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

PRT254

SPONSORED BY WIZ

Context is everything: Join the CNAPP revolution to secure your AWS deployments

Yinon Costica

Co-Founder and VP of Product
Wiz

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

Agenda

What is holding back your cloud journey?

A new approach to reducing risk

Fireside chat with John Visneski, CISO of MGM Studios

Open Q&A

© 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™

What is holding back your cloud security journey?



Complex environment

Multiple clouds

Multiple architectures

Thousands of technologies



Complex risk

Vulnerabilities & misconfigurations

Risk likelihood

Risk impact



Complex to operationalize

Lack of visibility

Fragmented suite of tools

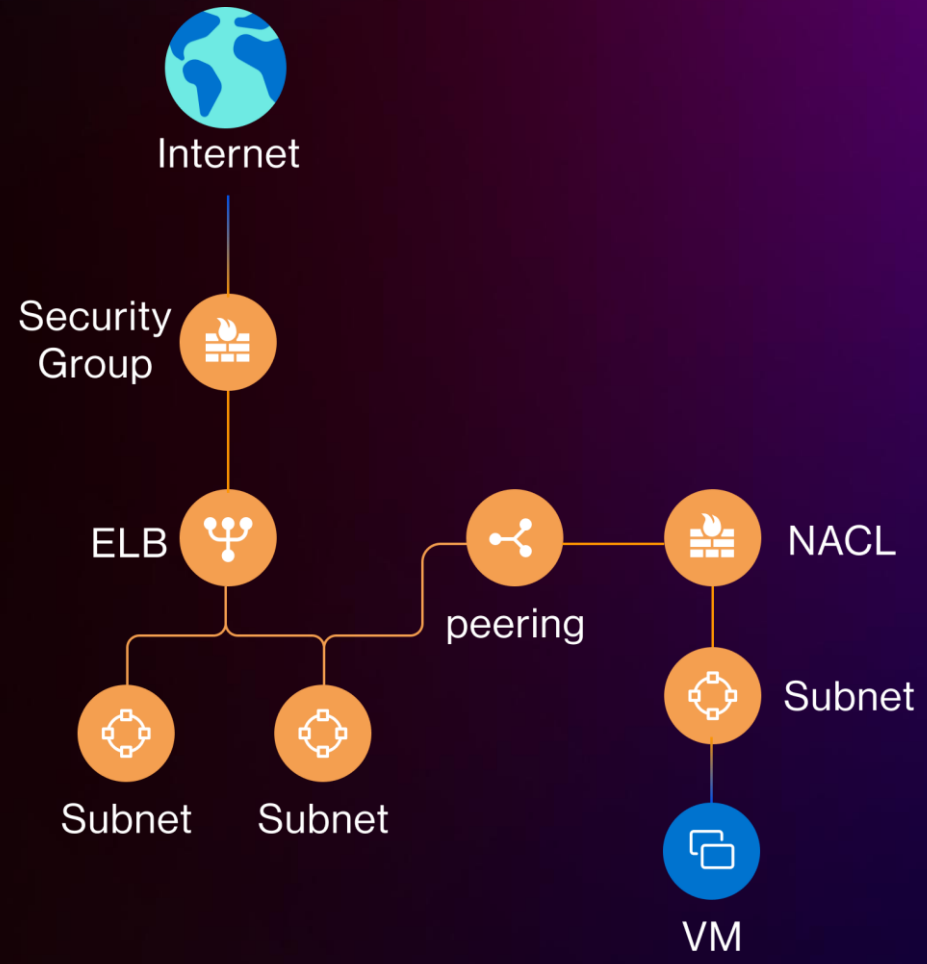
Remediation process across teams

aws

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

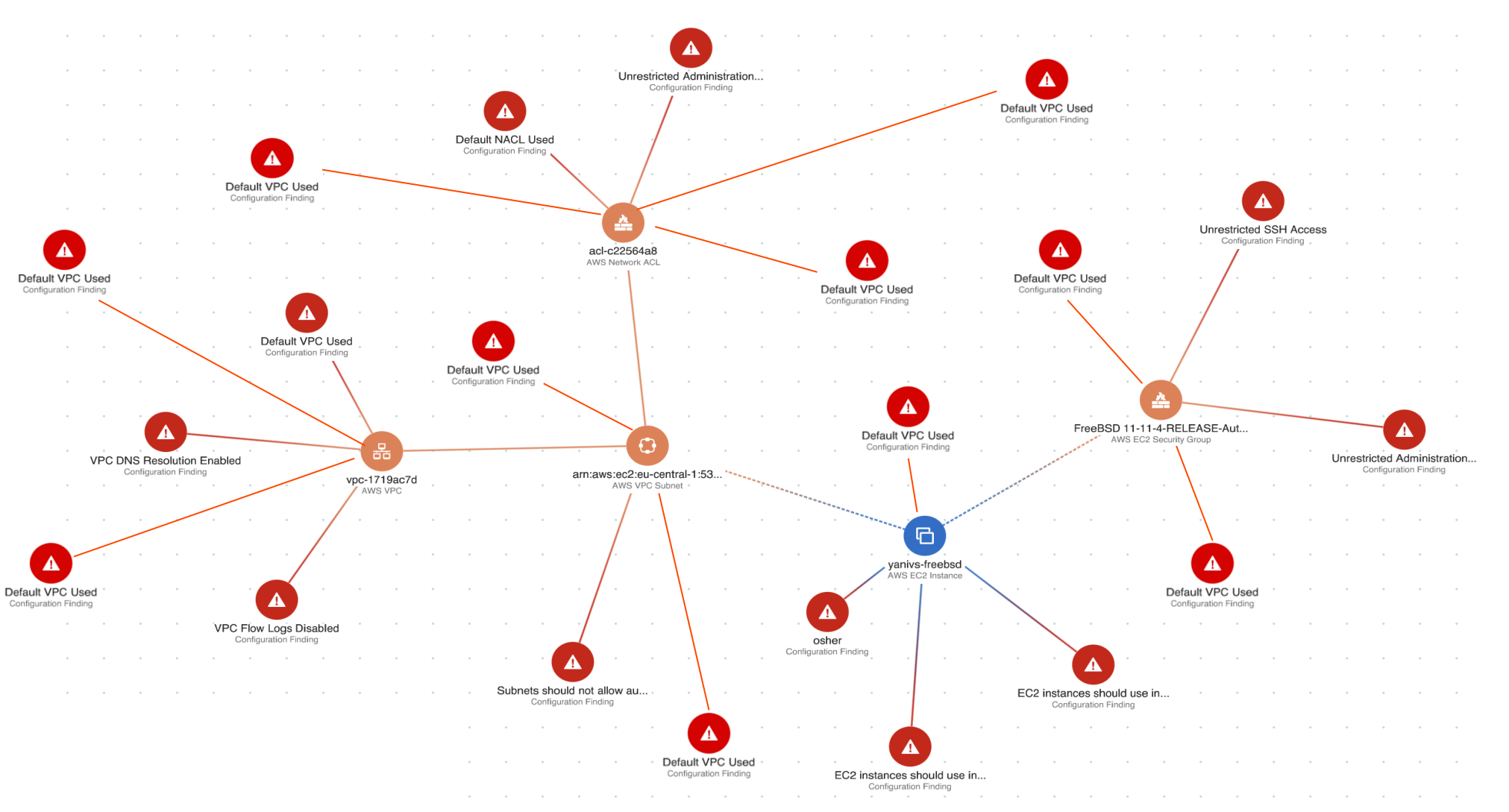
Traditional security does not always detect the real issues

- Traditional tools like CSPMs and vulnerability scanners don’t always detect the real issues
- Scan independently and lack context, unable to prioritize
- Generate noise and may increase your key security metrics



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

Misconfigurations != risks

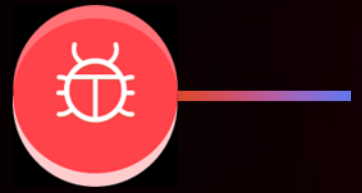


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: Which security issues do you prioritize?

