AISHIELD

WIZ

Secure Everything You **Build** and **Run** in the Cloud

Patrick Chen | Director of SecOps | AIShield Co.

WIZ

AISHIELD

Nothing changed.

The deal is subject to regulatory review, so we are not yet part of Google.

Wiz will continue to remain multi-cloud

and work across AWS, Azure, Google, Oracle and more, as well as on-premises environments.

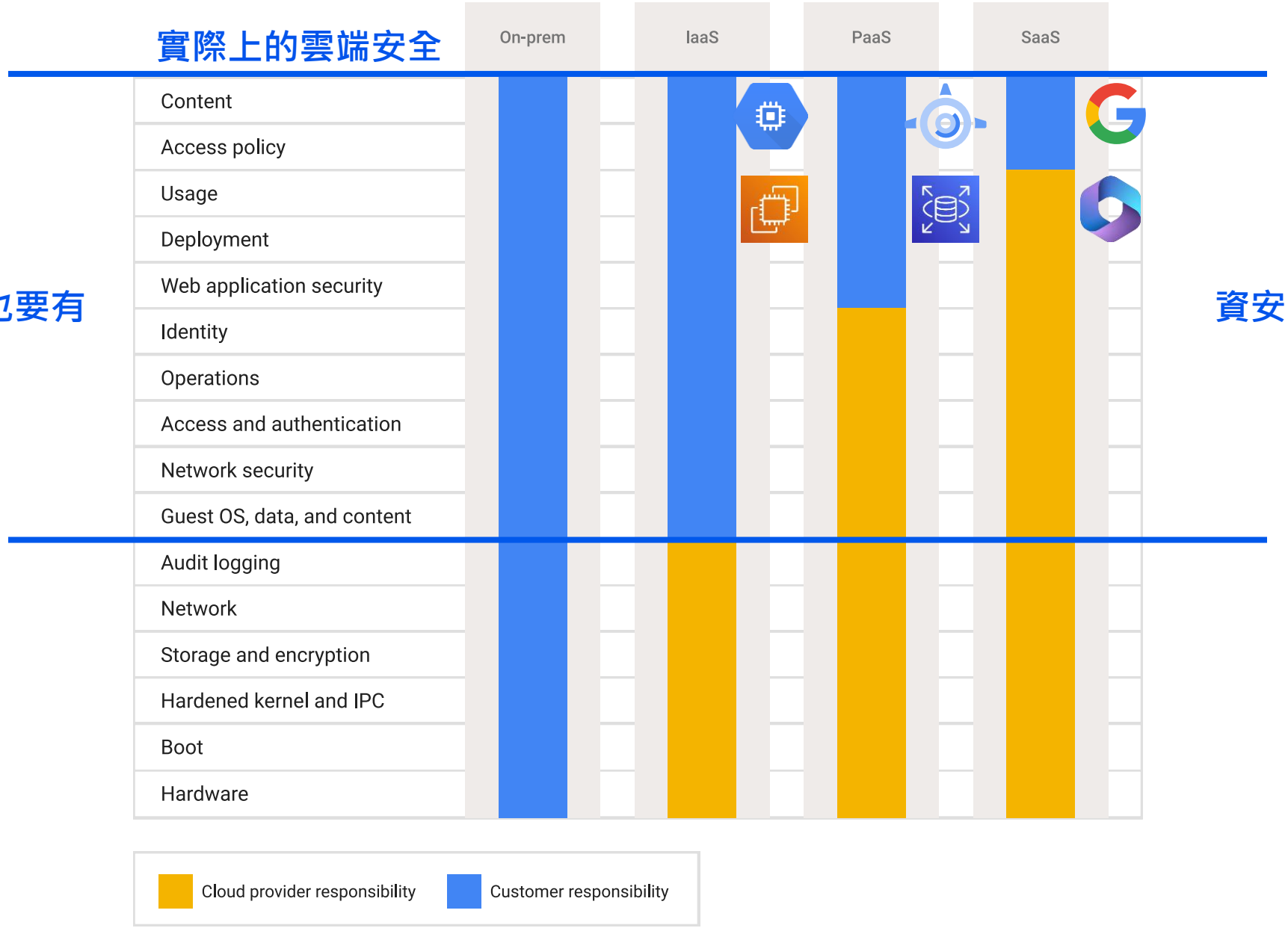
Shared responsibilities and shared fate on Google Cloud

Shared responsibilities and shared fate on Google Cloud

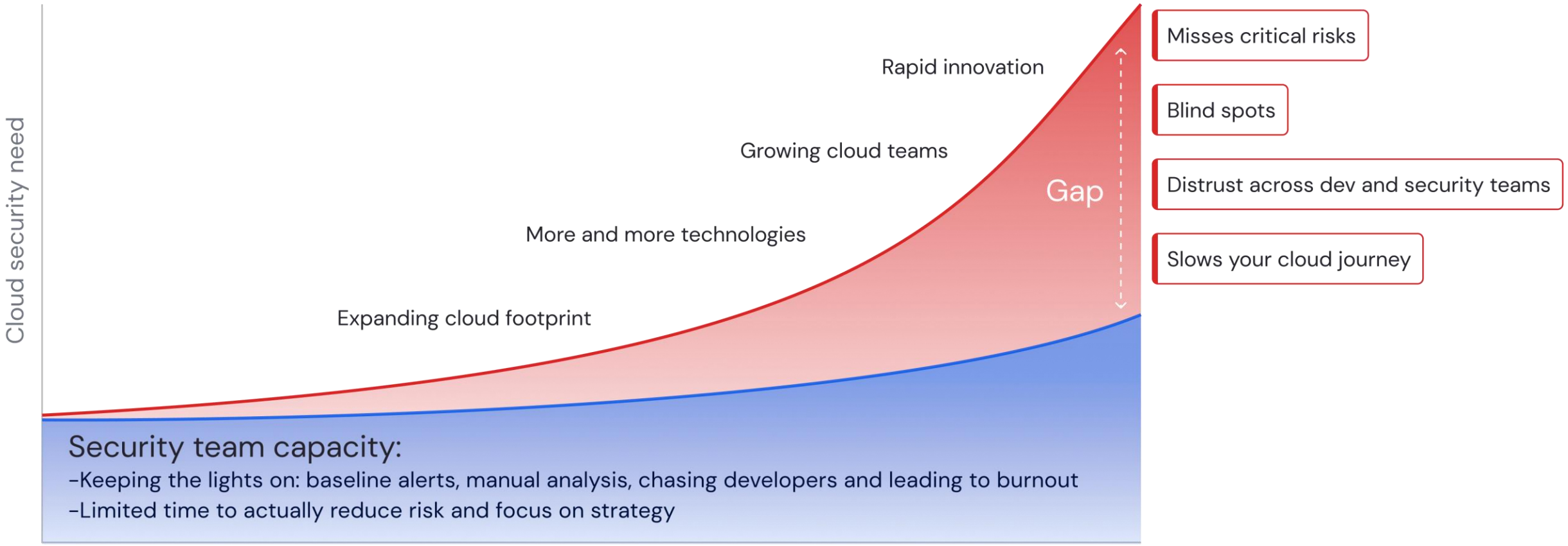
實際上的雲端安全

地端的防護雲端也要有

資安人員該如何應對



The time to scale your cloud security model is now



We can't keep doing the same thing.

