WIZ

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

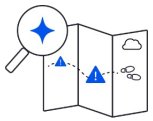
Bryan McClellan
Principal Sales Engineer

Aug 2023

Cloud changes everything

New environment

How do I get visibility into my environment?



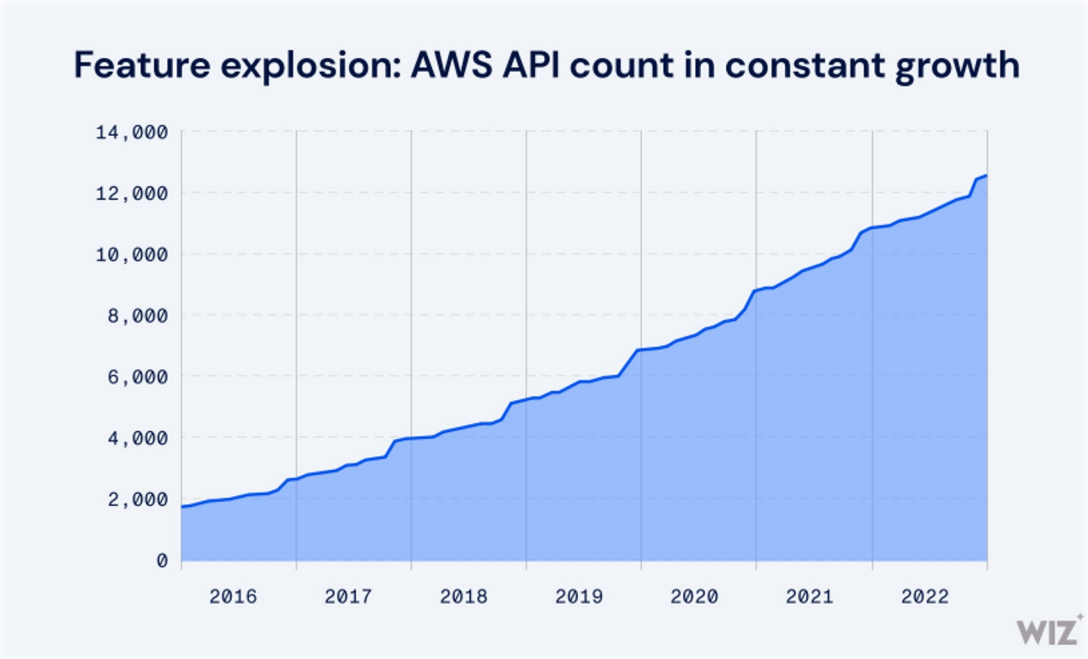
New risks

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

New ownership model

How do I ingrain security into our teams?