- Traditional security tooling drive alert fatigue

- Your team lacks the context to focus on the right issue
  - Workload
  - Cloud
  - Business context



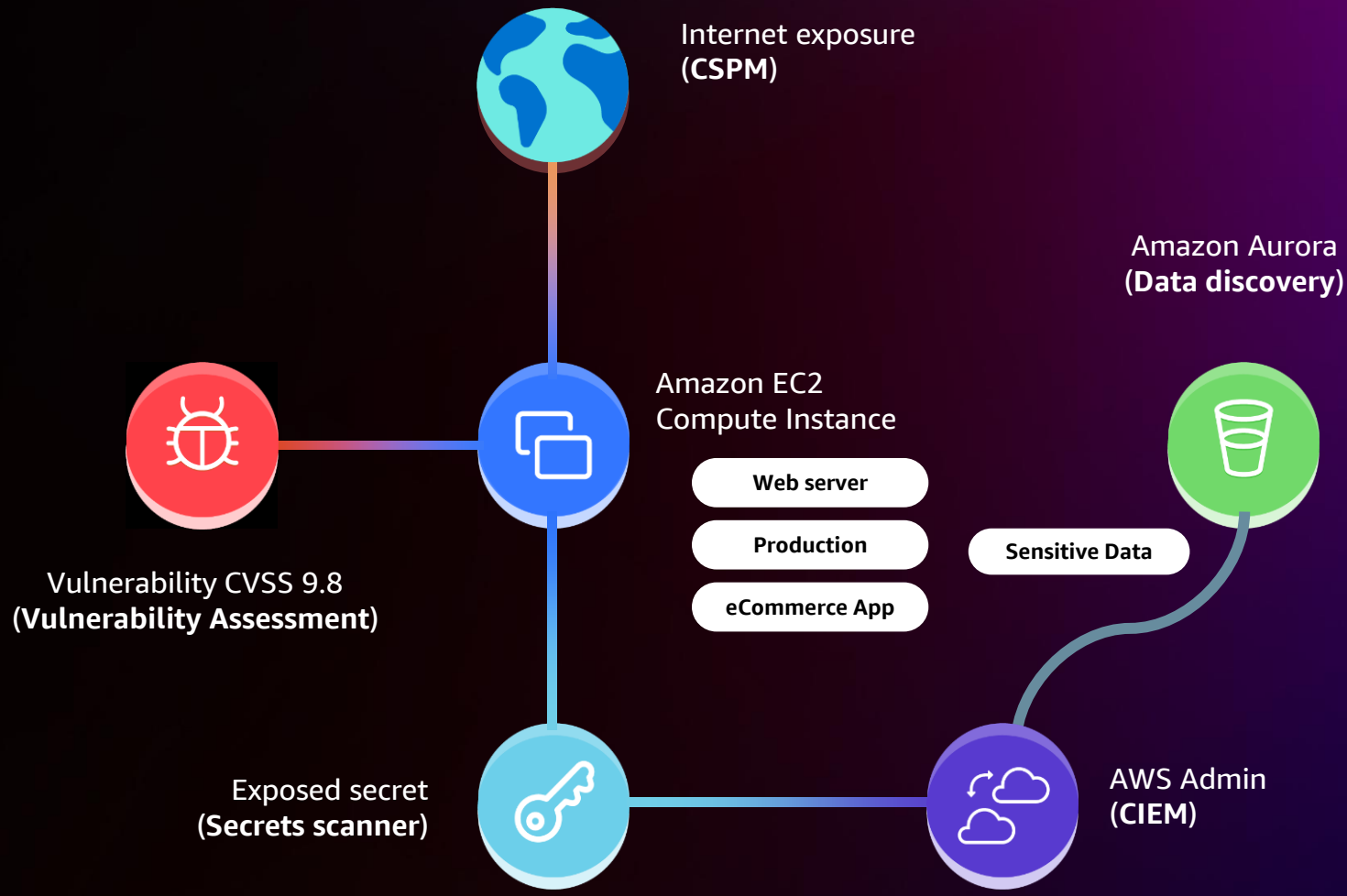
Vulnerability CVSS 9.8
(**Vulnerability Assessment**)

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

Example: Which security issues do you prioritize?

- Traditional security tooling drive alert fatigue

- Your team lacks the context to focus on the right issue
  - Workload
  - Cloud
  - Business context



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

Cloud Native Application Protection Platform (CNAPP)

CSPM	Compliance reporting	Host Configuration
Serverless Security	CWPP	Cloud CMDB
Network Architecture	IaC Scanning	Container Security
Secrets scanning	CIEM	Vulnerability Management

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

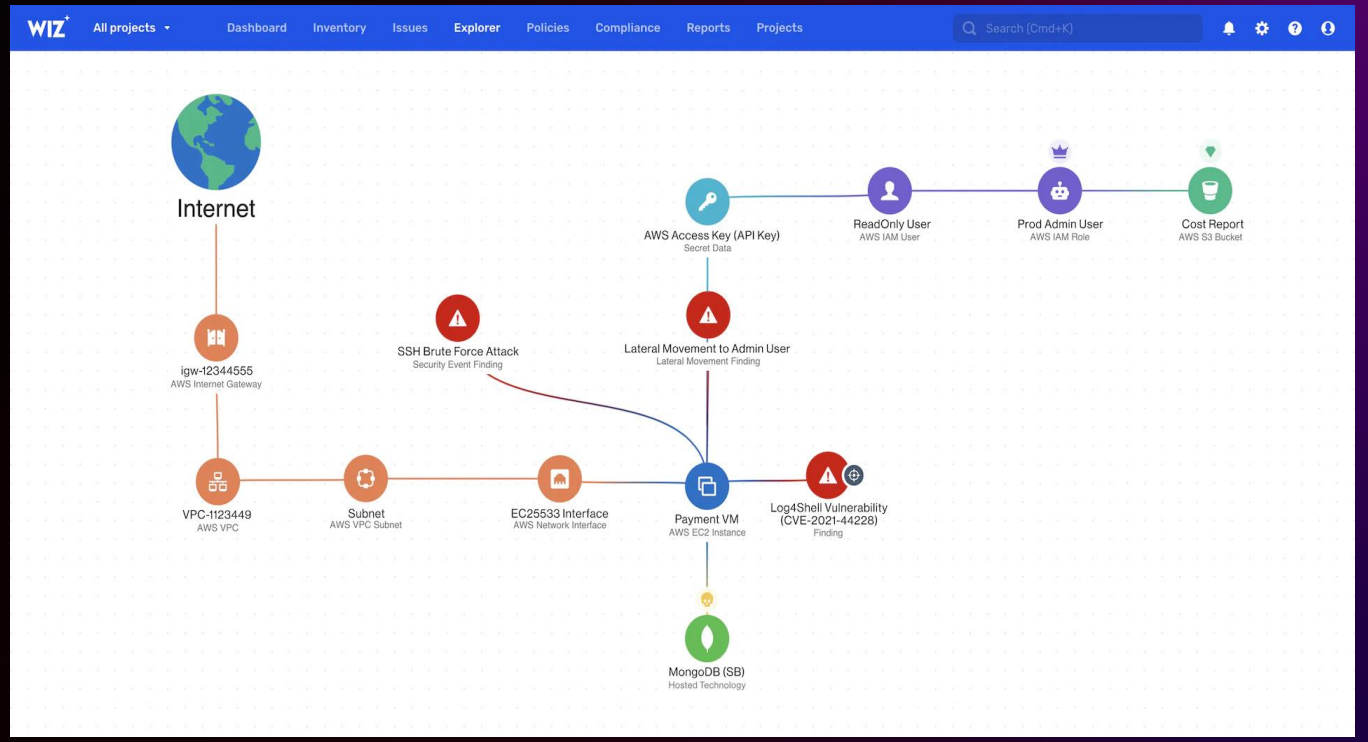
Wiz is a new approach to securing your cloud

Agentless, graph-based security solution to give you a comprehensive understanding of your AWS resources and risk

Frictionless visibility

Prioritization and context

Democratized for agility



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

Securing your AWS environment in 4 steps

1 Agentless scan of cloud metadata and workloads



Serverless
Containers
VMs
PaaS

2 Perform a deep cloud assessment

Traditional scanning

Vulnerabilities and patches
Misconfigurations
Malware
Sensitive data

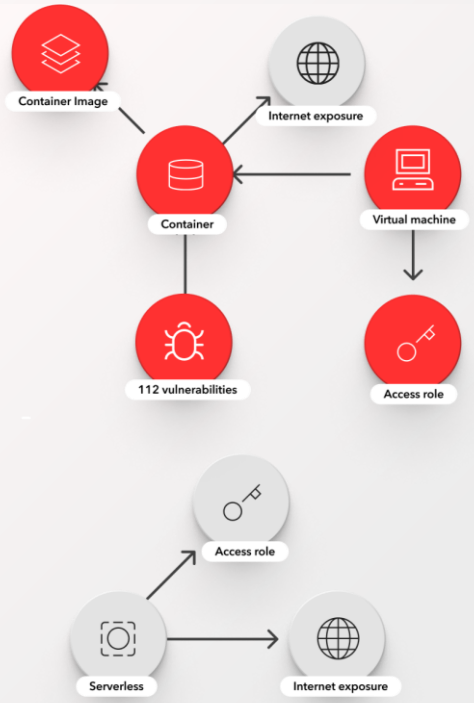
Cloud risk engine

External exposure
Excessive permissions
Exposed secrets
Lateral movement paths

Integrated tools

AWS CloudTrail
Amazon GuardDuty
Amazon Macie
3rd party tools

3 Identify the most critical risks



4 Proactively harden your cloud

Partner integrations

20+ integrations

Cloud remediation

One-click remediation
Automated security response
Remediation guidance

CI/CD Guardrails

One policy across the stack
Container and VM image scan
IaC scanning

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

Step 1: Full visibility in minutes across 60+ AWS services without agents

1 **Agentless scan of cloud metadata and workloads**

Frictionless visibility

- Agentless scanning via API
- Cloud and architecture agnostic
- Quick deployment, low maintenance



Compute

Amazon EC2 · Amazon EKS · AWS Fargate · AWS Lamba function · Amazon ECS

AWS Transit Gateway · Amazon VPC · Amazon Route 53 · Elastic Load Balancer · Amazon ECR