Cloud Risks, Threats, and Challenges

Risks

1. **Data breaches**(#2018 #Uber #data_breach #misconfiguration)
2. **Inadequate identity access management**(#2017 #Equifax #data_breach #IAM_controls)
3. **Insecure APIs**(#2018 #Facebook #Cambridge #presidential_election)
4. **Insufficient cloud configuration management**(#2019 #Capital_One #WAF #data_breach)
5. **Shared infrastructure vulnerabilities**(#2018 #GCP #configuration_change)
6. **Shadow IT**(#2019 #healthcare_org #file_sharing_service #data_breach)
7. **Human error**(#2025 #DeepSeek #data_breach #misconfiguration)

Cloud Risks, Threats, and Challenges

#2016 #Uber #data_breach #misconfiguration

Bloomberg 針對該起事件的說明如下：

- 駭客進入了 Uber 所使用的私人 GitHub 程式碼網站。
- 駭客在該 GitHub 網站當中發現了 AWS 登入憑證。
- 駭客利用這些 AWS 登入憑證取得了個人身分識別資訊。

如同大多數駭客事件一樣，這並非什麼複雜的攻擊，而且可歸咎於受害者自身流程上的疏失，決非因為 GitHub 或 AWS 的安全問題而導致。

Uber 採取了最糟的做法:試圖掩蓋

但這次的案例，Uber 卻採取了最糟的做法。他們選擇不公開資料外洩的事實，而且還支付歹徒 10 萬美元的封口費。不但如此，他們還刻意讓這筆款項看起來像是臭蟲懸賞計畫的獎金，讓場面更加難看。

付款給歹徒絕對是不明智的作法，而試圖掩蓋一起影響數千萬人的事件更是讓人無法容忍。

掩蓋個資外洩事件 Uber前安全長遭判2項罪名成立

2022/10/6 15:19

（中央社舊金山5日綜合外電報導）美國叫車服務業者優步（Uber）2016年間遭駭客竊取大量用戶和駕駛個資。加州北區聯邦地區法院陪審團今天裁定，Uber前安全長蘇利文的妨礙司法和隱匿重罪兩項罪名成立。

綜合法新社和路透社報導，蘇利文（Joseph Sullivan）遭控在2016年Uber遭駭時選擇隱瞞，不僅未向聯邦貿易委員會（Federal Trade Commission）通報非法入侵事件，還涉嫌以加密貨幣比特幣支付駭客10萬美元，要求對方銷毀個資，並簽下保密協議，承諾對此事三緘其口。

這起事件造成5700萬名乘客及司機個資外洩，且在發生1年後，Uber才揭露自己遇駭。

根據刑事訴狀，蘇利文試圖透過「安全漏洞回報獎勵計畫」（Bug Bounty Program），匯款給駭客。這項計畫旨在獎勵開發人員，在不造成任何傷害的情況下，找出安全漏洞。

Cloud Risks, Threats, and Challenges

#2018 #Facebook #Cambridge #presidential_election

新聞

Meta以7.25億美元和解劍橋分析事件引發的集體訴訟

這是美國獲賠金額最高的隱私集體官司，也是Meta支付賠償金額最高的集體官司

2018 年的劍橋分析案中，臉書平台上的第三方 App 透過其 API 存取用戶個資，超過 8,000 萬用戶受害。當時臉書也說已經全面檢視所有 API 及可存取的廠商名單，承諾減少 App 開發商不當接獲用戶個資的可能性。

劍橋分析如何取得資料？如何運作？

劍橋分析透過一位劍橋大學教授柯根(Aleksandr Kogan)所建置的性格分析APP(thisisyourdigitallife)來搜集個人用戶資料。這款APP吸引了幾十萬人下載，而這些人也在使用App的同時同意了個人資料可作為學術用途。但有爭議的是，使用者不知道此款APP所搜集的資料不只是使用此APP的用戶，也包含使用用戶的所有好友的個人資料，最後他們總共非法搜集了5000萬個用戶資料。

"劍橋分析"公司正面臨是否利用個人數據影響美國2016年總統大選和英國脫歐公投的調查。

"劍橋分析"究竟是一家什麼樣的公司？該公司網站吹噓曾在世界五大洲支持並開展過逾100場活動，其涵蓋範圍遠遠超出英國和美國。

"劍橋分析"公司已暫停首席執行官亞力山大·尼克斯（Alexander Nix）的職務。英國電視台第四頻道（Channel 4）周一（3月19日）播出了該台一名記者對尼克斯進行臥底採訪時秘密拍攝的視頻畫面。尼克斯在視頻中舉例說明了該公司怎樣通過耍花招來影響選舉，比如對候選人進行抹黑，或施以圈套或誘惑等手段。

這家總部位於英國的公司否認有任何不當行為。"劍橋分析"在世界各地有眾多的活動記錄，下面我們來看看有哪些：

Cloud Risks, Threats, and Challenges

#2025 #DeepSeek #data_breach #misconfiguration

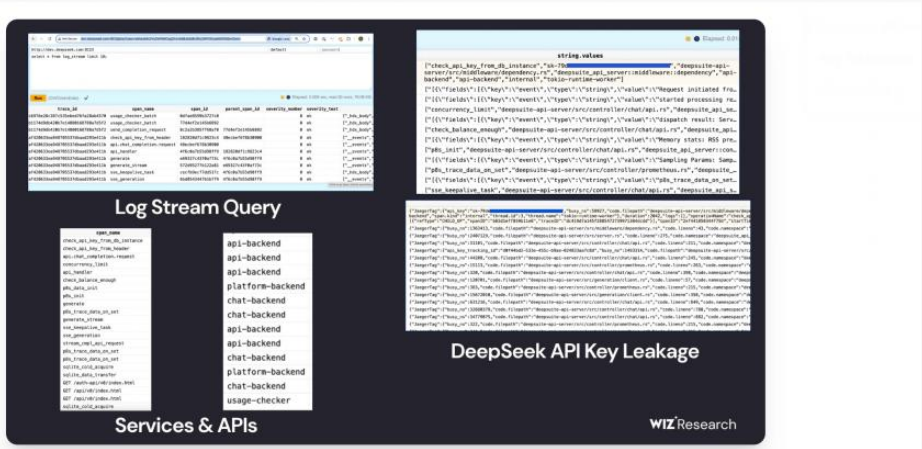
新聞

爆紅中國AI服務DeepSeek資料庫配置錯誤導致機密日誌外洩

Wiz Research發現中國人工智慧服務DeepSeek的ClickHouse資料庫配置錯誤，未設身分驗證，導致百萬筆機密日誌外洩，含聊天記錄、API金鑰與內部資料

文/ 李建興 | 2025-01-30 發表

讚 1,004 分享



中國人工智慧公司DeepSeek因其模型DeepSeek-R1表現亮眼而備受關注，不過，雲端資安公司Wiz Research研究團隊發現，DeepSeek服務存在重大資安漏洞，導致大量機密日誌資料外洩。研究人員在進行例行性安全評估時，發現DeepSeek的ClickHouse資料庫對外開放，未設定任何身分驗證機制，允許任何人存取內部資料，甚至具備完整的資料庫控制權限。

Wiz Research透過網域探測技術，發現DeepSeek旗下多個公開網域，其中部分開放了非標準的HTTP連接埠，進一步檢測後確認ClickHouse資料庫可透過9000及8123連接埠直接存取，且無需提供任何驗證資訊。這個資料庫包含超過百萬筆日誌紀錄，涵蓋聊天記錄、API金鑰、內部服務資訊、目錄結構與營運相關細節。更具風險的是，研究人員發現該ClickHouse資料庫允許透過HTTP介面執行任意SQL查詢，攻擊者不僅能存取內部資料，還可能透過特定查詢獲取機密資訊，進一步擴大攻擊影響範圍。

Cloud Risks, Threats, and Challenges

Threats

1. **Account hijacking**(#2019 #Capital_One #IAM_token #data_breach)
2. **Denial of service attacks**(#2020 #AWS #DDoS #2.3Tb/s)
3. **Insider threats**(#2023 #Tesla #employees #data_breach)
4. **Cloud malware injection**(#2017 #Coinhive #mining)