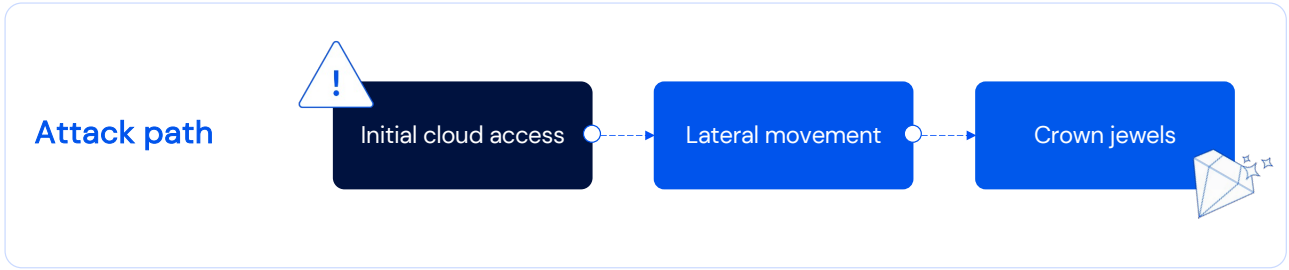
Agility introduces more attack surface

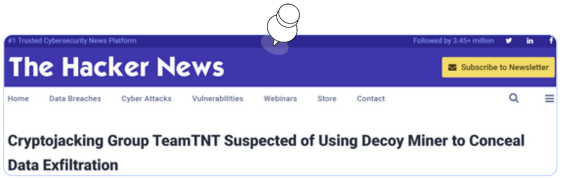


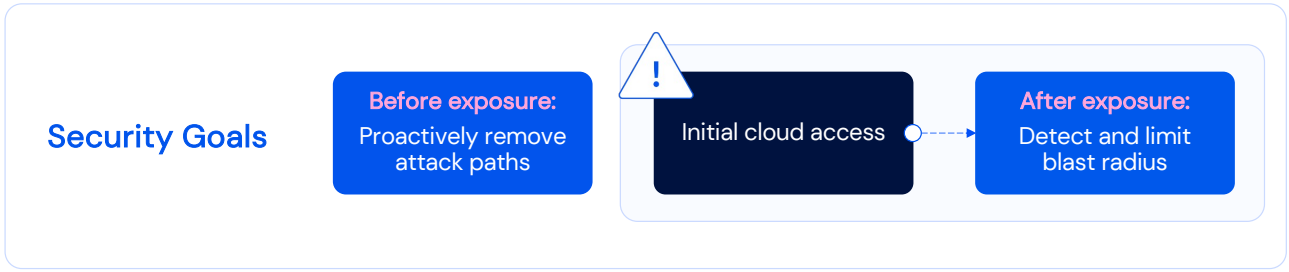
Multiple clouds, multiple architectures, multiple technologies

