WIZ

From CSPM to CNAPP: Defining a new operating model for cloud security

Yinon Costica
Co-Founder and VP Product
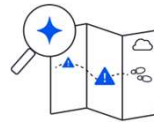
July 2023

Cloud changes everything

New environment

New risks

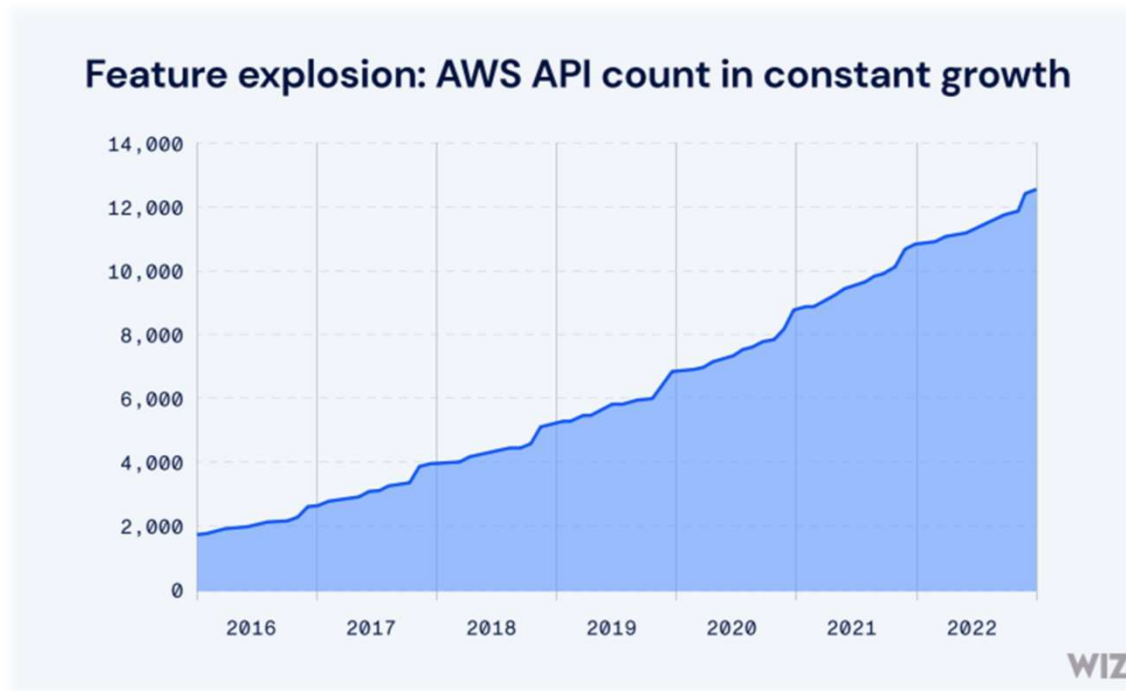**New ownership model**

How do I get visibility into my environment?

How do I prioritize the real risks and eliminate the noise?

How do I ingrain security into our teams?

wiz

Agility introduces more attack surface
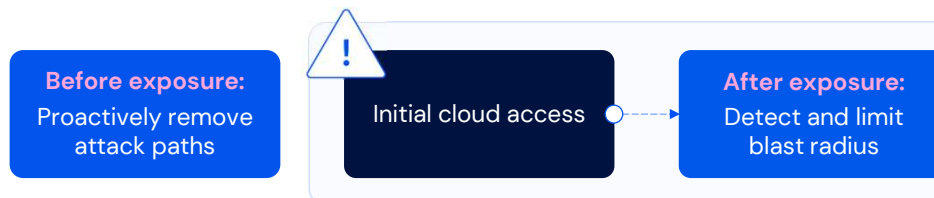

Feature explosion: AWS API count in constant growth

Multiple clouds, multiple architectures, multiple technologies

Cloud–native applications introduce unique attack vectors that are challenging to identify before and after exposure

Attack path

Initial cloud access	→	Lateral movement	→	Crown jewels

The Hacker News

#1 Trusted Cybersecurity News Platform   Followed by 3.45+ million

Home   Data Breaches   Cyber Attacks   Vulnerabilities   Webinars   Store   Contact

Cryptojacking Group TeamTNT Suspected of Using Decoy Miner to Conceal Data Exfiltration