Cloud Risks, Threats, and Challenges

#2023 #Tesla #employees #data_breach

特斯拉100GB機密傳外洩 馬斯克個資遭露出「最重罰千億」

徐如奕
2023年5月29日

特斯拉被爆出大規模資料外洩，包含馬斯克本人、前現任員工、客戶個資，以及內部機密，德國政府著手調查中。(AP)

電動車特斯拉（Tesla）日前遭德國媒體爆料有大規模資料外洩，包含員工、客戶的個資，以及電動車製造商的文件，甚至連自家執行長馬斯克（Elon Musk）的私人信箱、電話都在其中。德國資料保護辦公室正在調查，若認定違反歐盟《一般資料保護規則》（GDPR），特斯拉將面臨最高35億美元（約新台幣1072億元）的罰金。

特斯拉位於荷蘭的歐洲總部獲報後，已對此提供初步報告說明，《商報》也引述特斯拉法律團隊的說法：「一名『心懷怨恨的前員工』，濫用他擔任服務技術人員的權限獲得個資、機密，公司將對這名疑似洩密的人採取法律行動。」

Cloud Risks, Threats, and Challenges

Challenges

1. **Complex regulatory compliance**(#2020 # British_Airways #GDPR #£20_million)

2. **Lack of visibility**(#2017 #Target #data_breach)

3. **Lack of cloud security professionals**(#2023 #T-Mobile #data_breach)

4. **Data governance** (#2019 #Facebook #Third_Party #S3_Bucket)

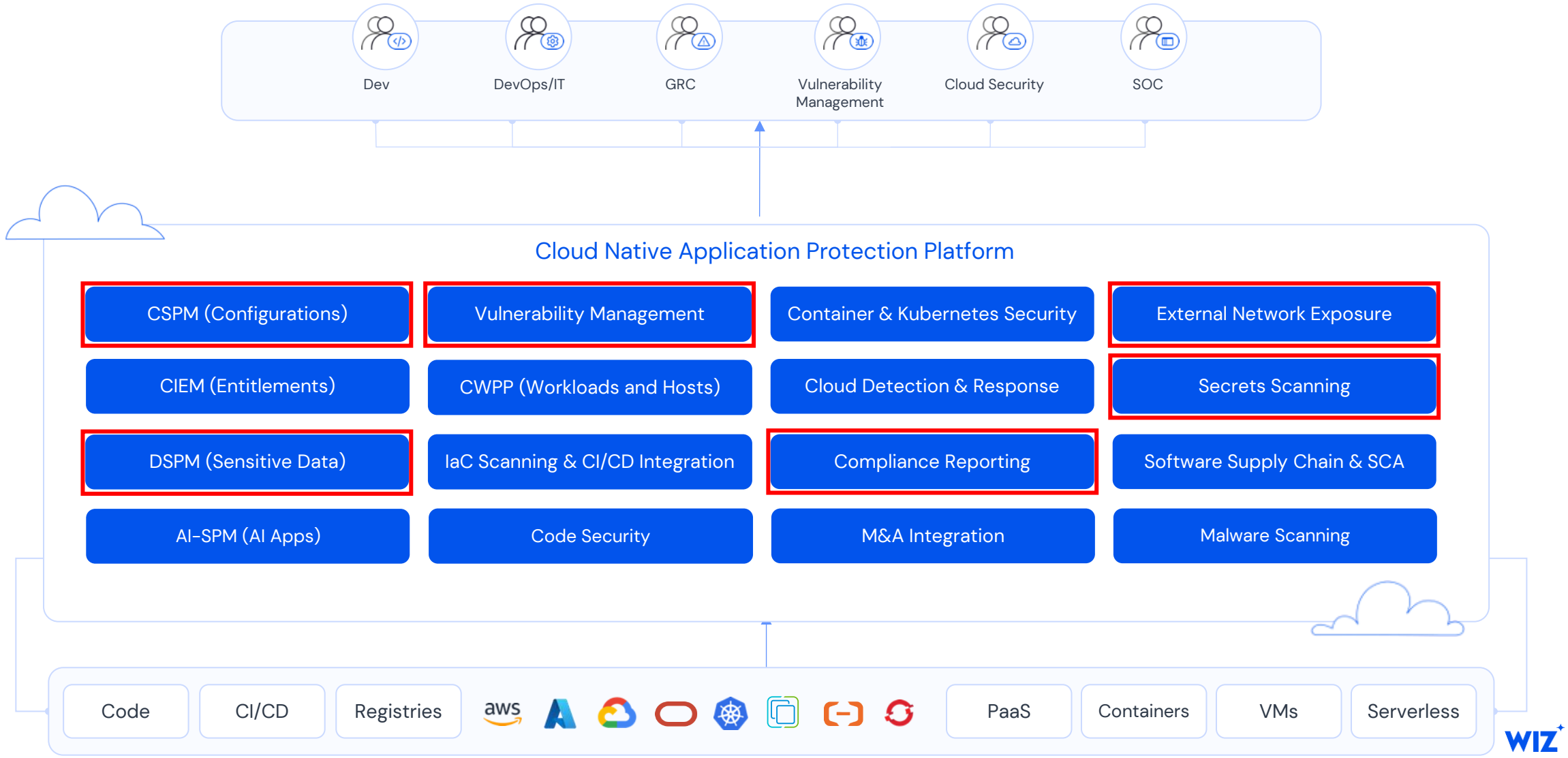
5. **Managing a rapidly evolving attack surface**(#2022 #Microsoft #Blob_Storage #2.4TB)

6. **Multi-cloud security**

   Benefits of a multi-cloud strategy

   - Increased flexibility
   - Reduced vendor lock-in
   - Improved uptime through geo-redundancy
   - Better compliance with regulations.

One **unified platform** for your cloud security journey



One platform for the modern cloud security operating model

Dev | DevOps/IT | GRC | Cloud Security | Vuln Mgmt | SOC | IR

Wiz Platform

Wiz Code
Secure Cloud Development

Secure every stage of your SDLC to gain visibility & prevent risks in code, pipeline, registries and images

Wiz Cloud
Manage Security Posture

Agentless visibility & risk prioritization that proactively reduces the attack surface

Wiz Defend
Respond to Cloud Threats

Cloud events and lightweight eBPF-based sensor to protect from unfolding threats as a last line of defense

Root cause analysis for risks and threats (Cloud to Code)

Build securely by design and detect drift (Code to Cloud)

One platform for the modern cloud security operating model

Dev | DevOps/IT | GRC | Cloud Security | Vuln Mgmt | SOC | IR

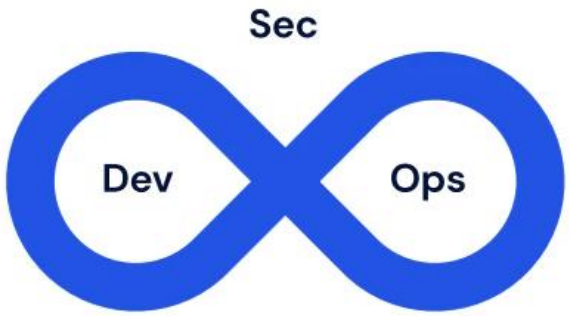
CNAPP Detailed View

Wiz Code

Artifact Scanning

- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Wiz Cloud



Cloud Configuration

- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlement Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