WIZ

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

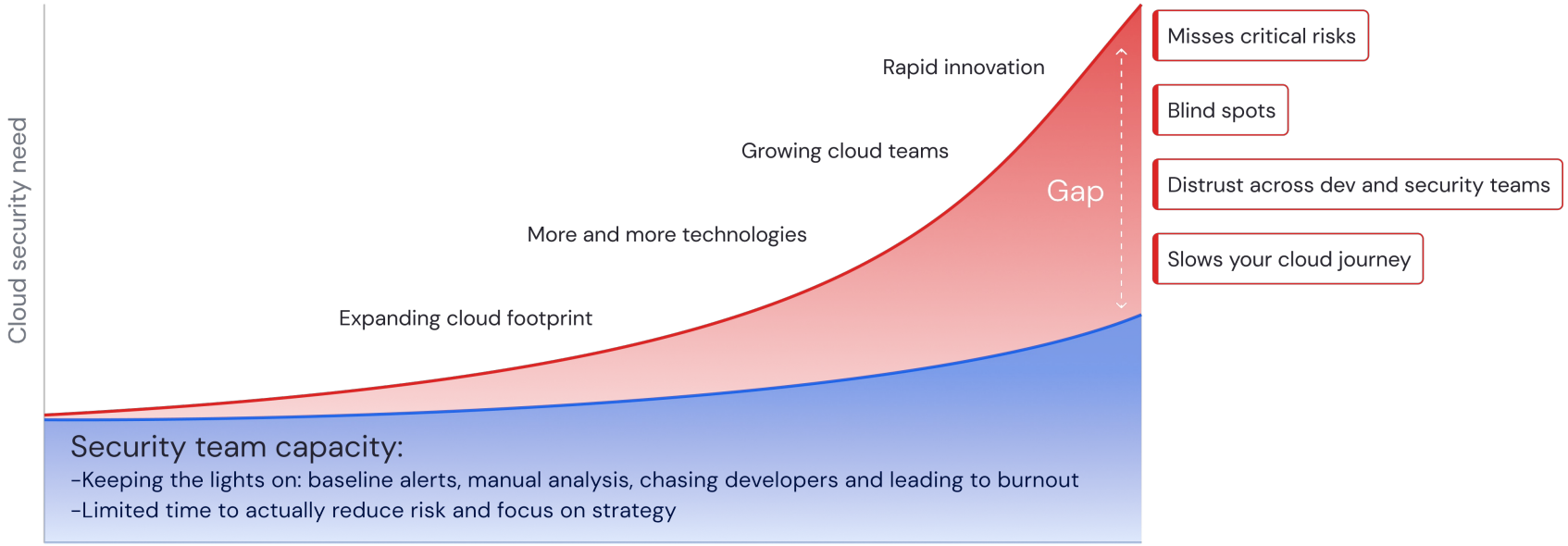






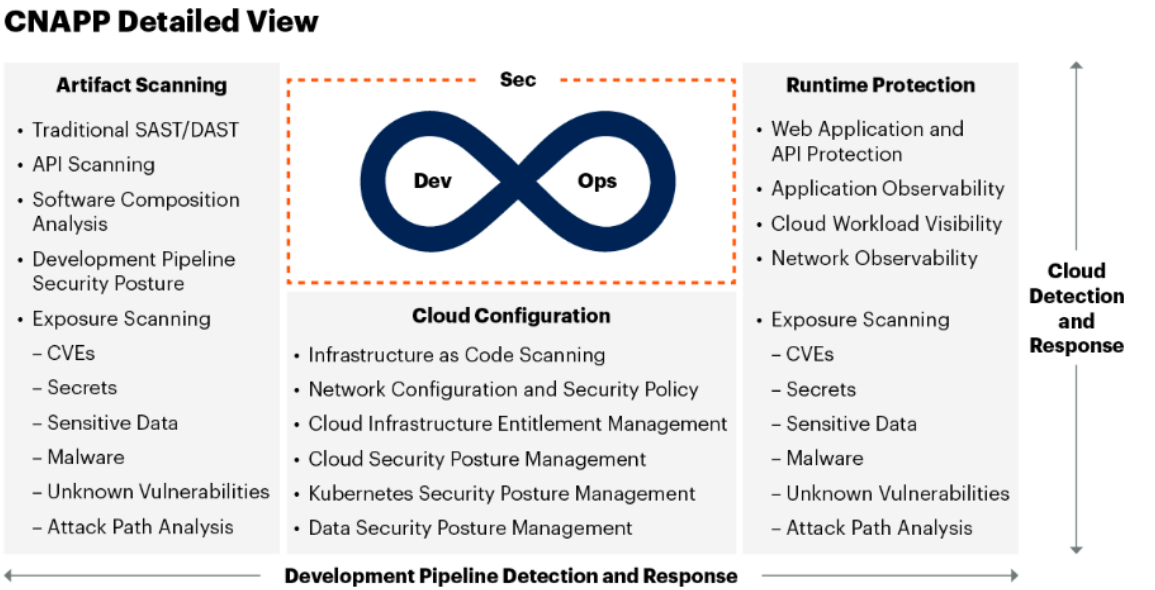
WIZ

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



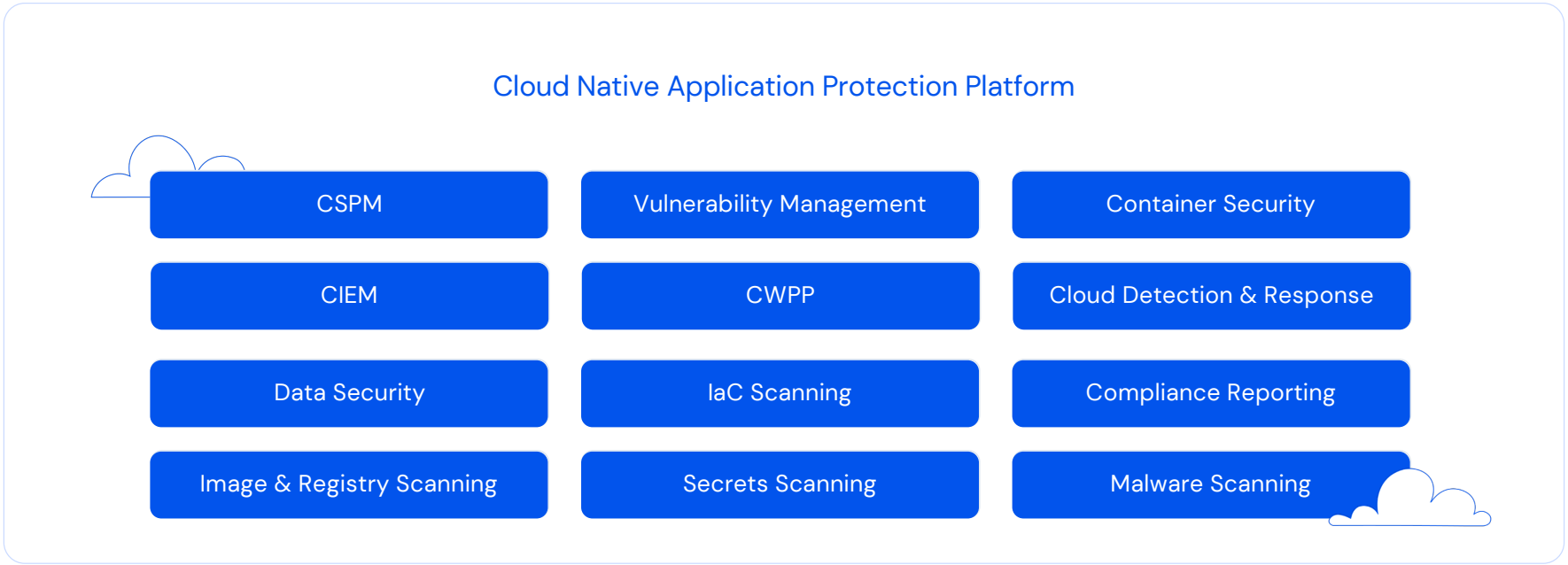
Introducing CNAPP:
The Cloud Native Application Protection Platform