Security Goals

Before exposure: Proactively remove attack paths

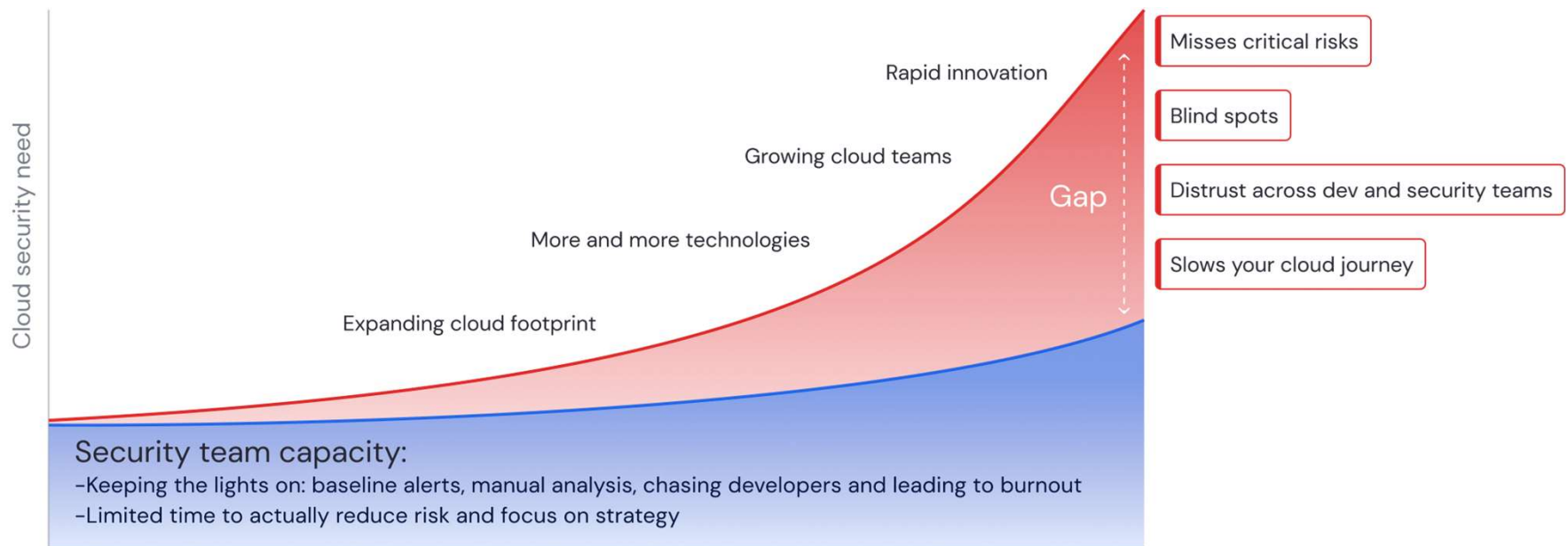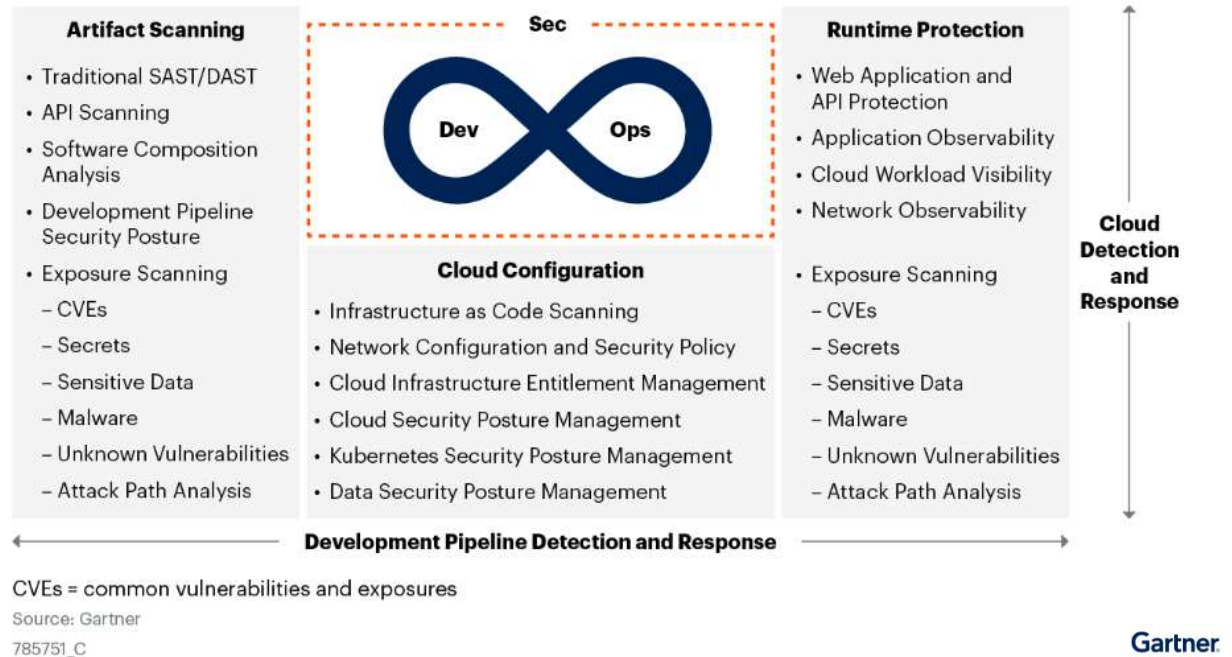| Initial cloud access	→	**After exposure:** Detect and limit blast radius

Cloud

Orchestration

Container

WIZ

We can't keep doing the same thing, it's time to scale

Introducing CNAPP:
The Cloud Native Application Protection Platform

"CNAPPs address **the full life cycle protection requirements of cloud-native applications from development to production**. Security and risk management leaders responsible for cloud security strategies should use this research to analyze and evaluate emerging CNAPP offerings".[1]

CNAPP Detailed View

Artifact Scanning	Cloud Configuration	Runtime Protection

• Traditional SAST/DAST
• API Scanning
• Software Composition Analysis
• Development Pipeline Security Posture
• Exposure Scanning
  – CVEs
  – Secrets
  – Sensitive Data
  – Malware
  – Unknown Vulnerabilities
  – Attack Path Analysis
	Sec
	Dev ∞ Ops
	
	• 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
		• Web Application and API Protection
		• Application Observability
		• Cloud Workload Visibility
		• Network Observability
		
		• Exposure Scanning
		  – CVEs
		  – Secrets
		  – Sensitive Data
		  – Malware
		  – Unknown Vulnerabilities
		  – Attack Path Analysis

Cloud Detection and Response

← Development Pipeline Detection and Response →

CVEs = common vulnerabilities and exposures
Source: Gartner
785751_C

Gartner

[1]. Gartner, Market Guide for Cloud-Native Application Protection Platforms, Neil MacDonald, Charlie Winckless, Dale Koeppen, 14 March 2023.

One unified platform for many cloud security use cases

Cloud Native Application Protection Platform

CSPM	Vulnerability Management	Container Security
CIEM	CWPP	Cloud Detection & Response
Data Security	IaC Scanning	Compliance Reporting
Image & Registry Scanning	Secrets Scanning	Malware Scanning

CNAPP drives massive tool consolidation

By 2026, 80% of enterprises will have consolidated security tooling for the life cycle protection of cloud-native applications to three or fewer vendors, down from an average of 10 in 2022 (Gartner*)

Gartner, Market Guide for Cloud-Native Application Protection Platforms, Neil MacDonald, Charlie Winckless, Dale Koeppen, 14 March 2023.