Security and Identity

Amazon Cognito · IAM · AWS KMS · AWS Secrets Manager

Amazon GuardDuty · AWS CloudTrail · AWS Systems Manager

Application and Data

Amazon ElastiCache · Amazon S3 · Amazon Neptune · Amazon Redshift

Amazon DynamoDB · Amazon RDS · Amazon SNS · Amazon SQS

Amazon SageMaker · AWS Glue · MQ · Amazon CloudFront

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

Step 2: See the whole risk picture with the Wiz Security Graph

2 **Perform a deep cloud assessment**

Traditional scanning

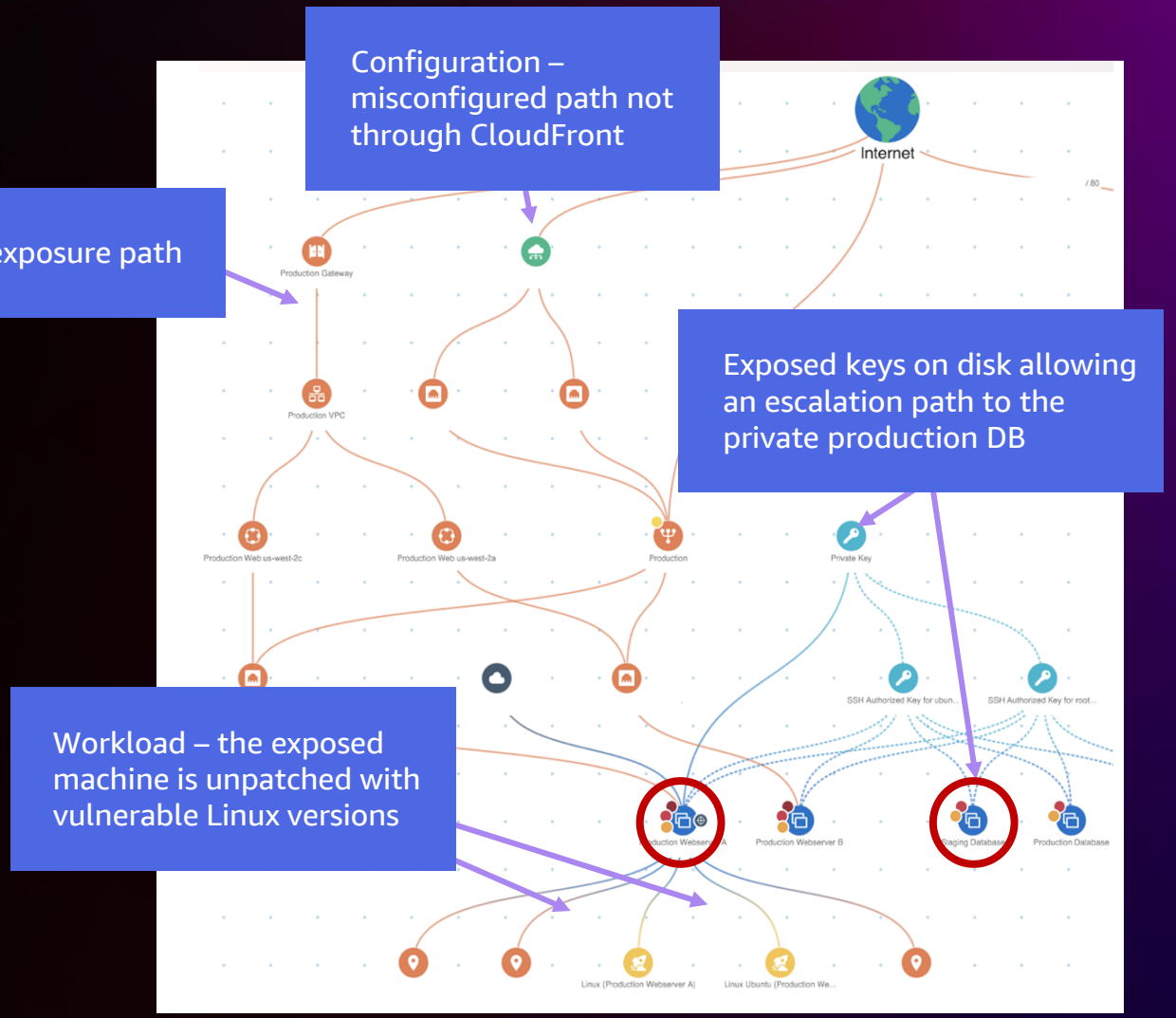
- Vulnerabilities and patches
- Misconfigurations
- Malware
- Sensitive data

Cloud risk engine

- External exposure
- Excessive permissions
- Exposed secrets
- Lateral movement paths