"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]



[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



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

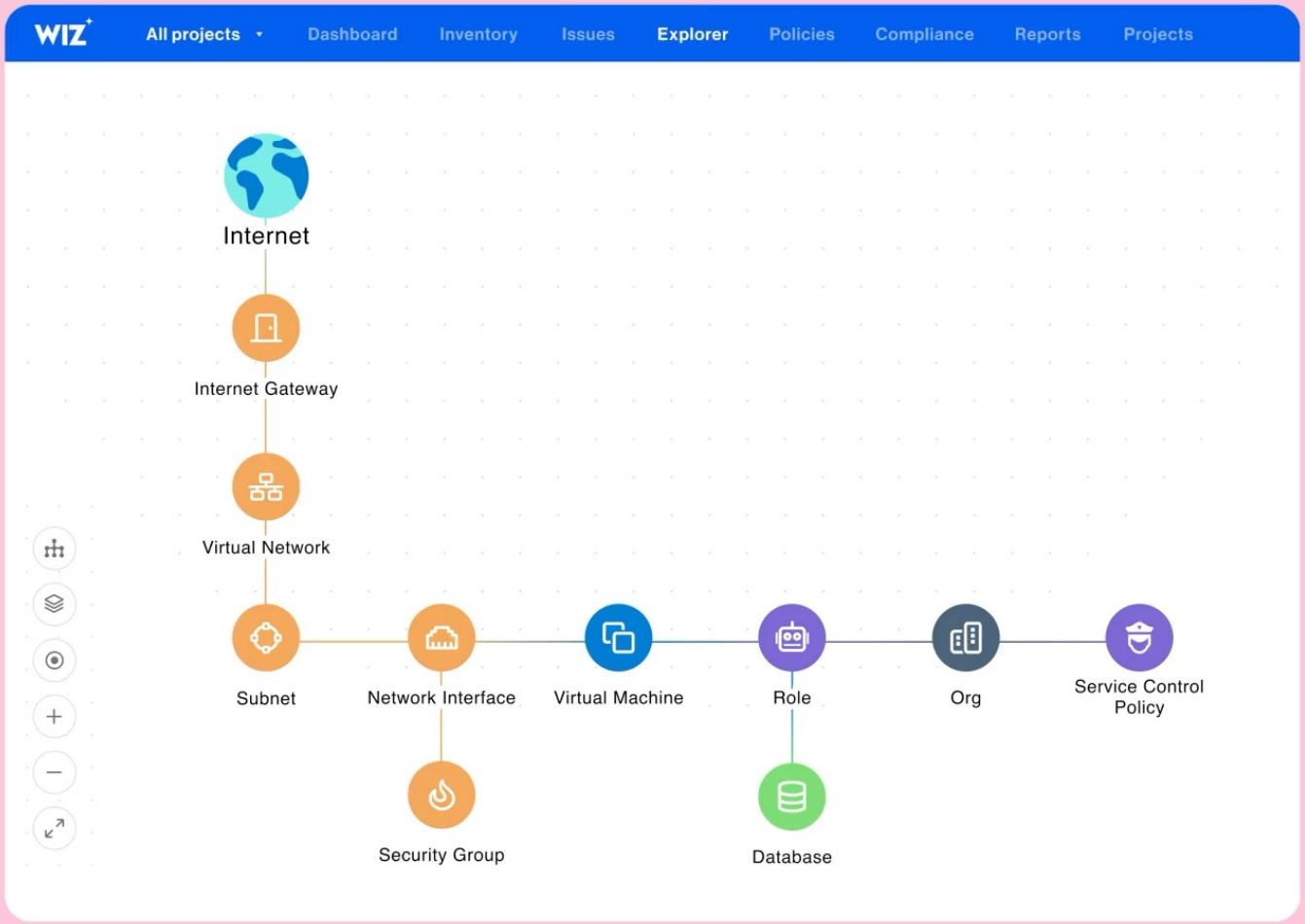
Scan your cloud without agents and build the graph