Wiz Defend

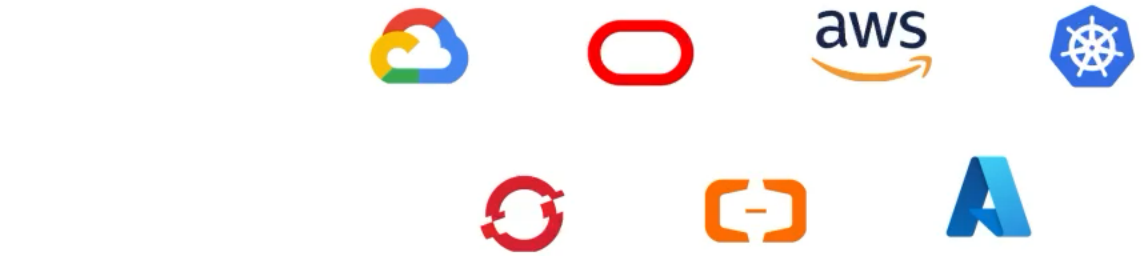
Runtime Protection

- Web Application and API Protection
- Application Observability
- Cloud Workload Visibility
- Network Observability
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

The cloud security operating platform

Scan your cloud without agents and build the graph

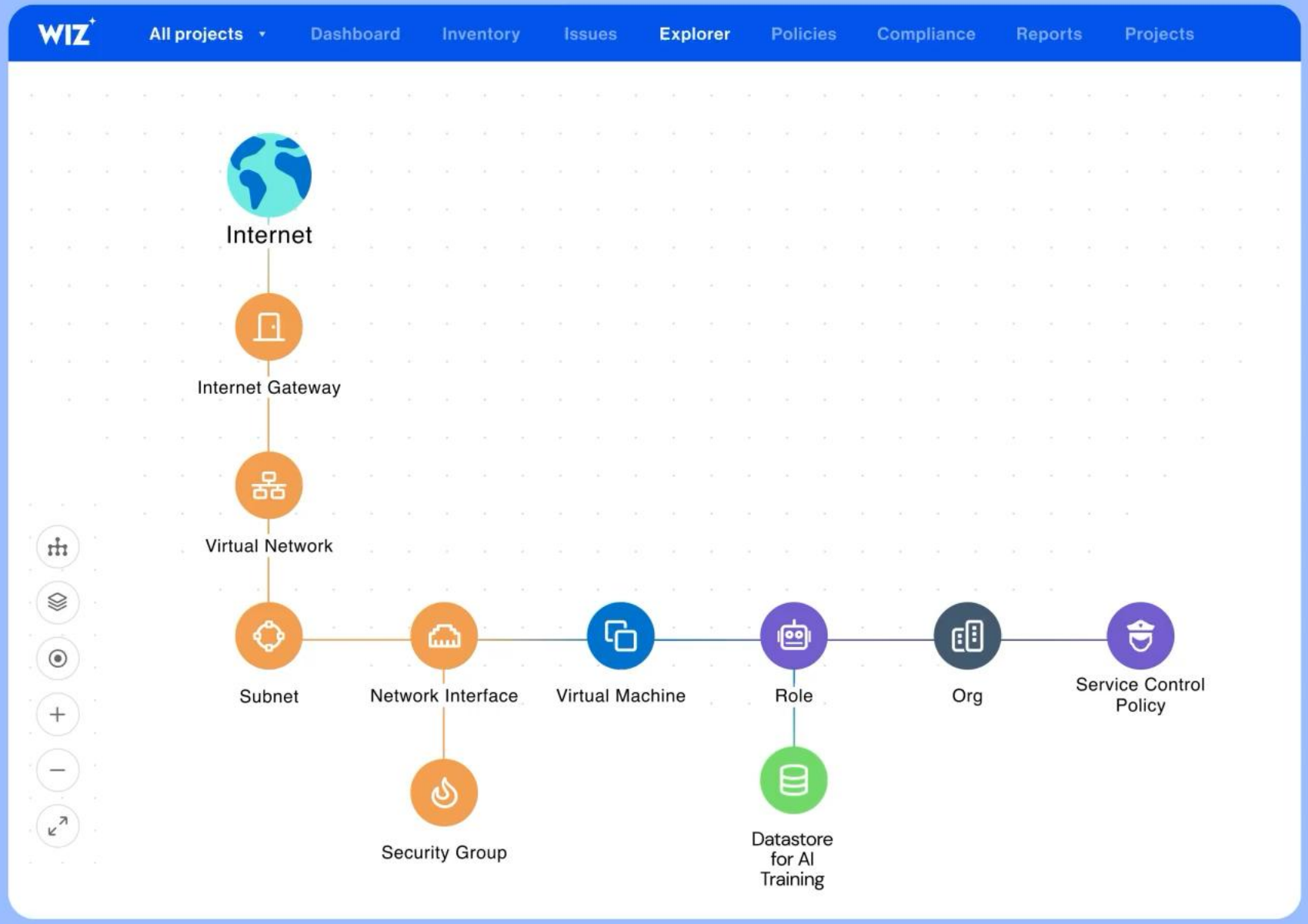
- Serverless
- Containers
- VMs
- PaaS



The cloud security operating platform

Identify risks

- Misconfigurations
- Vulnerabilities
- Malware
- Sensitive data
- External exposure
- Excessive permissions
- Exposed secrets
- Lateral movement
- AI risks
- Novel vulnerabilities and attacks
- Business impact



The cloud security operating platform

Prioritize attack paths

wizlabs | All projects

Search CTRL K

Security Graph

New Search | Save as...

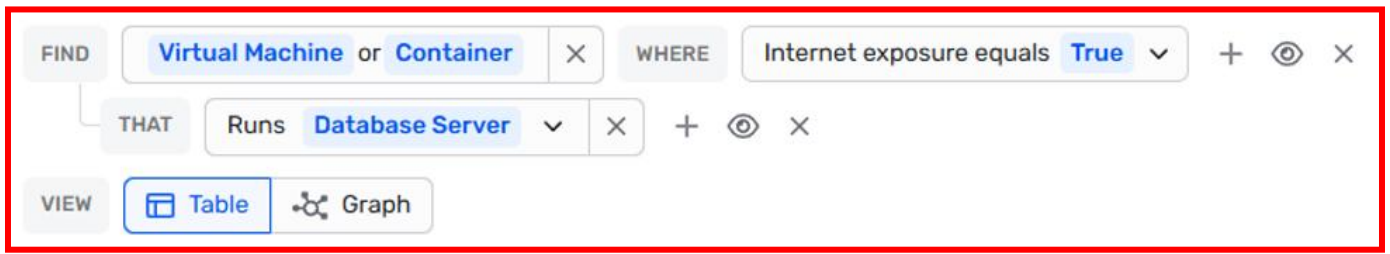
FIND Virtual Machine or Container | WHERE Internet exposure equals True