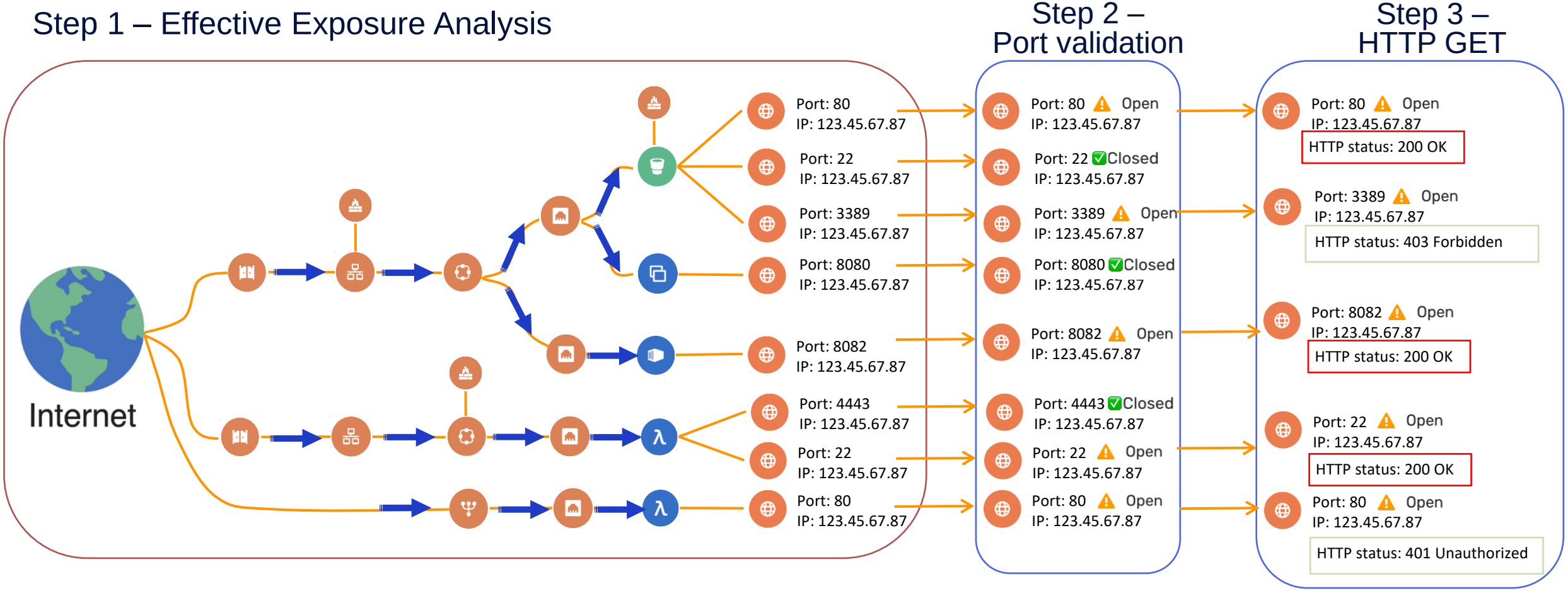
Integrated tools

- AWS CloudTrail
- Amazon GuardDuty
- Amazon Macie
- 3rd party tools



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

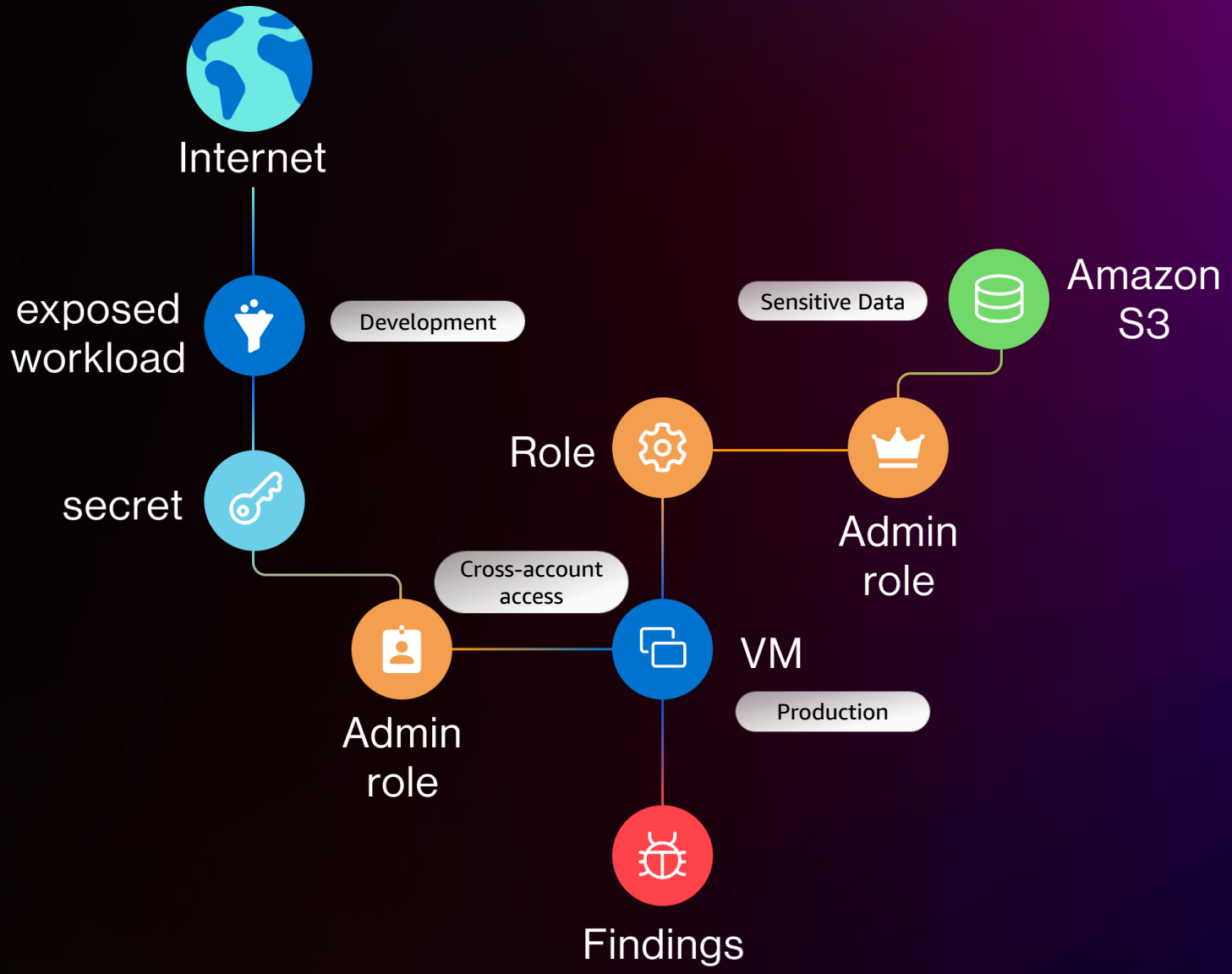
Example: Effective network exposure



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

Example: Escalation path

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



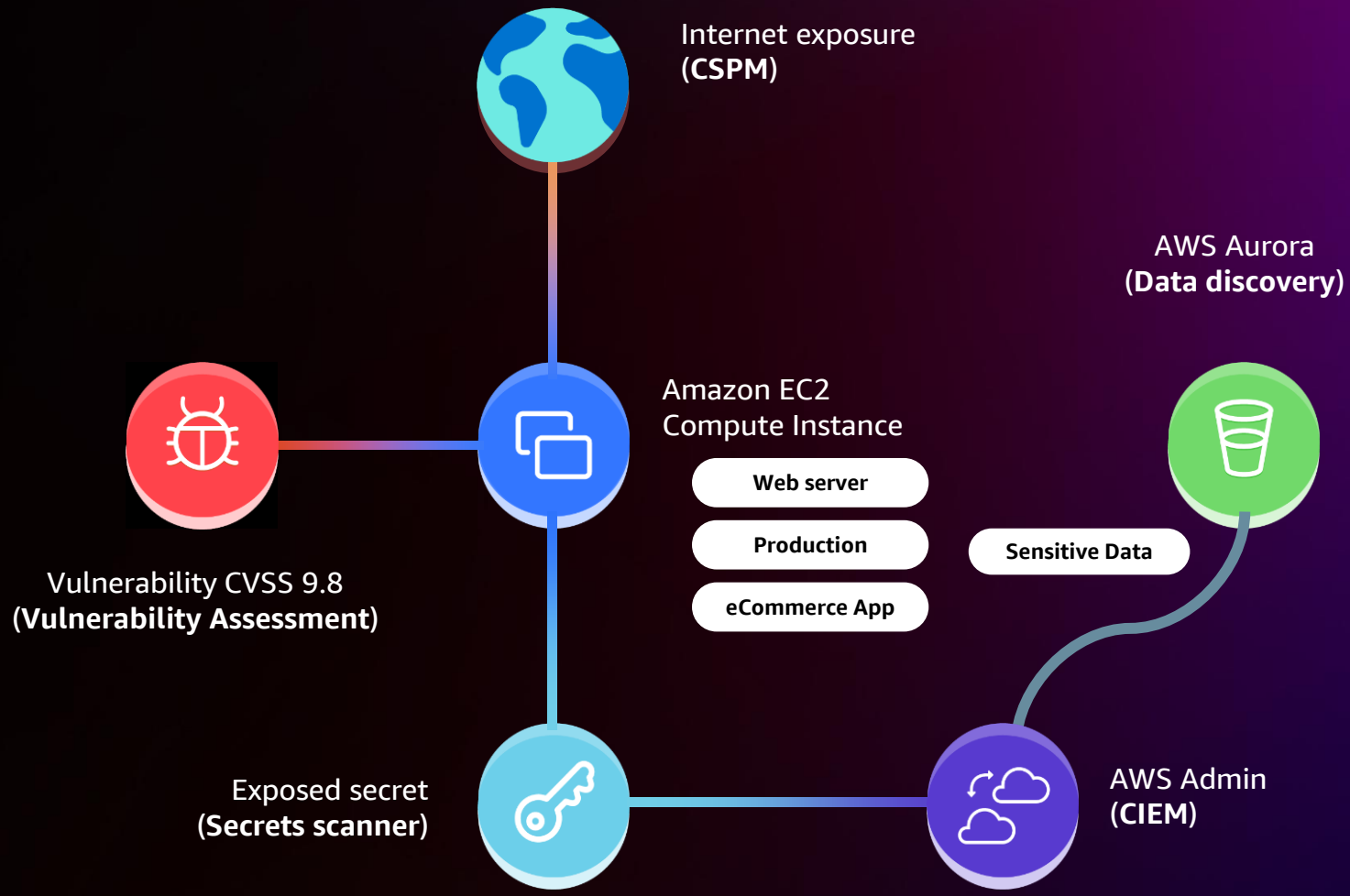
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 3: Prioritize risk and attack paths to critical assets

3 **Identify the most critical risks**

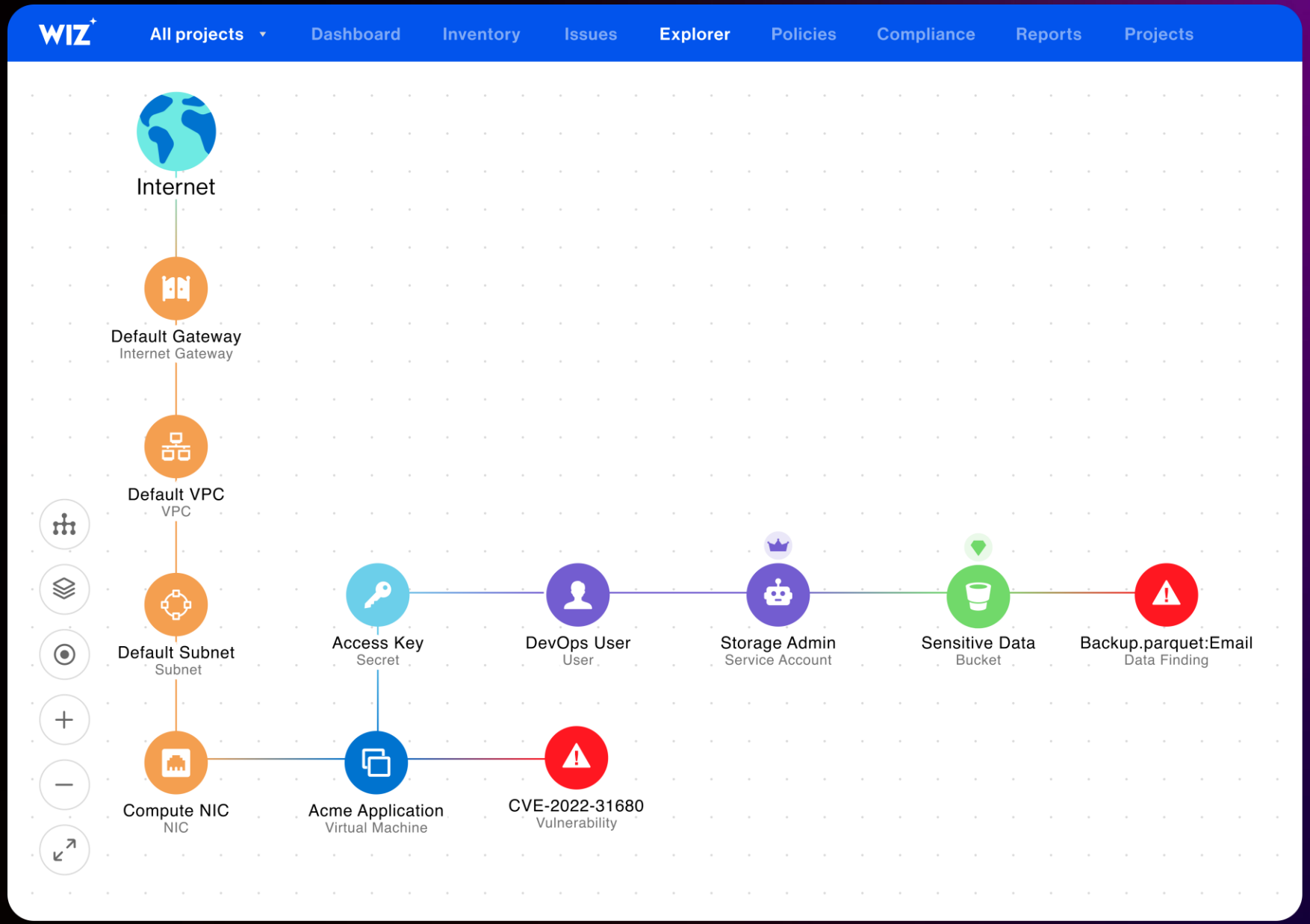
Prioritization and context

- Security findings from Wiz and AWS
- Correlates risk from multiple security domains
- Provides meaningful context
- High fidelity alerting