- Serverless
- Containers
- VMs
- PaaS

The cloud security operating platform

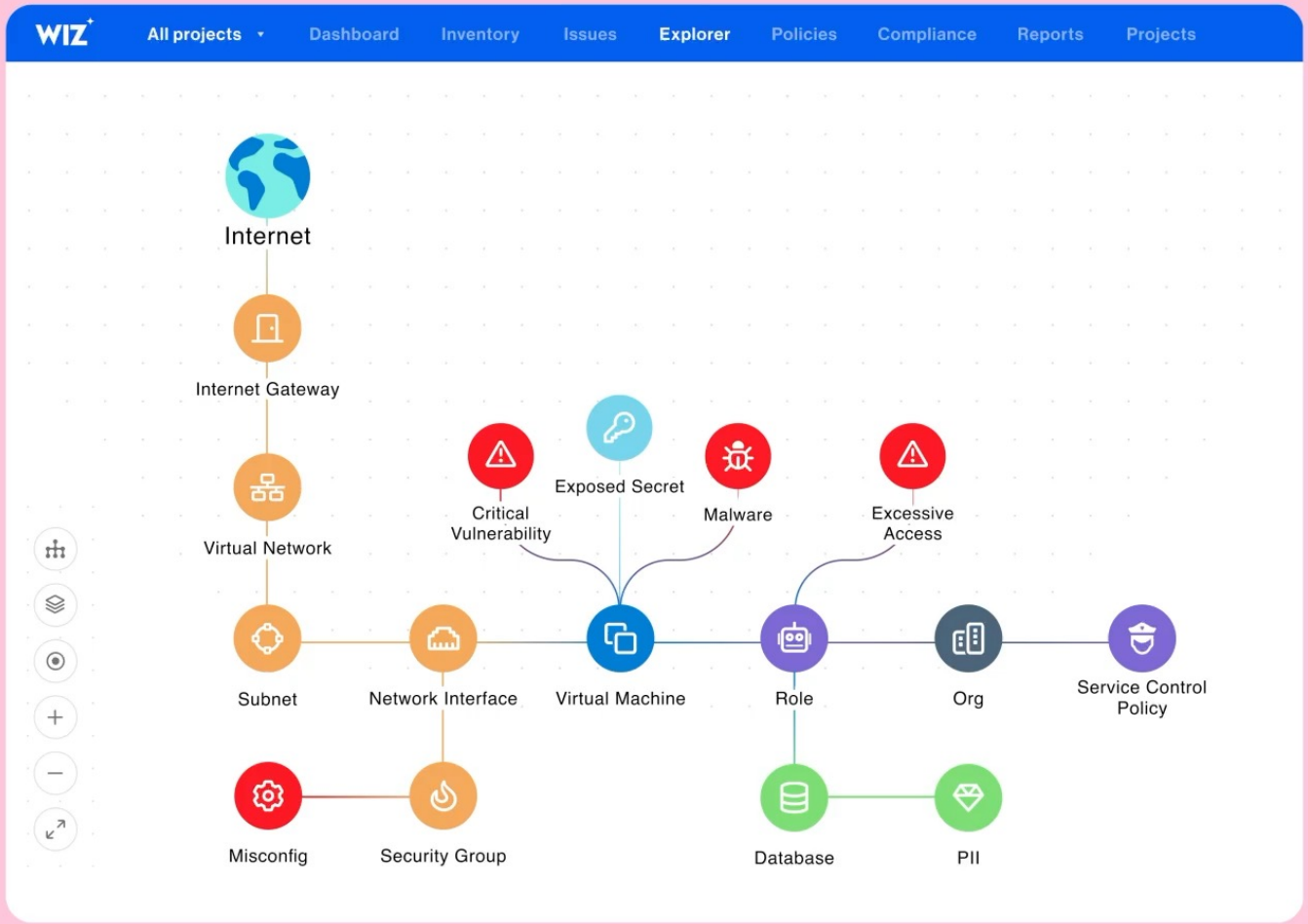
Identify risks

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



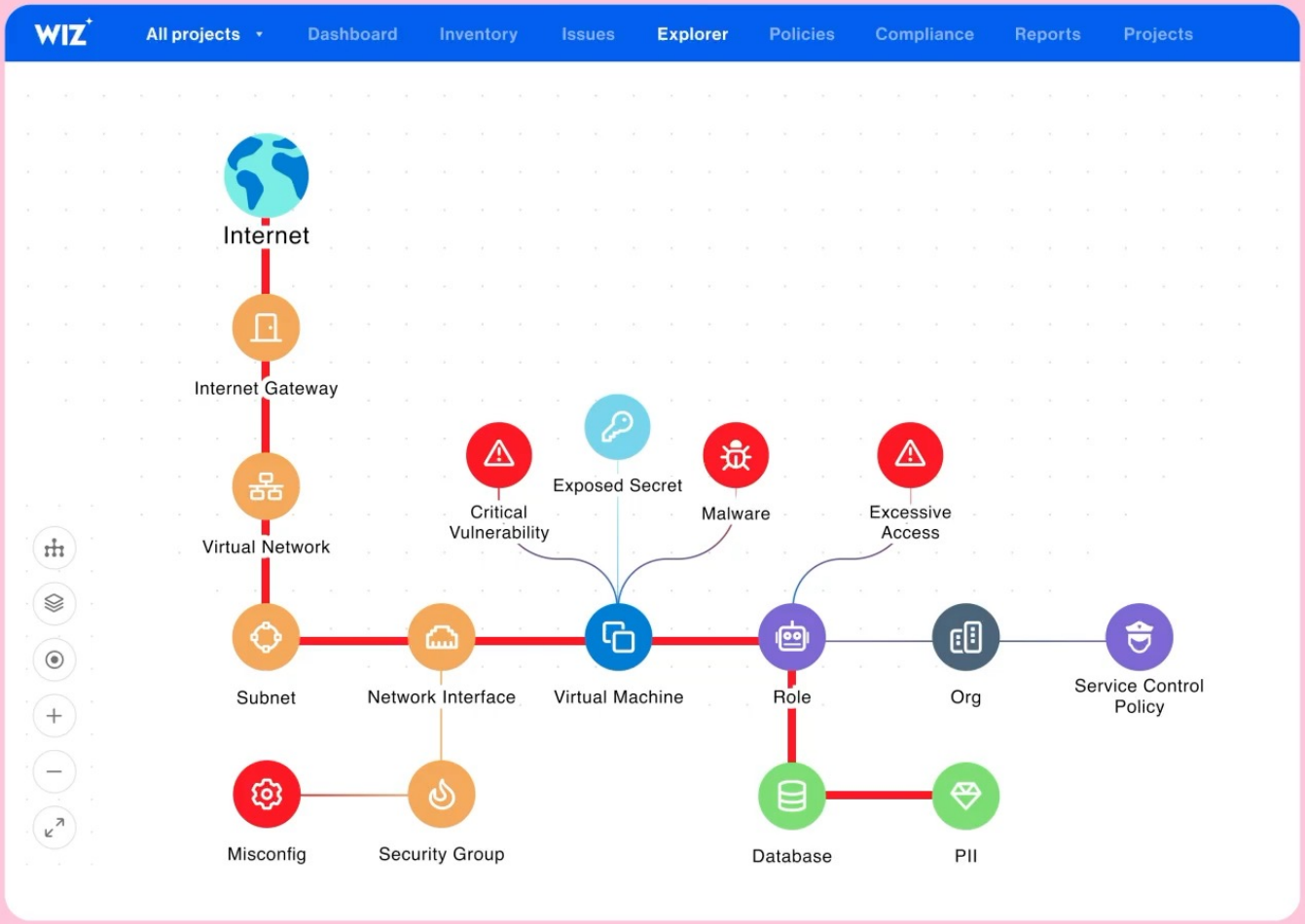
The cloud security operating platform