The cloud security operating platform
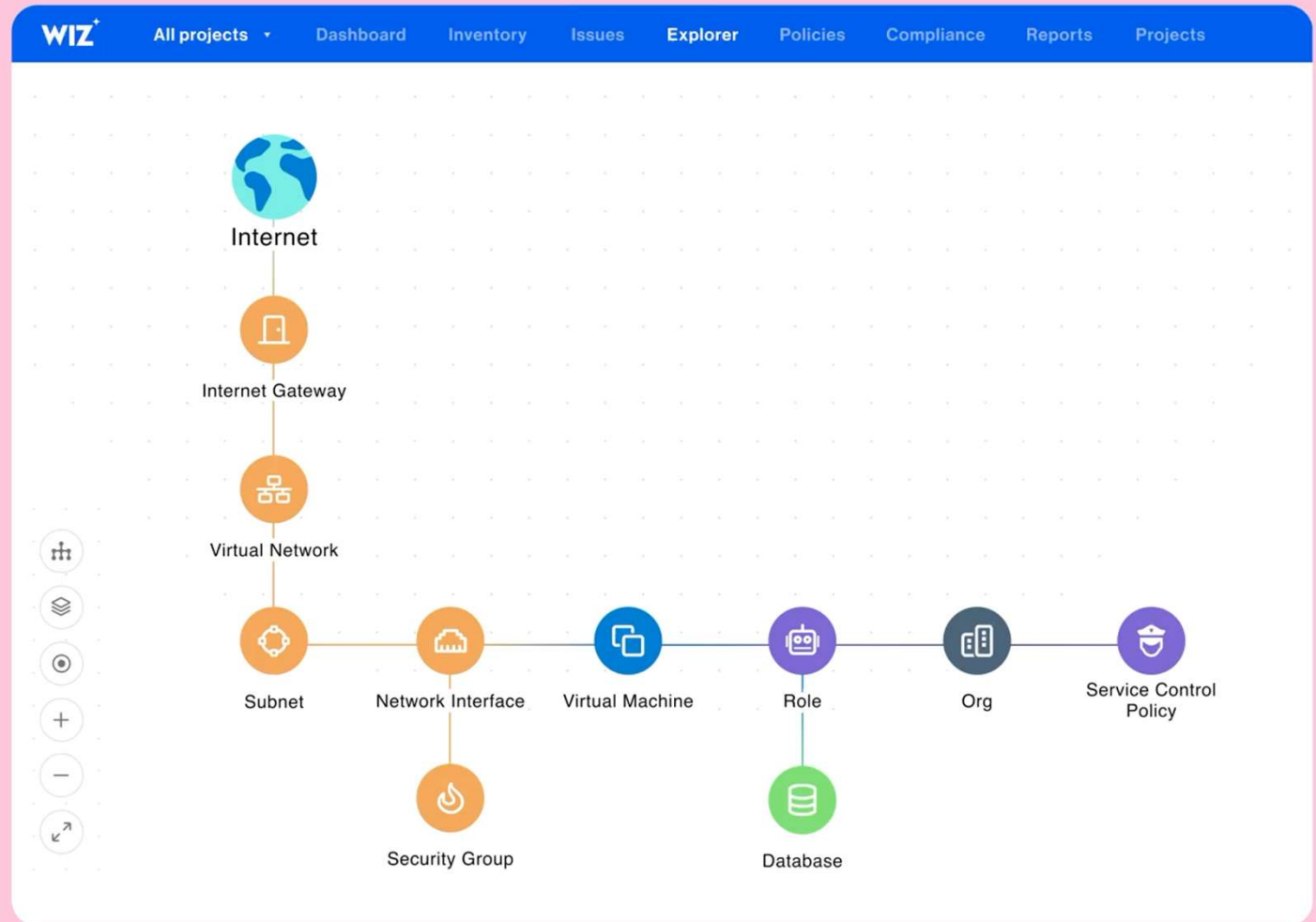
Scan your cloud without agents and build the graph

- Serverless
- Containers
- VMs
- PaaS

The cloud security operating platform

Identify risks

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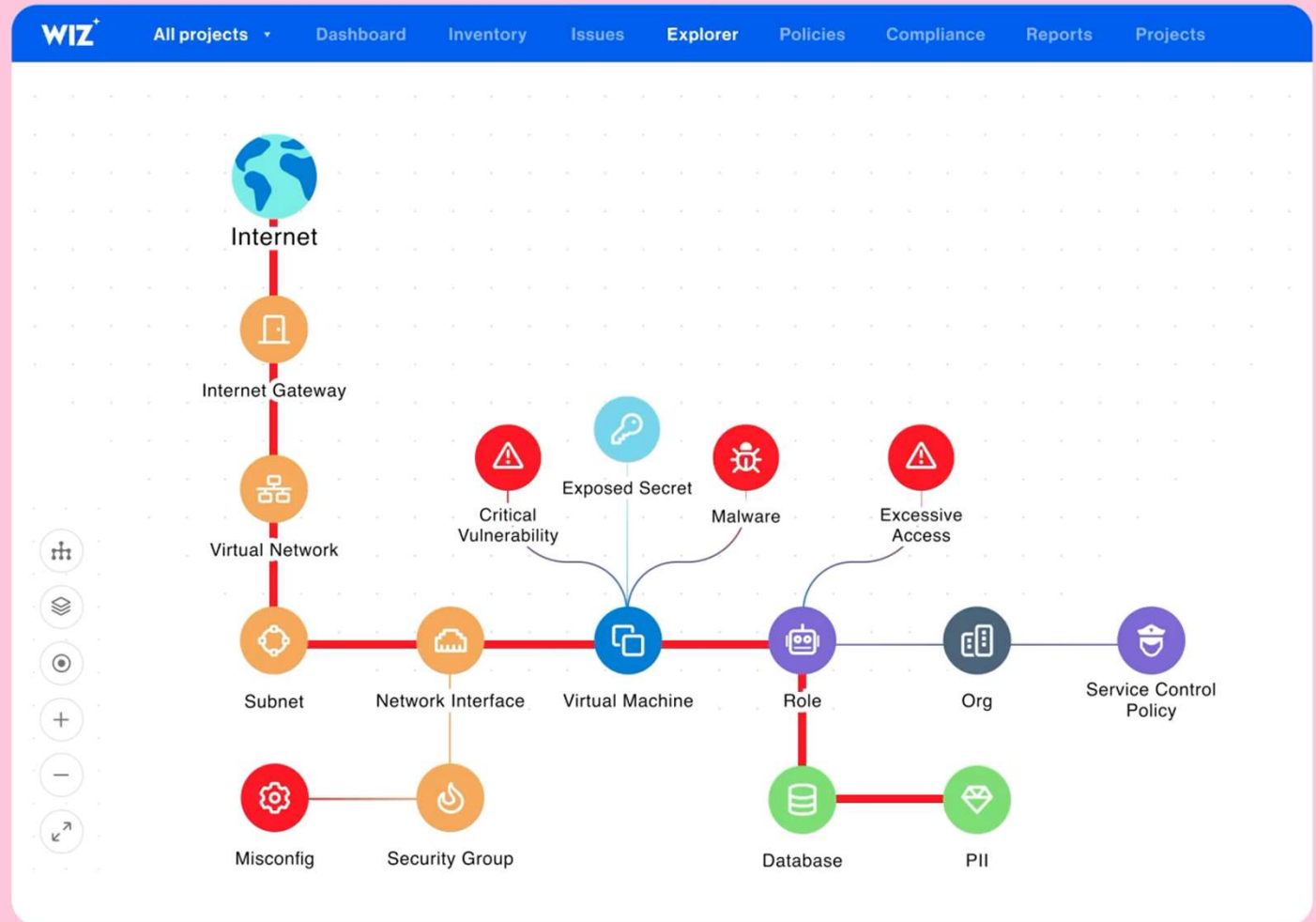- Business impact