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

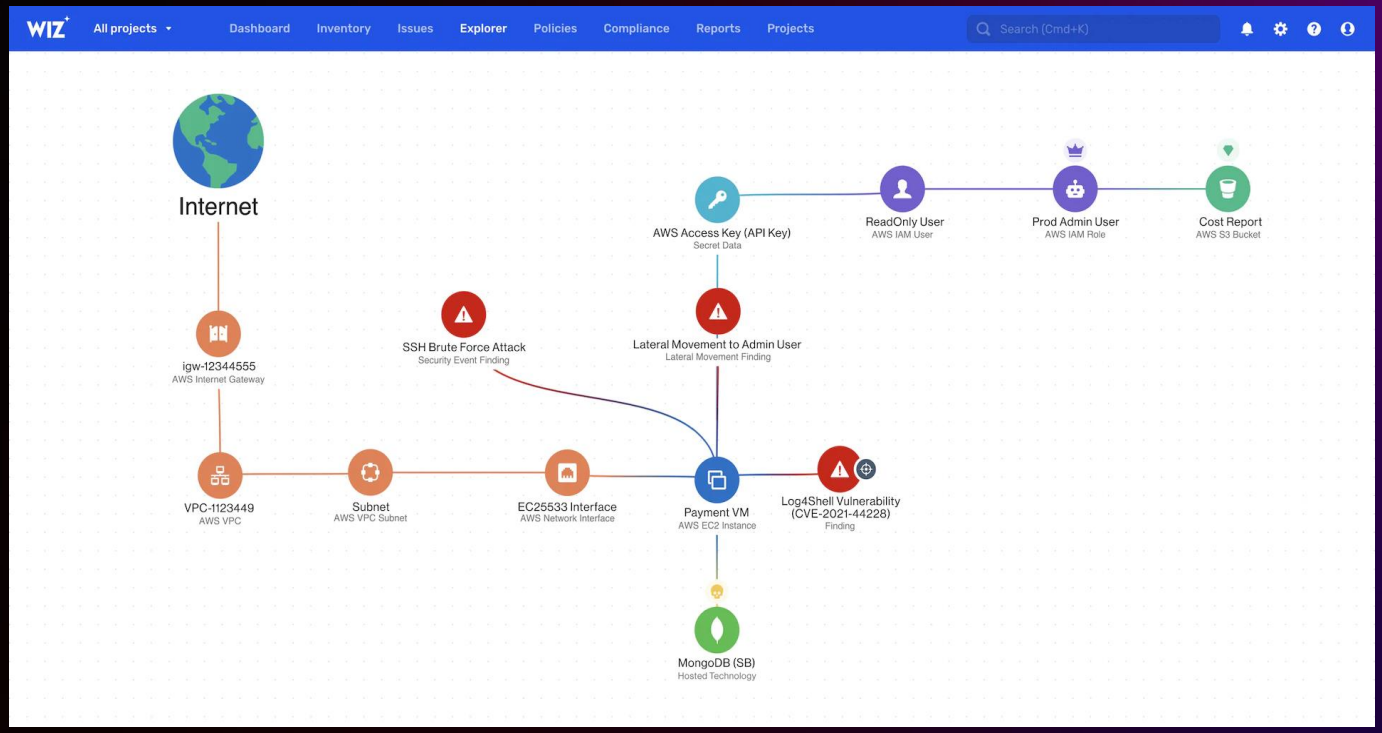
Exposure
+
Vulnerability
+
Secrets
+
Identity
+
Data



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

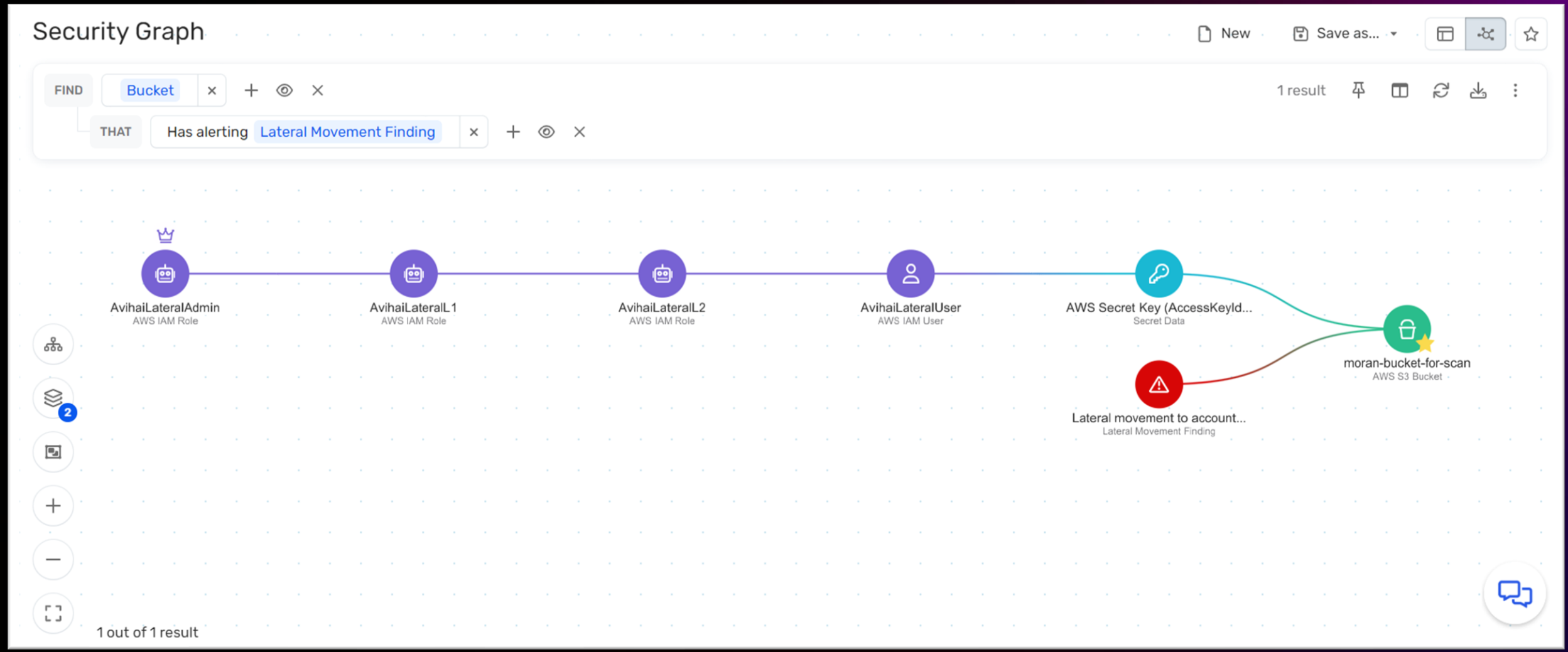
Amazon GuardDuty findings prioritization

- Cloud alerts lack context as well
- Contextualize and prioritize threat detection with the graph
- SSH brute force correlated to a:
  - High-risk workload
  - Password authentication
  - User with a weak password
  - Lateral movement path