Prioritize attack paths



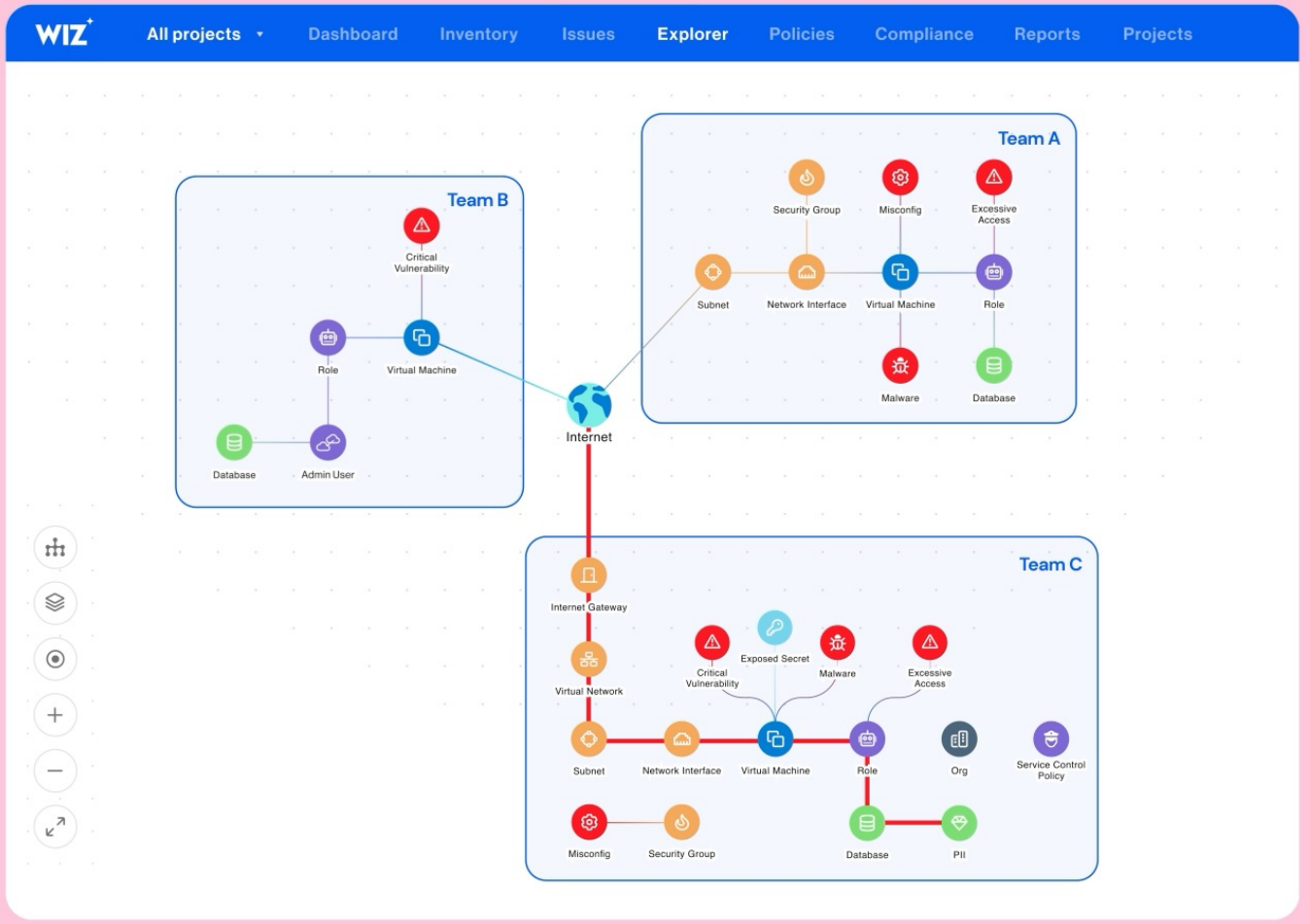
The cloud security operating platform

Determine ownership



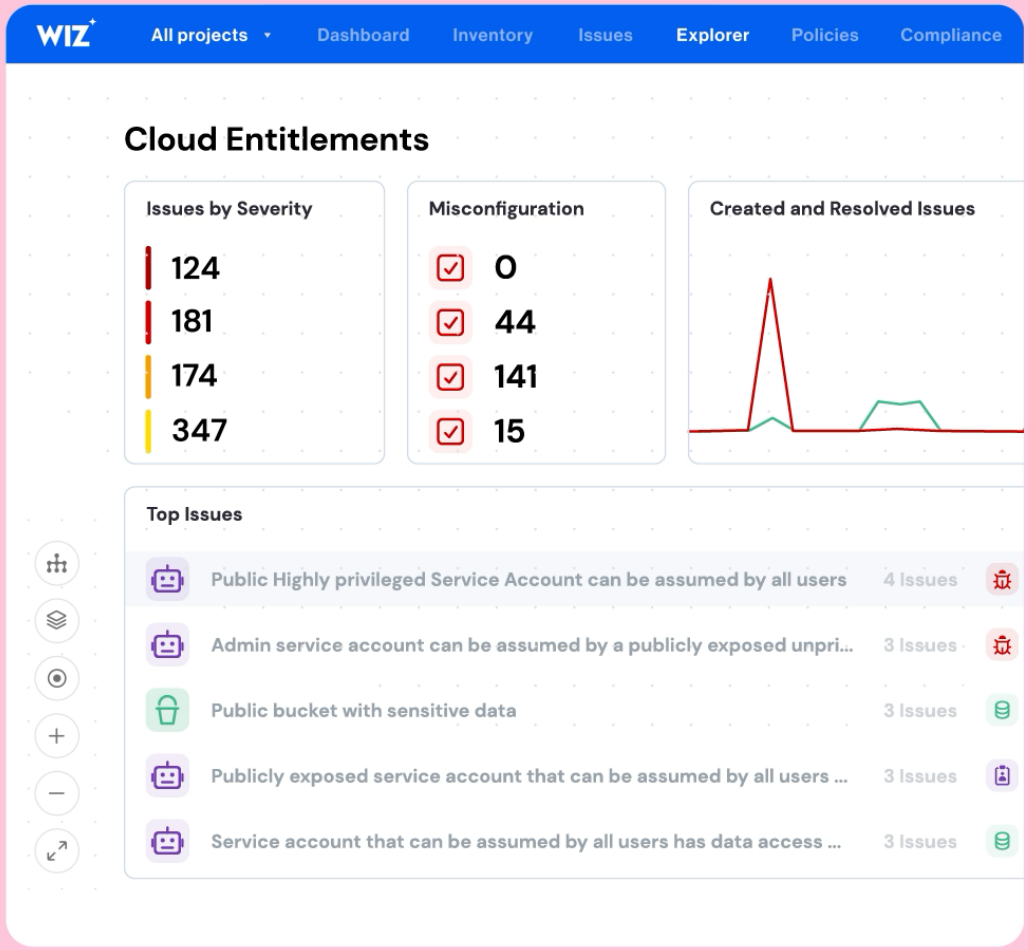
The cloud security operating platform

Automate workflows to speed remediation



