-herzberg (linkedin)

Brad Bebee
beebs@amazon.com
B2ebs (twitter)



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.