THAT Runs Database Server

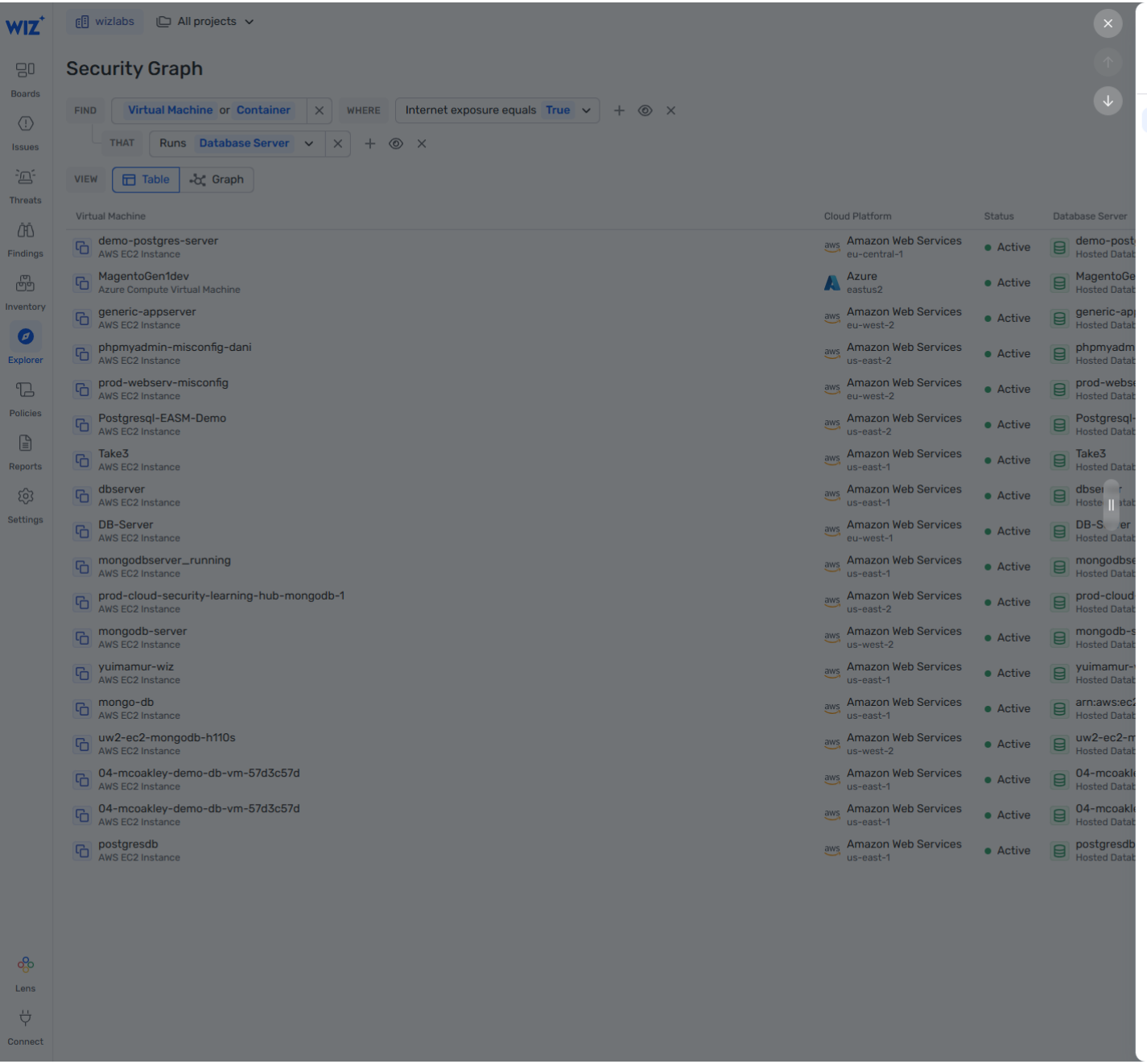
VIEW Table | Graph

18 results

Virtual Machine	Cloud Platform	Status	Database Server	Cloud Platform	Requires SSL
demo-postgres-server AWS EC2 Instance	Amazon Web Services eu-central-1	Active	demo-postgres-server Hosted Database Server	Amazon Web Services eu-central-1	-
MagentoGen1dev Azure Compute Virtual Machine	Azure eastus2	Active	MagentoGen1dev Hosted Database Server	Azure eastus2	-
generic-appserver AWS EC2 Instance	Amazon Web Services eu-west-2	Active	generic-appserver Hosted Database Server	Amazon Web Services eu-west-2	-
phpmyadmin-misconfig-dani AWS EC2 Instance	Amazon Web Services us-east-2	Active	phpmyadmin-misconfig-dani Hosted Database Server	Amazon Web Services us-east-2	-
prod-webserv-misconfig AWS EC2 Instance	Amazon Web Services eu-west-2	Active	prod-webserv-misconfig Hosted Database Server	Amazon Web Services eu-west-2	-
Postgresql-EASM-Demo AWS EC2 Instance	Amazon Web Services us-east-2	Active	Postgresql-EASM-Demo Hosted Database Server	Amazon Web Services us-east-2	-
Take3 AWS EC2 Instance	Amazon Web Services us-east-1	Active	Take3 Hosted Database Server	Amazon Web Services us-east-1	-
dbserver AWS EC2 Instance	Amazon Web Services us-east-1	Active	dbserver Hosted Database Server	Amazon Web Services us-east-1	-
DB-Server AWS EC2 Instance	Amazon Web Services eu-west-1	Active	DB-Server Hosted Database Server	Amazon Web Services eu-west-1	-
mongodbserver_running AWS EC2 Instance	Amazon Web Services us-east-1	Active	mongodbserver_running Hosted Database Server	Amazon Web Services us-east-1	-
prod-cloud-security-learning-hub-mongodb-1 AWS EC2 Instance	Amazon Web Services us-east-2	Active	prod-cloud-security-learning-hub-mongodb-1 Hosted Database Server	Amazon Web Services us-east-2	-
mongodb-server AWS EC2 Instance	Amazon Web Services us-west-2	Active	mongodb-server Hosted Database Server	Amazon Web Services us-west-2	-
yuimamur-wiz AWS EC2 Instance	Amazon Web Services us-east-1	Active	yuimamur-wiz Hosted Database Server	Amazon Web Services us-east-1	-
mongo-db AWS EC2 Instance	Amazon Web Services us-east-1	Active	arn:aws:ec2:us-east-1:783764577402:instance/i-0b93218b9956e5b6c Hosted Database Server	Amazon Web Services us-east-1	-
uw2-ec2-mongodb-h110s AWS EC2 Instance	Amazon Web Services us-west-2	Active	uw2-ec2-mongodb-h110s Hosted Database Server	Amazon Web Services us-west-2	-
04-mcoakley-demo-db-vm-57d3c57d AWS EC2 Instance	Amazon Web Services us-east-1	Active	04-mcoakley-demo-db-vm-57d3c57d Hosted Database Server	Amazon Web Services us-east-1	-
04-mcoakley-demo-db-vm-57d3c57d AWS EC2 Instance	Amazon Web Services us-east-1	Active	04-mcoakley-demo-db-vm-57d3c57d Hosted Database Server	Amazon Web Services us-east-1	-
postgresdb AWS EC2 Instance	Amazon Web Services us-east-1	Active	postgresdb Hosted Database Server	Amazon Web Services us-east-1	-



Boards | Issues | Threats | Findings | Inventory | Explorer | Policies | Reports | Settings | Lens | Connect



demo-postgres-server

AWS EC2 Instance

AWS | 0 Past Activities | JSON | Add note | Download SBOM | Support

- Overview
- Issues
- Forensics
- Response
- Activity
- Vulnerability
- Configuration
- Network
- Identity
- Secrets
- Kubernetes
- Application
- Data
- Comments

Overview

Insights Summary

2 high configuration findings | 11 critical & 78 high vulnerabilities | Unpatched OS | Running EOL Technologies

Validated Public Network Exposure

Properties

Tags

Name: demo-postgres-server

Name	demo-postgres-server	Provider ID	arn:aws:ec2:eu-central-1:984186218765:instance/i-062a08…
Subscription	WizDemo-1 984186218765	Project	5 Projects
Cloud Platform	Amazon Web Services eu-central-1	Status	Active
External ID	i-062a088b61cedc373	Native Type	EC2 Instance
Operating System	Linux	Creation Date	May 1, 2023 at 4:31 PM
Ephemeral	No	Managed	No
Container Host	No	Updated At	April 10, 2025 at 8:22 PM
Has Data Finding	No	Region Location	Germany
Wiz Sensor	Unsupported	Is AWS Marketplace Resource	Yes
Memory (GB)	4	vCPUs	2
Architecture	x86_64	Instance Type	t2.medium