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

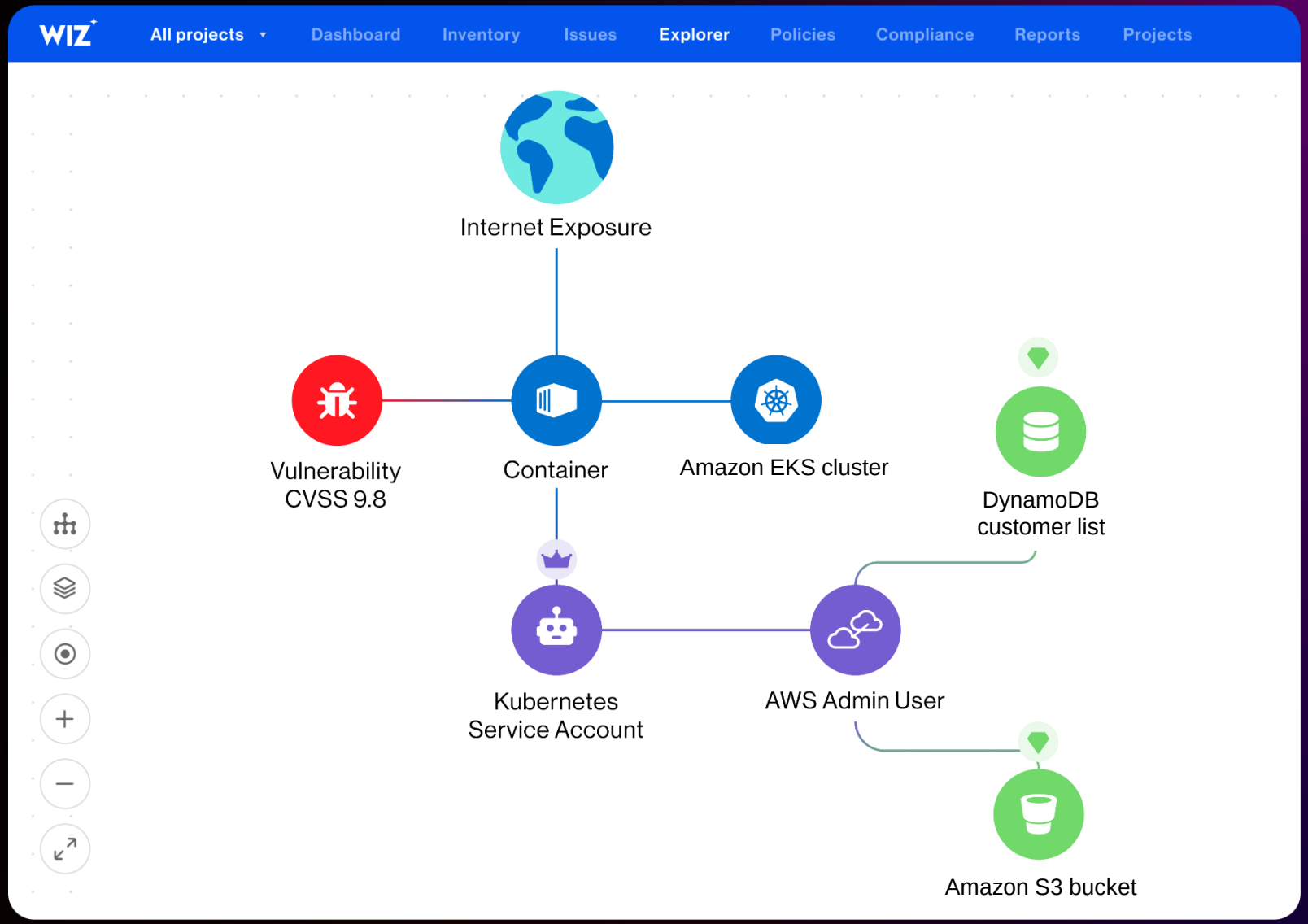
Secrets scanning in data assets



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

Kubernetes, containers, and serverless

- Network exposure
- Vulnerability scanning
- K8s to cloud identity
- Data scanning



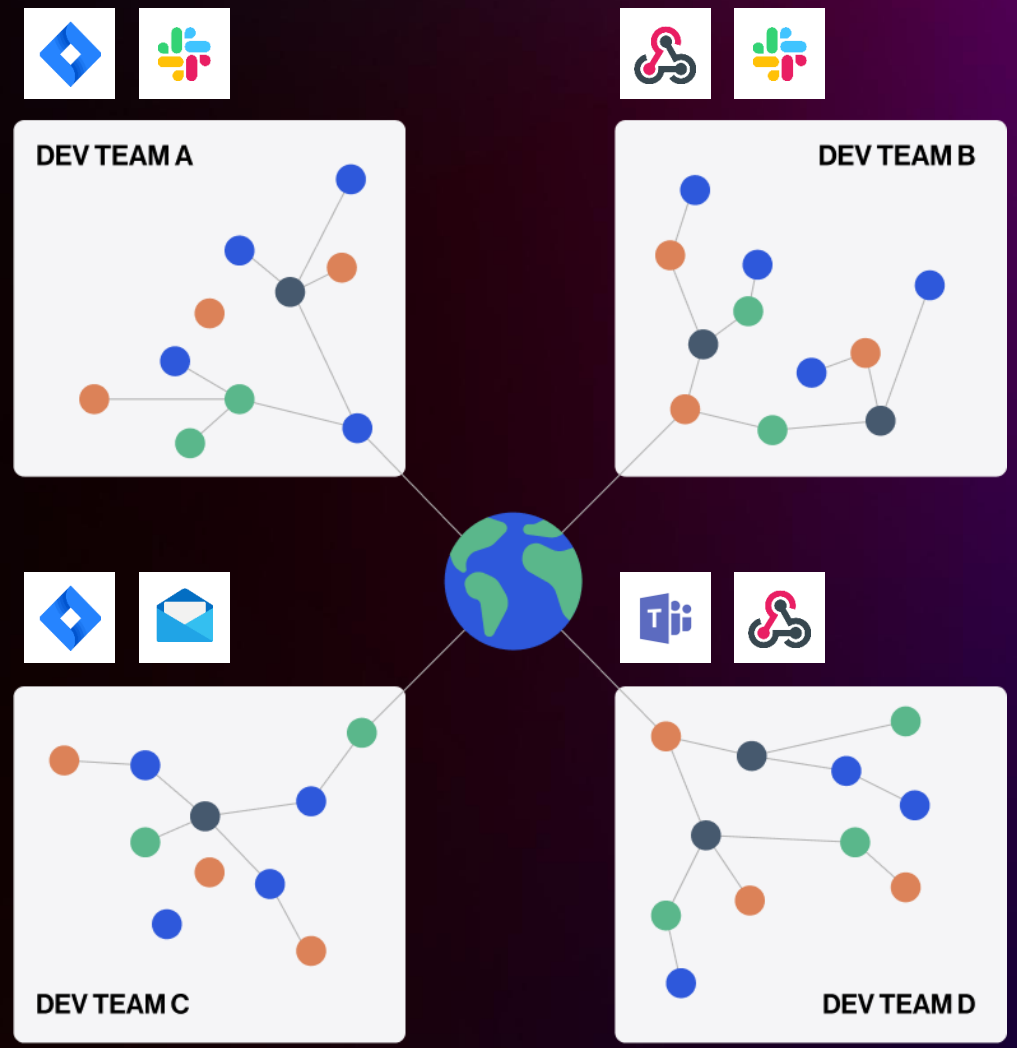
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 4: Proactively harden your cloud

4 Proactively harden your cloud

Democratize security and build process

- Works with your developers' native tooling
- All cloud teams get access to their risks
- Automation to correctly route issues
- Remediation to the left and to the right



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

Wiz for AWS: Cloud Security for Builders and Defenders



Set up within minutes using a cloud role

- Connect with 50+ AWS Services
- Agentless scanning via API
- Cloud and architecture agnostic
- Quick deployment, low maintenance



Real risks, out of the box, no tunning required

- Security findings from Wiz and AWS
- Correlates toxic combinations
- Provides meaningful context
- High fidelity alerting



Democratize security and build a program

- Works with AWS Tooling
- All cloud teams get access to risk
- Automation for correctly routing issues
- Remediation to the left and to the right

aws

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

Connect to Amazon Web Services (AWS)

1. Connection
2. Details

Connection Details



Connect Wiz to your Amazon Web Services (AWS) to gain visibility into your projects security.

How to connect to AWS?

Installation Type

- (•) Standard
- ( ) Wiz Outpost

Create Wiz Role

- (•) CloudFormation
- ( ) Terraform
- ( ) Manual

[ ] **Allow Data scanning**

This will grant the Wiz Role permissions to scan buckets and databases for PII/PCI/PHI or secrets and provide DSPM capabilities

Launch CloudFormation Stack

Before launching the CloudFormation Stack, make sure that you're logged into the AWS account where you intend to deploy the role

Wiz Role ARN

The ARN of the role you have created. How to find Wiz Role ARN.