The cloud security operating platform
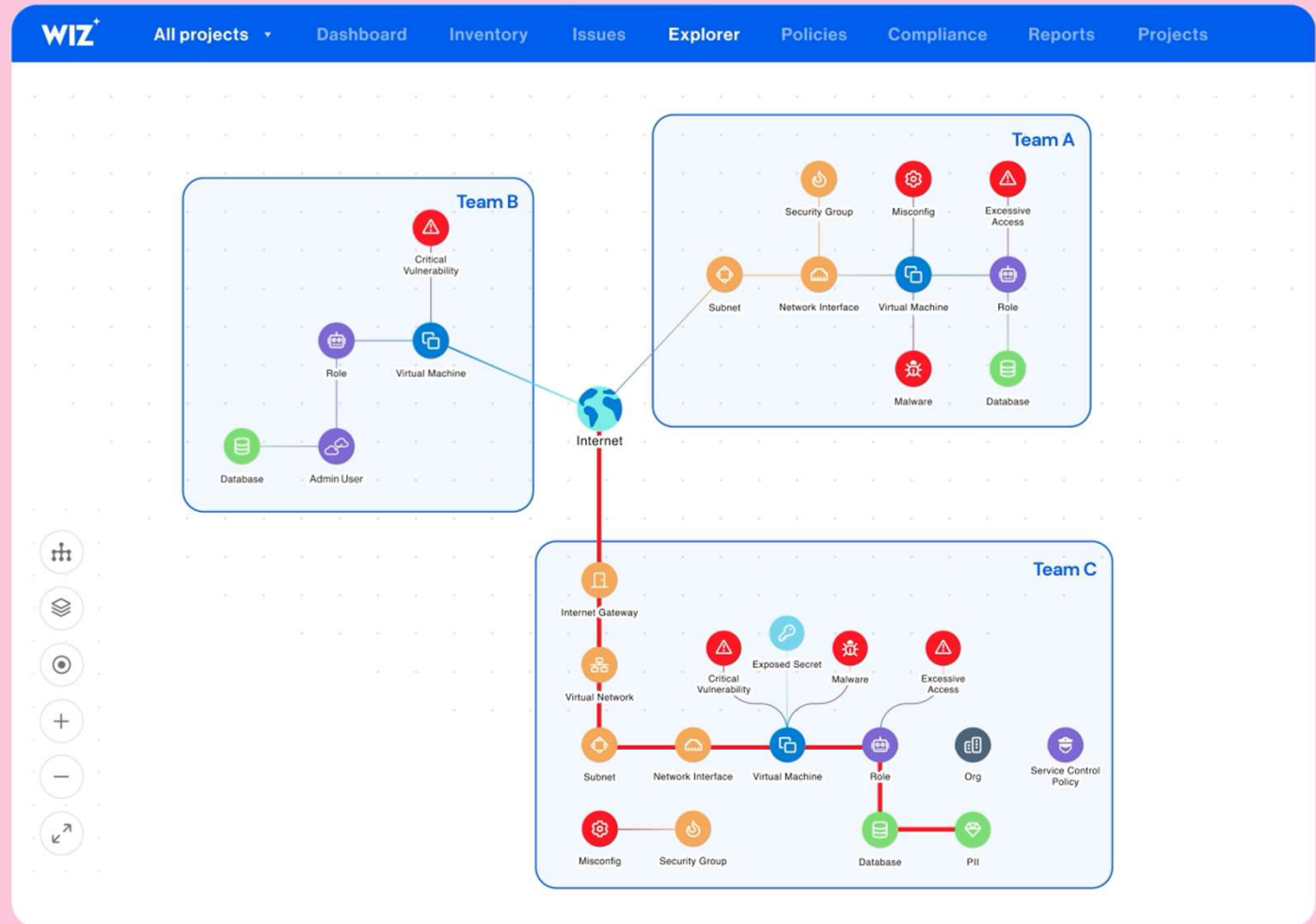
Prioritize attack paths