First seen: Sep 28, 2023, 5:39 AM | Last changed: Apr 10, 2025, 8:22 PM | Last seen: Apr 14, 2025, 8:35 AM

Network Insights

Internet exposure	Yes	Wide internet exposure	Yes
Accessible from other subscriptions	No	Accessible from other VNets	Yes
Accessible from VPN	No	Addresses Open For SSH	4,294,967,295
Addresses Open To Internet	4,294,967,295	Addresses Open To Other Vnets	65,536
Ports Open To Other Vnets	1	Ports Open To Internet	1
Validated Open Ports	22		

Identity Insights

Has High Privileges	No	Has Admin Privileges	No
Has Access To Sensitive Data	No		

Technologies

View All

Linux CentOS 7.9.2009	OpenSSL 1.0.2k	PostgreSQL 11.19	Linux 3.10.0-1160.88.1.el7

wizlabs | All projects

Search CTRL K

Security Graph

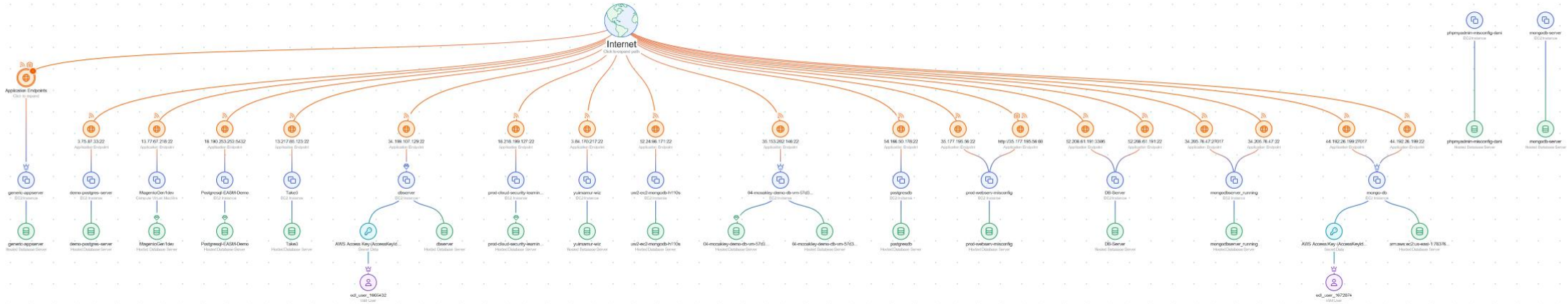
New Search | Save as...

FIND Virtual Machine or Container | WHERE Internet exposure equals True

THAT Runs Database Server

18 results

VIEW Table | Graph



18 out of 18 results

Boards | Issues | Threats | Findings | Inventory | Explorer | Policies | Reports | Settings | Lens | Connect

Security Graph

New Search | Save as...

FIND Finding

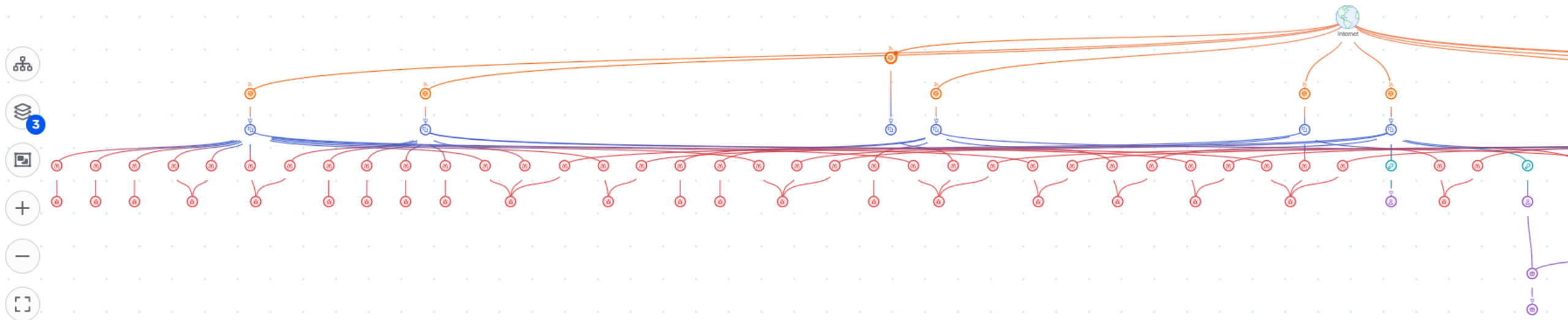
10,000+ results

THAT Is caused by Vulnerability WHERE Severity equals Critical or High

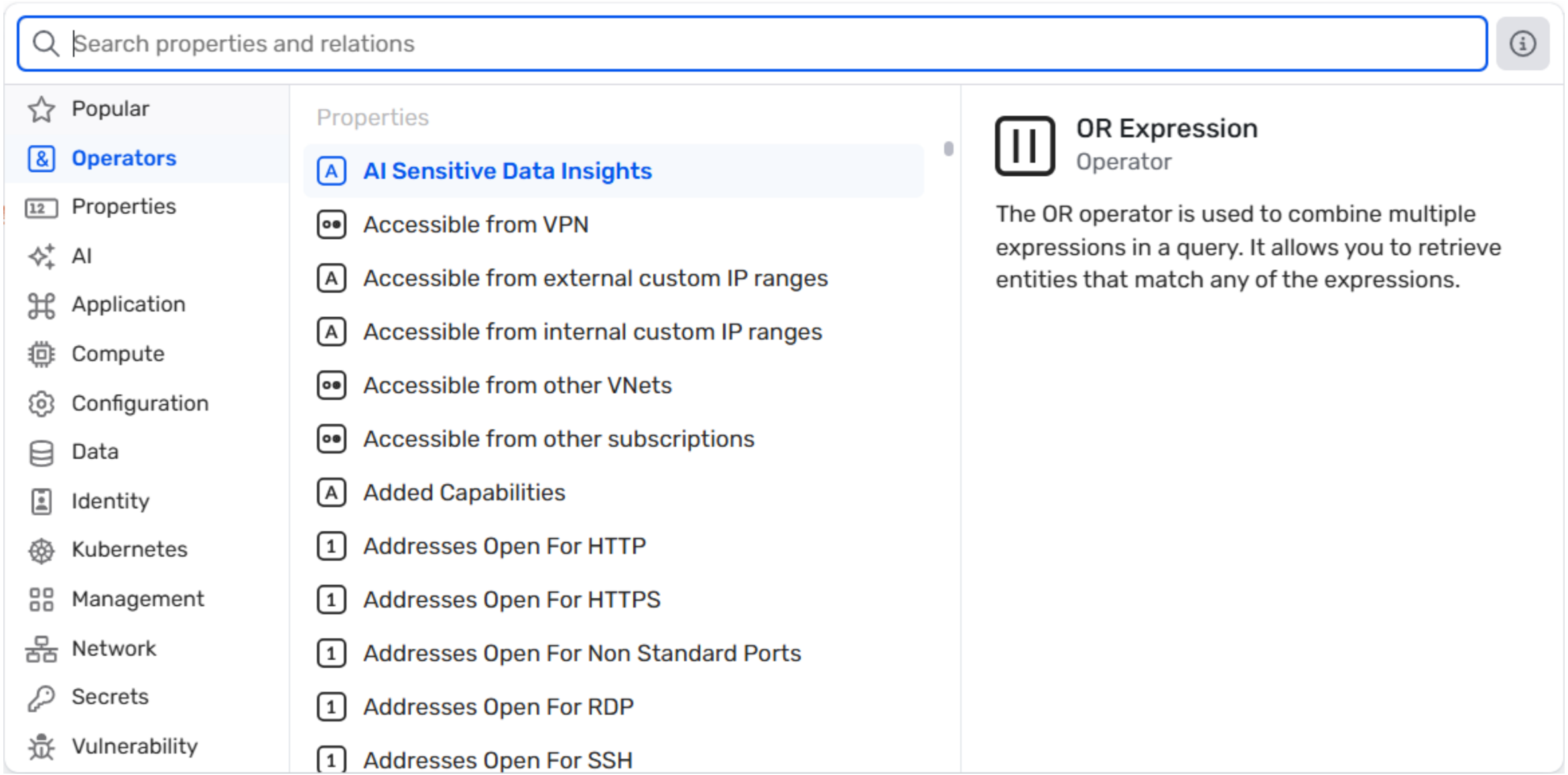
THAT Alerted on Container or Virtual Machine WHERE Internet exposure equals True