Cancel

Continue →

Inventory

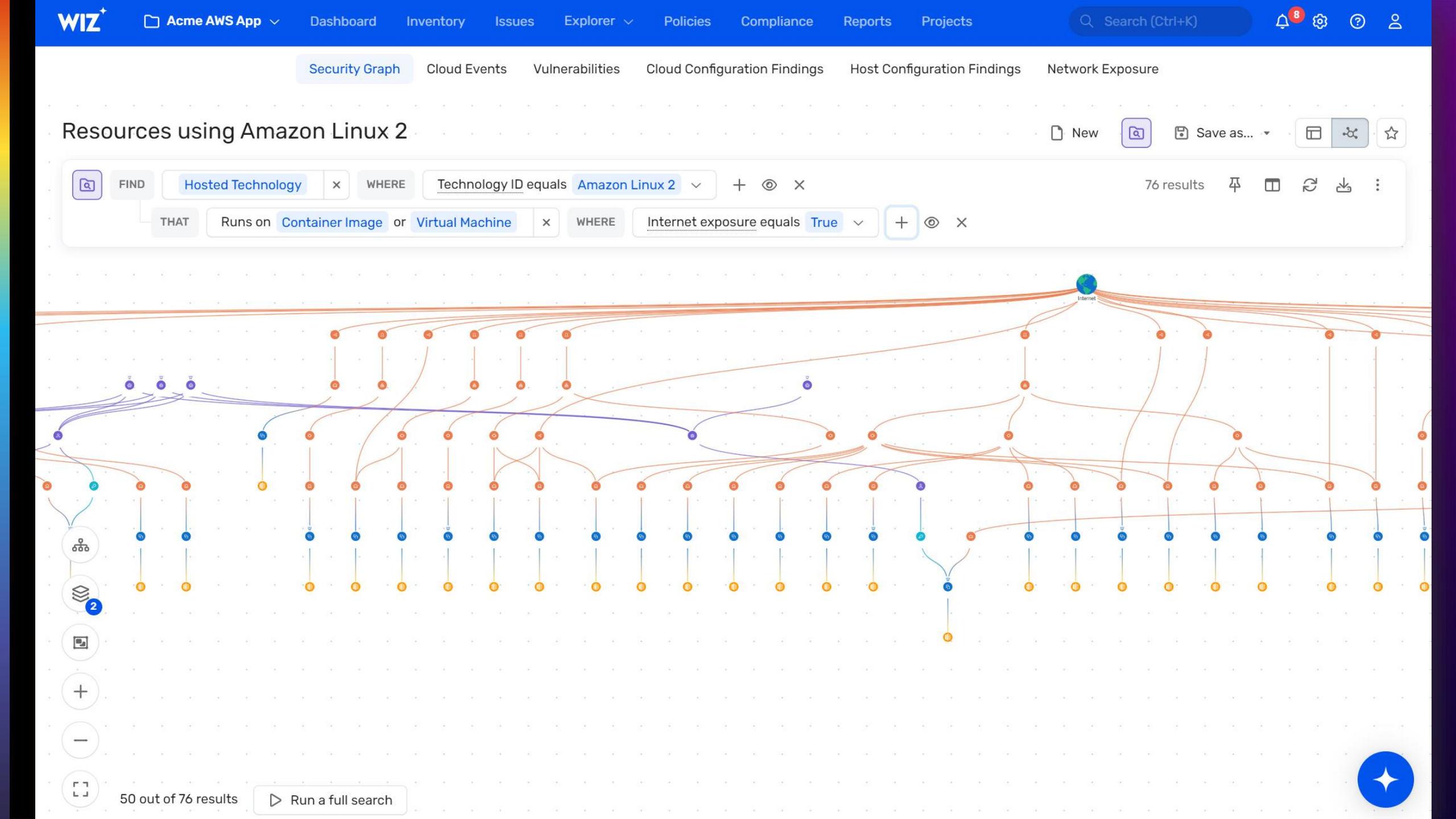
Learn about the Inventory | Suggest a technology

- All Technologies 154
- Code 19
- CI/CD & Management 18
- Compute Platforms 37
  - Cloud Subscriptions 1
  - Container Services 6
  - Serverless 1
  - Virtual Machines 3
  - Operating System 12
  - Networking 14
- Application & Data 42
- Security 25
- Cloud Entitlements 13

Search technologies | Type | Properties | Subscription | 12 technologies

More Filters

Technology	Resource Count	Org. Usage	Type	Status
Amazon Linux 2 Operating System	124 Resources	1 projects Uncommon	Server Application	Approved
Linux Alpine Operating System	4 Resources	1 projects Rare	Server Application	Approved
Linux CentOS Operating System	2 Resources	1 projects Rare	Server Application	Approved
Linux Debian Operating System	16 Resources	1 projects Uncommon	Server Application	Unwanted
Linux Gentoo Operating System	4 Resources	1 projects Rare	Server Application	Unreviewed
Linux Kernel Operating System	157 Resources	1 projects Uncommon	Server Application	Approved
Linux Red Hat Operating System	9 Resources	1 projects Uncommon	Server Application	Required
Linux Ubuntu Operating System	23 Resources	1 projects Uncommon	Server Application	Unwanted
Windows Cumulative Update Operating System	3 Resources	1 projects Rare	Server Application	Approved
Windows Server 2012 R2 Operating System	1 Resource	1 projects Rare	Server Application	Unreviewed
Windows Server 2016 Operating System	1 Resource	1 projects Rare	Server Application	Unreviewed


WIZ
Acme AWS App
Dashboard
Inventory
Issues
Explorer
Policies
Compliance
Reports
Projects
Search (Ctrl+K)
8
Security Graph
Cloud Events
Vulnerabilities
Cloud Configuration Findings
Host Configuration Findings
Network Exposure
Resources using Amazon Linux 2
New
Save as...
FIND
Hosted Technology
WHERE
Technology ID equals Amazon Linux 2
76 results
THAT
Runs on Container Image or Virtual Machine
WHERE
Internet exposure equals True
Internet
2
50 out of 76 results
Run a full search

Controls

Select Framework: Wiz

Learn about Controls | + Create Control

Apply security controls on your cloud environment to have them trigger Issues for your teams to resolve. Controls can create issues for new Security Graph query matches, or for new Cloud Configuration Rule findings.

All Controls 483
1 Patch Management 11
2 Vulnerability Assessment 26
3 Baseline Configuration 91
4 Exposure Management 164
5 Identity Management 210
6 Key & Secret Management 101
7 Supply Chain Management 5
8 Data Security 42
9 Container Security 199
10 Serverless Security 64
11 Malware Detection 12
12 Logging & Monitoring 6
13 Operationalization 1
14 Detection & Response 13

Search control name... | Category | Severity | Created by | Risk | Status | 483 controls

More Filters

Control	Issues	Projects	Severity	Risks	Status
Publicly exposed VM instance with effective global admin permissions Security graph control	18 issu...	All			
High/Critical network vulnerability with a known exploit on a publicly faci... Security graph control	1 issues	All			
CVE-2022-23131 (Zabbix vulnerability) detected on a publicly exposed V... Security graph control	-	All			
CVE-2022-30190 (Follina) detected on a highly privileged container Security graph control	-	All			
Lateral movement path via clear text cloud keys to an admin user Security graph control	-	All			
SSH Brute Force on Admin VM Security graph control	4 issu...	All			
CVE-2022-22963 (Spring Cloud Function RCE vulnerability) detected on ... Security graph control	-	All			
Suspicious network activity on VM infected with malware Security graph control	-	All			
Publicly exposed VM instance/serverless with high/critical severity netw... Security graph control	-	All			
Admin service account can be assumed by a publicly exposed unprivileg... Security graph control	3 issues	All			

Single Framework | Cross Framework

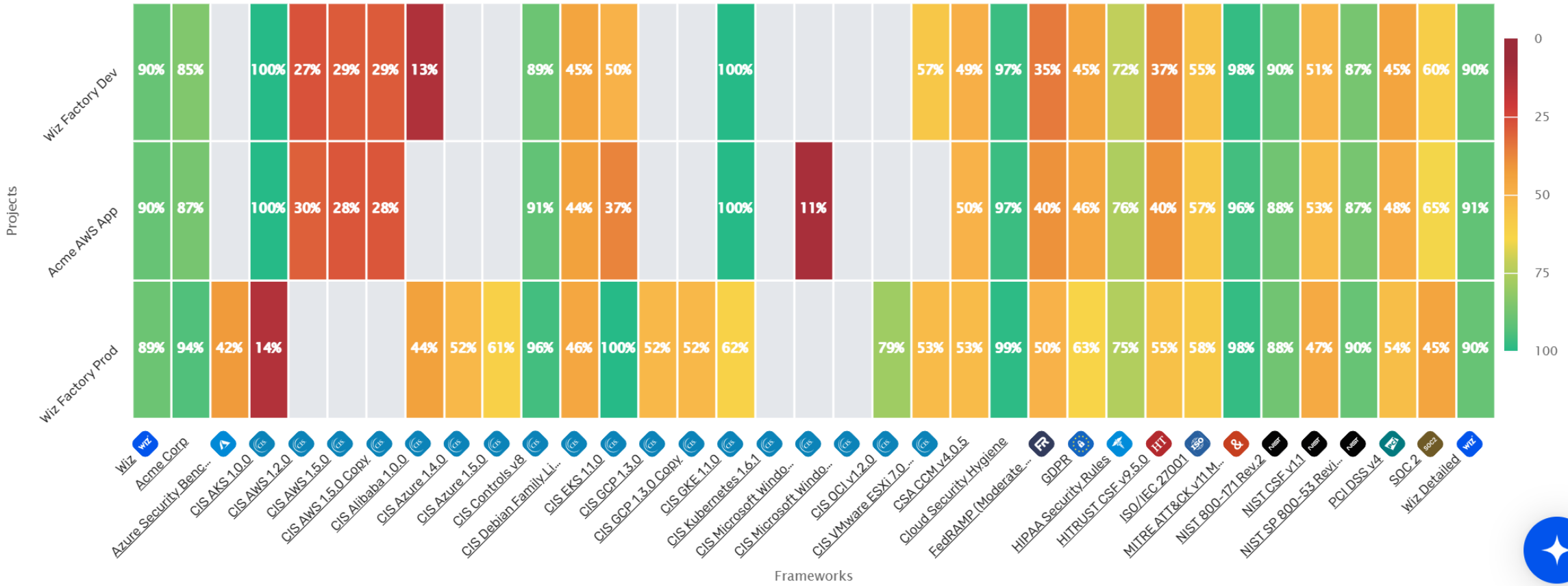
Compliance Heatmap

Learn about Cross Framework Compliance

BREAKDOWN BY: Project | Subscription

Search by name | HBI | MBI | LBI | Policy type | Category | Project is Acme AWS App or Wiz Factory Prod or Wiz Factory Dev | Hide percentages

More Filters | Clear



Issues

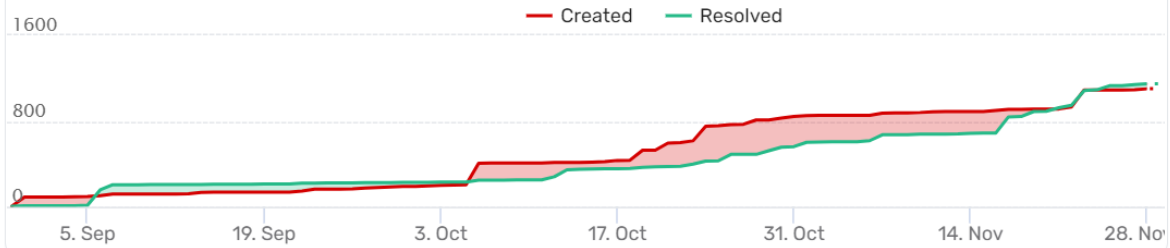
Learn about Issues | Create Automation...