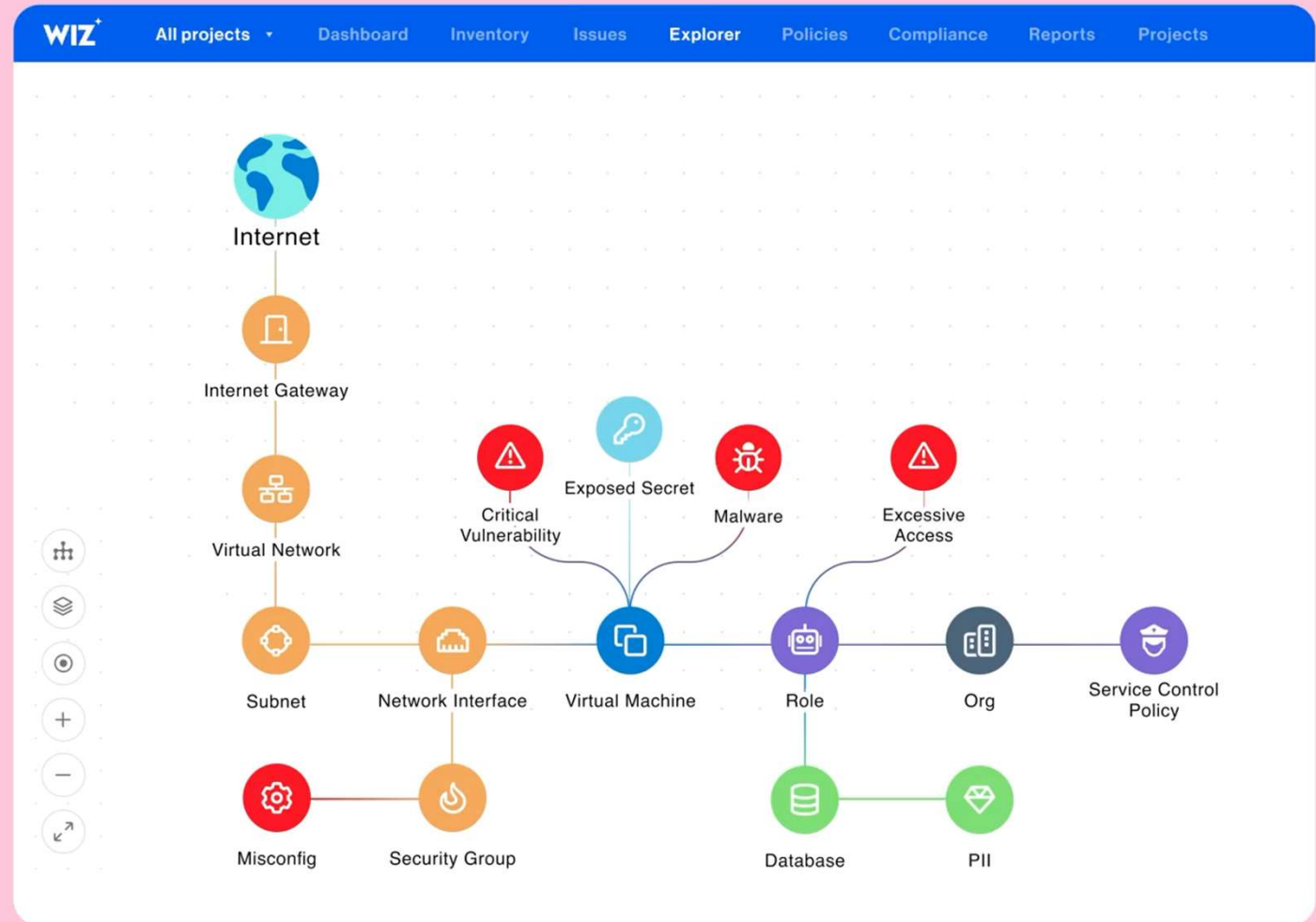
The cloud security operating platform
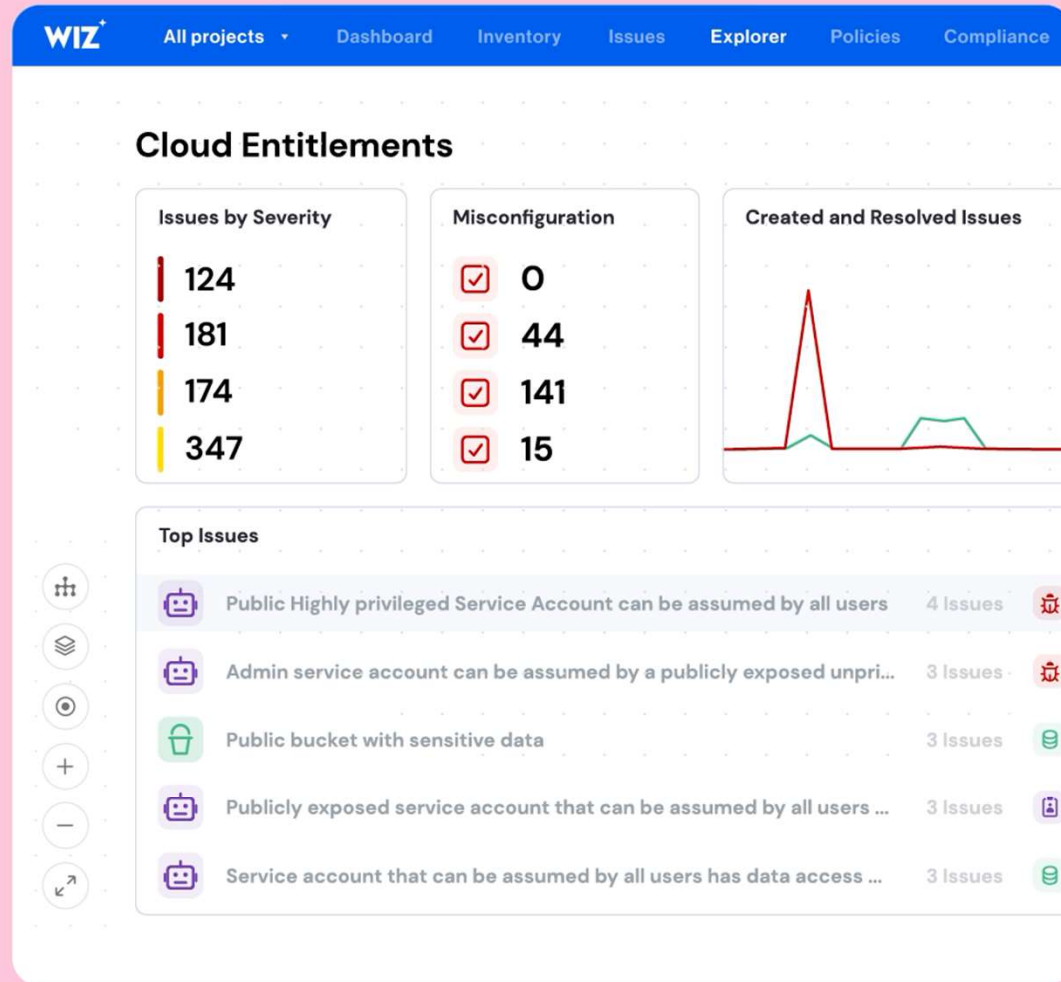
Determine ownership