Has High Privileges equals True

VIEW Table | Graph



WIZ

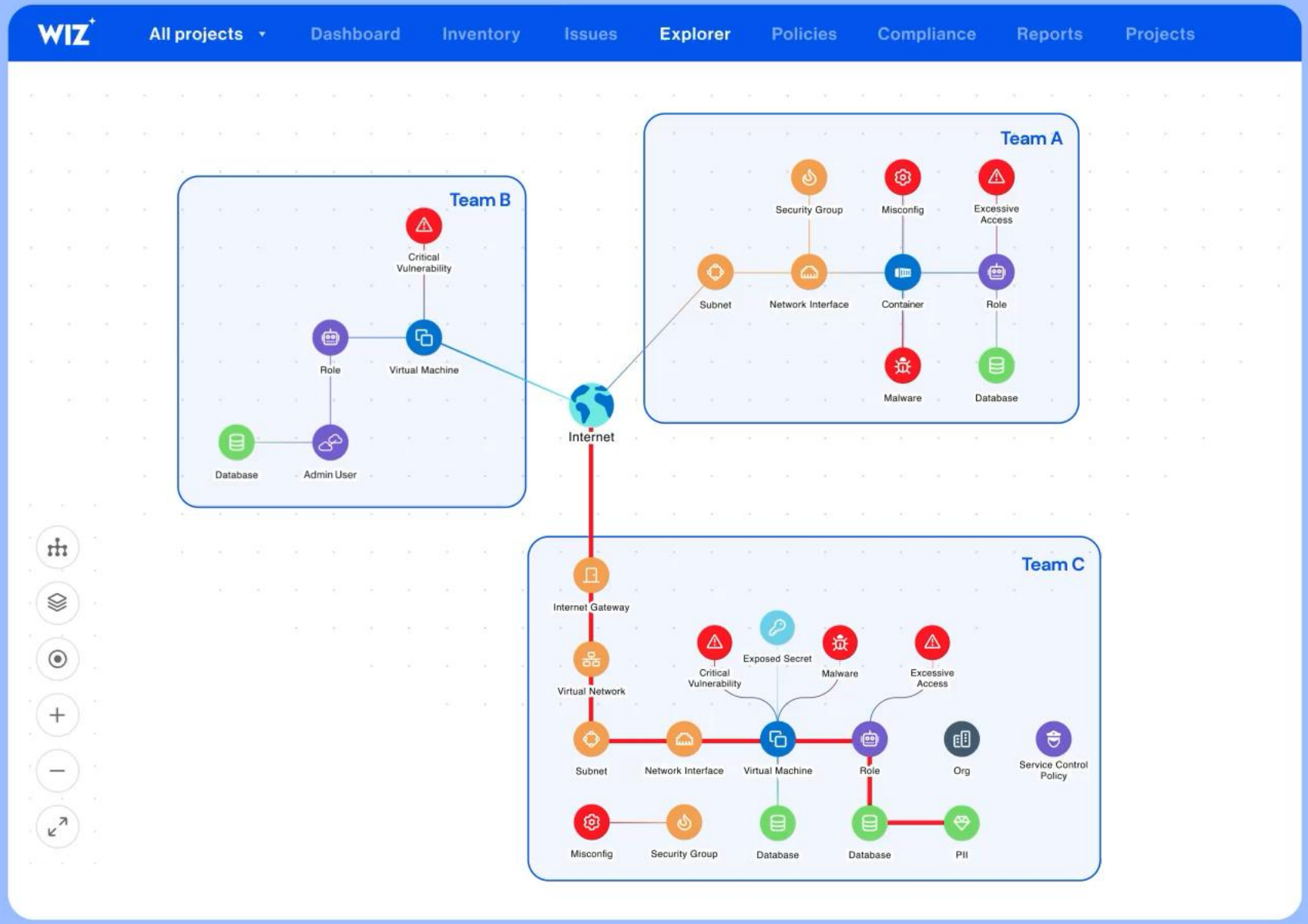

Search properties and relations
Popular
Operators
Properties
AI
Application
Compute
Configuration
Data
Identity
Kubernetes
Management
Network
Secrets
Vulnerability
Properties
AI Sensitive Data Insights
Accessible from VPN
Accessible from external custom IP ranges
Accessible from internal custom IP ranges
Accessible from other VNets
Accessible from other subscriptions
Added Capabilities
Addresses Open For HTTP
Addresses Open For HTTPS
Addresses Open For Non Standard Ports
Addresses Open For RDP
Addresses Open For SSH
OR Expression
Operator
The OR operator is used to combine multiple expressions in a query. It allows you to retrieve entities that match any of the expressions.