GROUP BY: Type | Resource | Subscription | None

Search control | Risk | Category | Subscription | Severity | Status | Resolution | More Filters | 147 controls

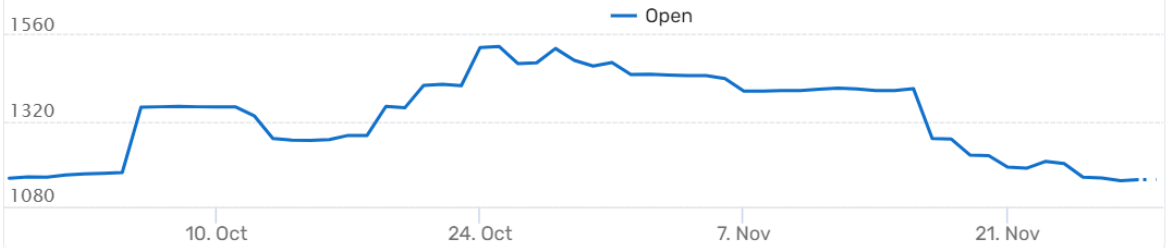
Created vs. Resolved Issues

Total | Last 90 days



Open Issues

Last 60 days



Issue Type (Control)	Total Issues	Risks	Severity
Publicly exposed VM instance with effective global admin permissions	18 issues		
Critical/High network vulnerability with a known exploit found on a publicly exposed VM instance with high permissions	18 issues		
Publicly facing VM instance with data access to sensitive data and high/critical severity network vulnerability with a known exploit	8 issues		
Publicly exposed service account that can be assumed by all users allows lateral movement to admin privileges	7 issues		
Publicly exposed VM instance/serverless assigned a permission combination that could lead to privilege escalation	6 issues		
SSH Bruteforce on Public Machine with Critical Vulnerabilities	5 issues		
Resource infected with critical/high severity malware	5 issues		

WIZ Acme AWS App Dashboard

Issues

GROUP BY Type Resource Subscription

Search control Risk

Created vs. Resolved Issues

1600 800 0 Create

5. Sep 19. Sep 3. Oct 17.

Issue Type (Control)

Publicly exposed VM instance with effec

Issue

Test-Encrypted
EC2 Instance

SB
EC2 Instance

EC2ContainerService-ecs-on-ec2-clu
Auto Scaling Group

Ephemeral_spotinst:aws:ec2:group:id
Spotinst Synthetic Instance Group

arn:aws:ec2:eu-west-2:984186218765
EC2 Instance

Publicly exposed VM instance with effective global admin permissions

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

Description

Description

This VM is exposed to the public internet and has admin permissions in the environment. Admin permissions allow persistence in the environment, or have wild card permissions on the subscription, account, or project level.

Potential Impact

Publicly exposed resources are more easily accessible for an attacker than internal ones. Moreover, highly privileged resources are a greater risk to the environment when compromised. Therefore, an attacker that manages to execute code on the publicly exposed VM can abuse the privileges, potentially performing administrative operations.

Status
Open

Due
Oct 23rd 2022

Created
Jul 18, 2022 at 3:46 PM

Updated
Nov 28, 2022 at 5:29 AM

Severity
Critical

Compliance Frameworks
+2

Risks

Subscription
AWS Demo Scenarios
us-east-2

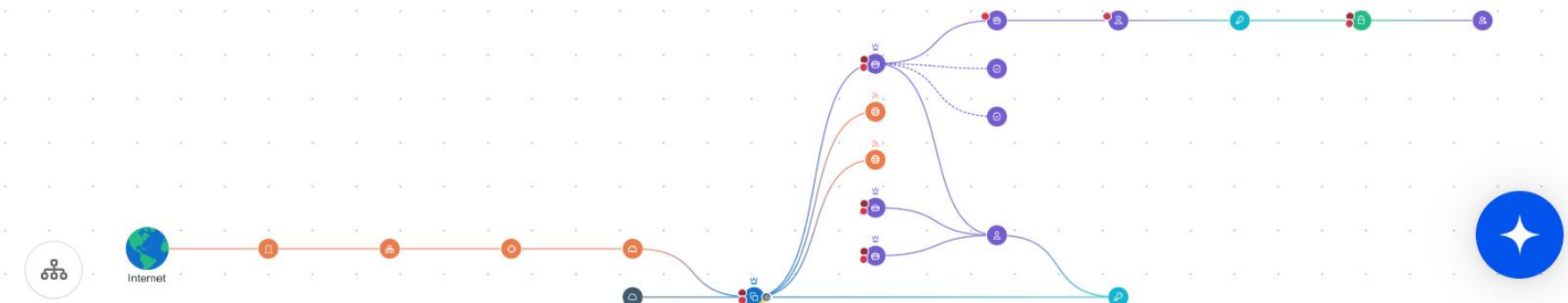
Projects
3 Projects

Related Tickets
1 Ticket

Evidence

Overview

View on Graph



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.

Dashboards

Quick Start Guide
Threat Center

Overview
External Exposure
Cloud Entitlements
Secure Configuration
Secure Use of Secrets
Data Security
Containers
Serverless
Vulnerabilities
Patch Management
Malware
Log4Shell Vulnerability
Monitoring

Threat Center

Hide threats without findings or issues | Create Automation

Last 30 days

Public bucket with sensitive data or secrets

Nov 23rd 2022, source: Wiz Threat Research

Data breaches have become more common as attackers become acutely aware of the value of sensitive data and the increasing difficulties in keeping it secure. Research shows that attackers continuously scan the internet for exposed databases and buckets, so it's vital to identify and address such issues immediately. Wiz analyzes your cloud infrastructure and data assets to determine whether they contain sensitive data or secrets, and correlates the Data Findings with other contextual risk factors such as exposure to help you identify any possible data leaks. Use the following controls to detect buckets with sensitive data exposure issues and follow the remediation steps for guidance on how to fix them.

Read more

4
Issues

More than 30 days old

High severity vulnerabilities in OpenSSL 3.0

Oct 27th 2022, source: Wiz Threat Research

On November 1, 2022, OpenSSL released version `3.0.7` to fix high severity vulnerabilities CVE-2022-3602 and CVE-2022-3786. This publication followed an earlier announcement of the OpenSSL team about a critical security issue in OpenSSL 3.x, however per the team's official message, the severity was **reduced to high**. According to Wiz Research analysis, exploitation of the published vulnerabilities is complex. For more details refer to our advisory.

Read more

1
Issue

Text4Shell: Critical RCE vulnerability in Apache Commons Text

Oct 19th 2022, source: Wiz Threat Research

CVE-2022-42889, a critical vulnerability, dubbed as "Act4Shell" or "Text4Shell", was found in the Apache Commons Text library and could potentially allow it execute code when processing malicious input. However, the nature of the vulnerable `StringSubstitutor` interpolator means that getting crafted input to the vulnerable object is less likely. Users are advised to

1
Issue

Where Wiz fits in the security stack today

Wiz CNAPP

CSPM	Secure cloud and Kubernetes configuration Cloud external attack surface management Cloud Infrastructure Entitlement Management (CIEM)
CWPP	Vulnerability and secure configuration assessment Container and serverless security Secrets scanning Malware scanning
CNAPP	Asset Inventory and Security Graph Attack Path Analysis (APA) Toxic Combination and risk prioritization Cloud Detection and Response (CDR) Data Security Posture Management (DSPM)

Wiz Guardrails (CI/CD integration)

DevSecOps	Container image scanning VM Image Gallery scans Registry scanning IaC Scanning (TF, CF, ARM, YAML, …) Kubernetes Admission Controllers

Wiz complements

SaaS security (CASB, SASE, SSPM)

Identity Management, Access and Zero trust (IAM, ZTNA)

Application Security (SAST, DAST, WAF)

Runtime Protection and behavior analysis (EDR, UEBA)

Orchestration and event management (SIEM, SOAR)

aws

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

Wiz provides immediate business value for AWS customers

Risk mitigation

- Eliminate blind spots
- Prevent issues in production
- Ensure readiness
- Scale in the cloud seamlessly

Operational efficiency

- Eliminate overhead of agents
- Reduce noise and manual effort
- Automate governance
- Speed remediation

Cost reduction

- Reduce license, deployment, integration, and support costs of point security products
- Identify unnecessary cloud usage

Accelerate the business

- Keep your devs focused on building
- Prevent issues in production
- Ensure readiness
- Scale in the cloud seamlessly

aws

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

Fireside chat



John Visneski
CISO – MGM Studios

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

Q&A

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

Visit us at booth #419

Learn more at www.wiz.io | Find Wiz in the AWS Marketplace

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

Thank you!



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

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