The cloud security operating platform

Automate workflows to speed remediation

The cloud security operating platform
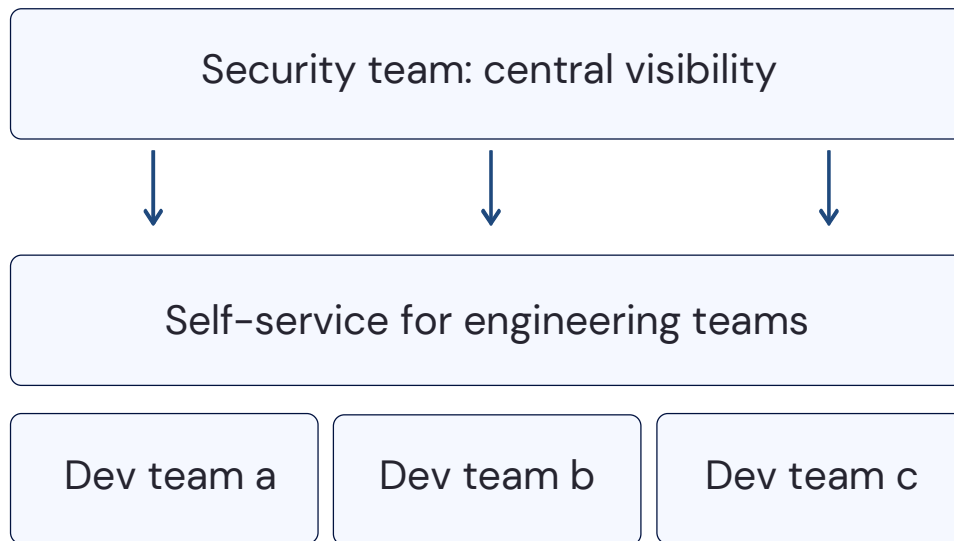
Shift left prevention

Cloud security is a team sport

Security team: central visibility

↓   ↓   ↓

Self-service for engineering teams

Dev team a	Dev team b	Dev team c

FOX

"Wiz allows us to achieve our philosophy of how to democratize security – scaling the cybersecurity team's reach through technology."

Melody Hildebrandt
CISO,
FOX Corp

Read more on https://wiz.io/customers

How CNAPPs simplify cloud security

New environment

Unconditional visibility

Gain full visibility, without bothering anyone

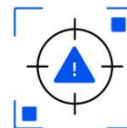### Security baselines

Best practices are shared knowledge and available OOTB

New risks

Single policy

across the development lifecycle, clouds and architectures

Context matters

Identify toxic combinations across layers and scanners

New ownership model

Focus like a dev

Prioritize ruthlessly based on the risk to the business

Dev power

Democratize security and empower developers to remediate

WIZ

The network effect:
Out-of-the-box security baselines

|		
2,000+ Cloud configuration rules	**3,000+** Inventoried technologies	**10,000+** Host configuration rules
130+ Mapped compliance standards	**800+** Cloud event rules	**80,000+** Vulnerabilities
100+ High-profile threat advisories	**700+** Attack paths detections	**100+** Partner integrations

WIZ

Practical steps to safely transform to a cloud–first organization

Driving CNAPP to consolidate stack across security teams
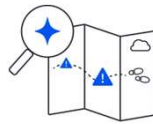
Nurture a risk–based approach to prioritize risks for remediation

Democratize security to your development teams – make it a team sport

WIZ

Organizations need a defense in depth strategy that starts with prevention and includes active detection and response as a last line of defense

Prevent

Harden from code-time: scan in the CI/CD pipeline

Harden in production: scan the cloud environment

Harden the software: scan workloads

Detect

Monitor in real-time: cloud events monitoring

Detect in runtime: real-time threat detection with sensor

Respond

Protect in real-time: Respond in real-time at scale during breaches

WIZ

Introducing the Wiz Runtime Sensor: Unified cloud security from prevention to real-time detection and response
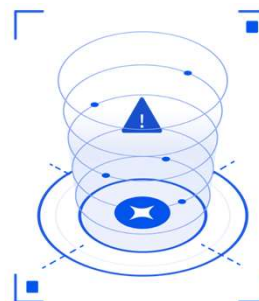
Prevention

Agentless visibility & risk prioritization that proactively reduces the attack surface

Real-time detection and response

Lightweight eBPF-based sensor to protect workloads from unfolding threats as a last line of defense

WIZ

How critical is this suspicious activity?