The cloud security operating platform

Determine ownership

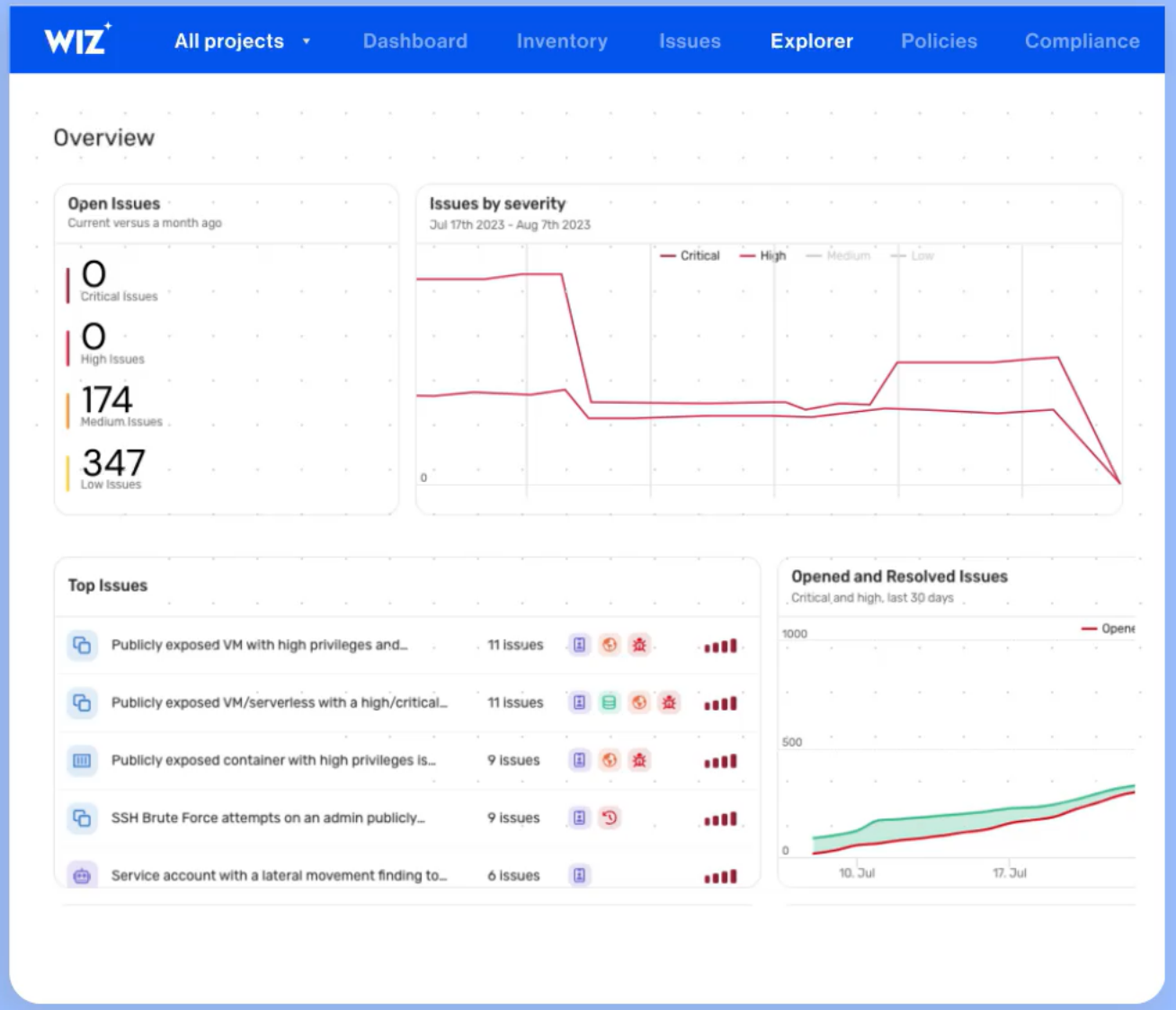
The cloud security operating platform

Automate workflows to speed remediation



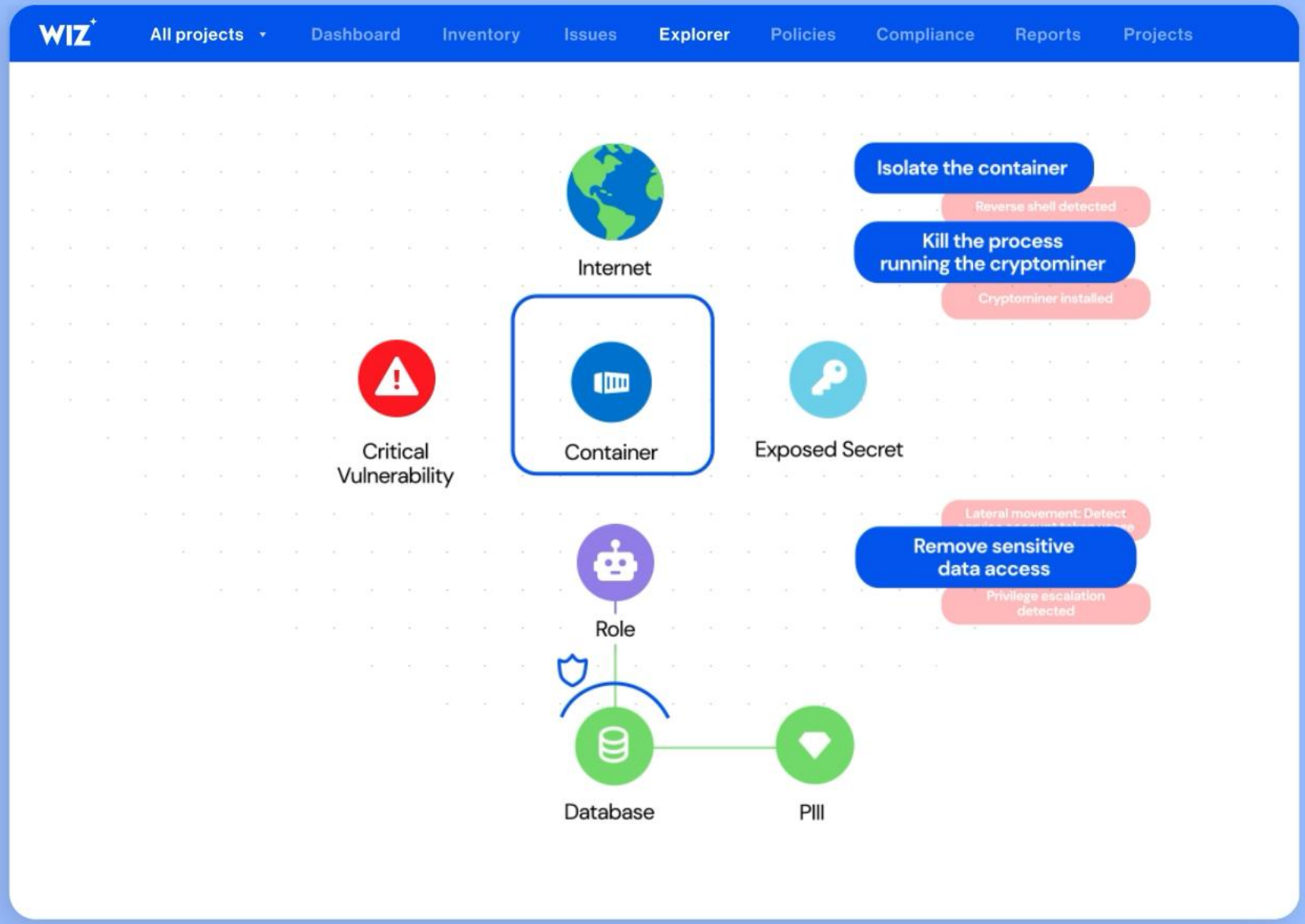
The cloud security operating platform

Build securely by design



The cloud security operating platform

Respond to unfolding cloud attacks in real-time



The Cloud Security Flywheel

A cloud security operating model that breaks the siloes between your cloud builders and defenders for defense-in-depth

AISHIELD

SEVCO SECURITY

Democratization to Business Units' teams

Root cause analysis and enforcement in code

Wiz Code

Same scanners, same policy framework across the SDLC

Build securely by design with Guardrails

Protect the supply chain

Continuous hardening in the SDLC

Comprehensive risk assessment and attack path analysis

Cloud API scans

Kubernetes API scans

Volume scans

Registry scans

Serverless scans

Data scans

Cloud Audit Logs

Kubernetes Logs

Wiz Runtime Sensor

3rd Party (EDRs, GuardDuty, Defender)

Wiz Security Graph

Enrich events with cloud context for threat detection

Wiz Cloud

Complete visibility + inventory

High-fidelity risk alerts

Remediation flows

Contextual remediation guidance

Automation

Dev Team A

Dev Team B

AI Team C

Cloud Context

INTEZER

Wiz Defend

High-fidelity threat alerts

Response flows

Investigation flows

Forensics+ evidence collection

Centralized SIEM/SOAR

Cyber Defense Team

Root cause analysis and enforcement in code

WIZ

AISHIELD

你遲早要WIZ的，何不現在就開始用WIZ

剛準備上雲：從初期建立良好的雲端治理框架

已經上雲的：檢視你現有的解決方案並增強
(Inspector, Security Hub, Macie, Config, GuardDuty, Audit Manager, IAM Access Analyzer)

左移科技提前防堵風險

化解資安與開發衝突，提升效率與安全品質

WIZ

AISHIELD

請參與艾盾資科品牌日下一場議程

了解更多與WIZ的加值整合

INTEZER

C122

SEVCO SECURITY

WIZ