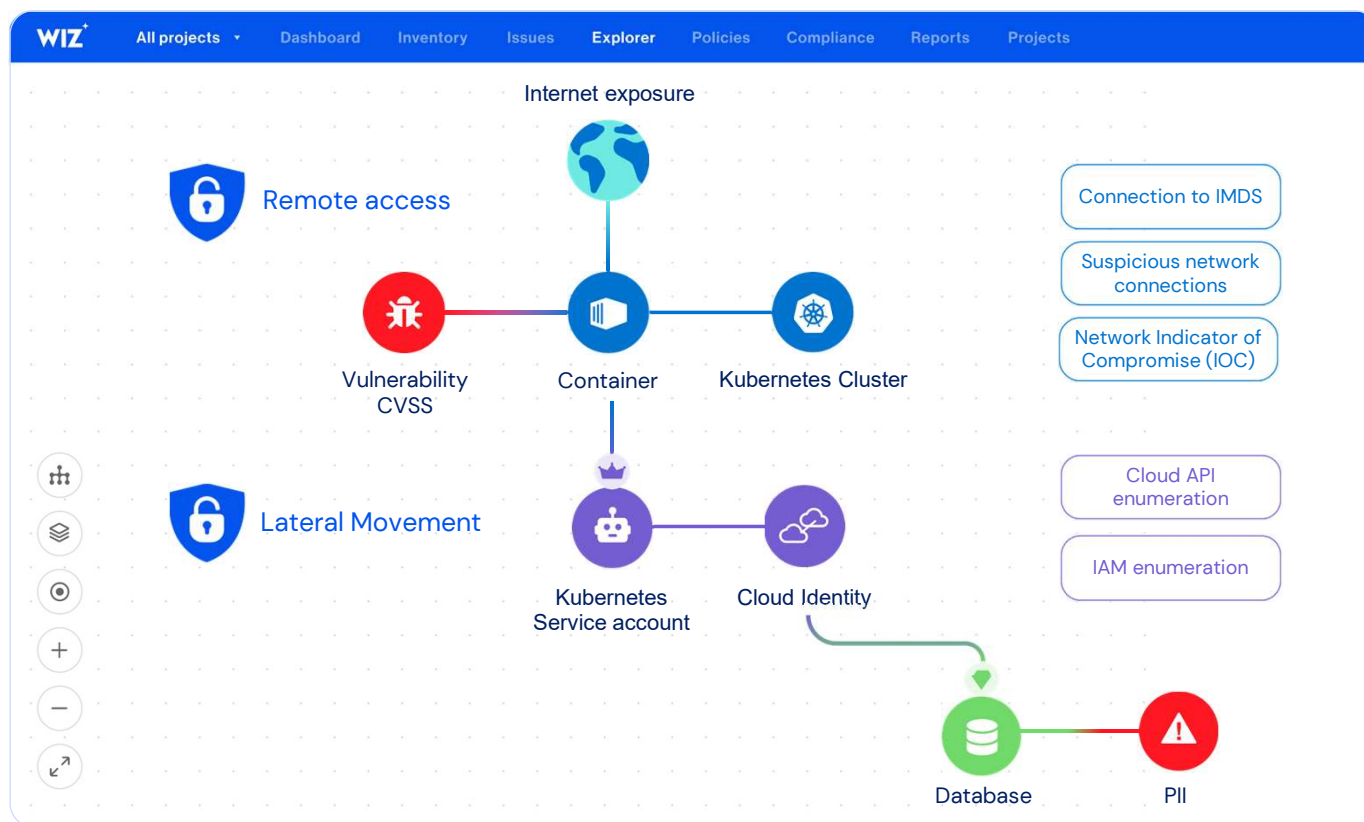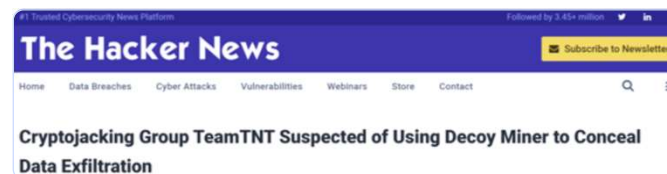## 01 Real time sensor detection

- Unknown and known threats
- Network activity
- Malicious behavior

02 Cloud activity and audit logs

- Configuration changes
- Suspicious events
- Identity activity

03 Agentless risk context

- Cloud and workload context
- Attack path analysis
- Potential blast radius

The Hacker News

Cryptojacking Group TeamTNT Suspected of Using Decoy Miner to Conceal Data Exfiltration

WIZ | All projects | Dashboard | Inventory | Issues | **Explorer** | Policies | Compliance | Reports | Projects

Internet exposure

Remote access

Vulnerability CVSS | Container | Kubernetes Cluster

Connection to IMDS

Suspicious network connections

Network Indicator of Compromise (IOC)

Lateral Movement

Kubernetes Service account | Cloud Identity

Cloud API enumeration

IAM enumeration

Database | PII

PyLoose: Python-based fileless malware targets cloud workloads to deliver cryptominer

PyLoose is a newly discovered Python-based fileless malware targeting cloud workloads. Get a breakdown of how the attack unfolds and the steps to mitigate it.

Avigayil Mechtinger, Oren Ofer, Itamar Gilad

July 11, 2023

6 min read
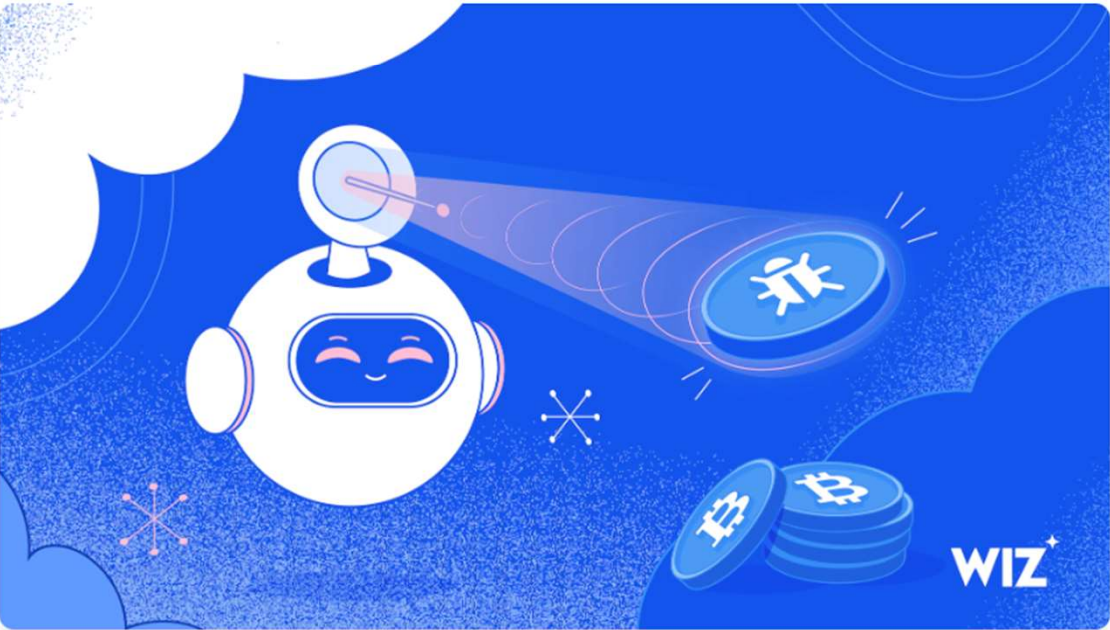
Fileless execution was detected

{} Raw Event Details   ⊕ Share Feedback   🔗 Share Link

Overview   Investigate

Process image path resolved to memfd or shared memory (shm). Memfd (memory file descriptor) and shm (shared memory) are interprocess communication mechanisms in Linux where memfd allows for the creation of anonymous memory objects that can be shared between processes using file descriptors, while shm enables the creation of shared memory segments that allow multiple processes to access and exchange data efficiently in a fast and synchronized manner. This could indicate the presence of a threat actor achieving fileless execution.

Event Properties

External Name		Event Time	
Cloud Platform	🔷 Kubernetes	Category	Detection
Path	/memfd: (deleted)	Hash	eba82ed21b329b0955ab87b2397a949628349b3f
MITRE Tactics	Defense Evasion	MITRE Techniques	Reflective Code Loading
Severity	■■		

Process Tree

Virtual Machine

Container

Process

Process
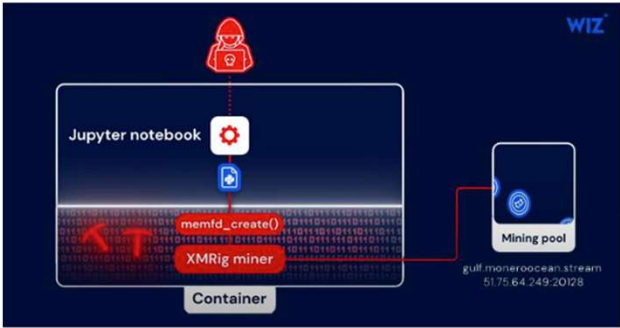
Process

Process

The Hacker News
468,600 followers
13h · 🌐

✓ Following   · · ·

A sophisticated threat actor has been employing a new Python-based fileless attack called PyLoose to mine #cryptocurrency on cloud workloads, bypassing traditional detection methods.
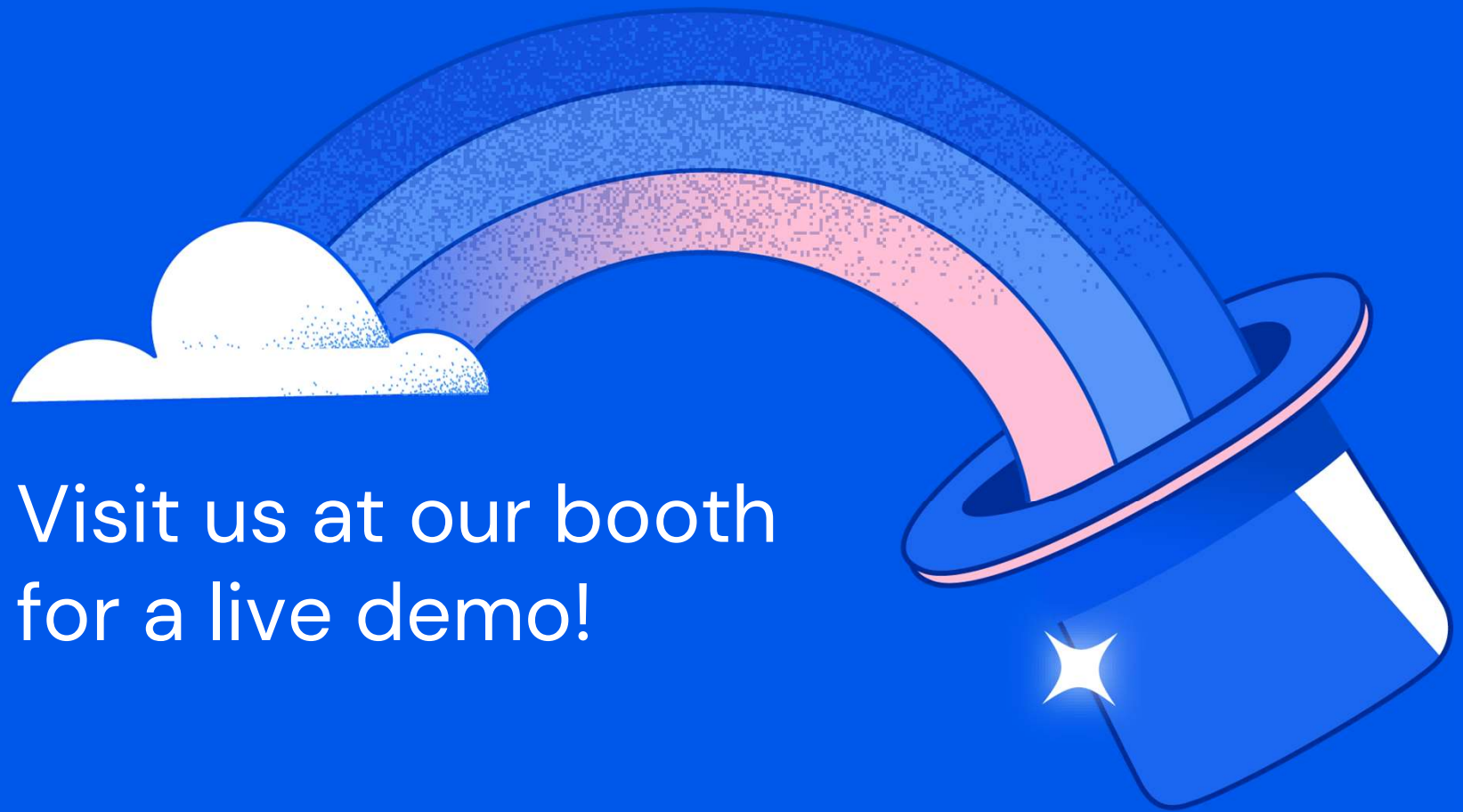
Read details: https://lnkd.in/dy96fT6a

#cybersecurity #malware #informationsecurity

Python-Based PyLoose Fileless Attack Targets Cloud Workloads for Cryptocurrency Mining

thehackernews.com · 2 min read

Visit us at our booth for a live demo!