The cloud security operating platform

Shift left prevention

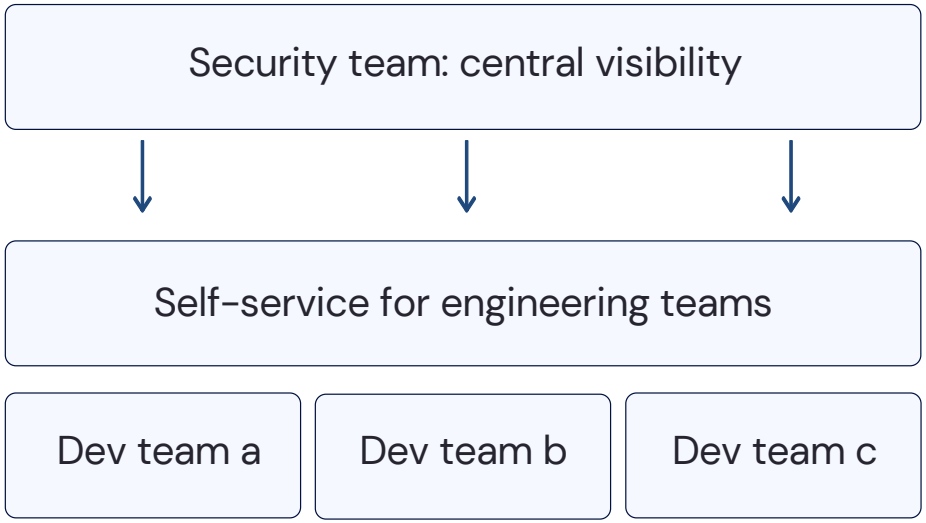


Team A

Team B

Team C

Cloud security is a team sport



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

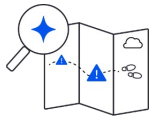
The network effect:
Out-of-the-box security baselines

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

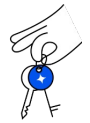
WIZ

Practical steps to safely transform to a cloud-first organization

Driving CNAPP to consolidate stack across security teams



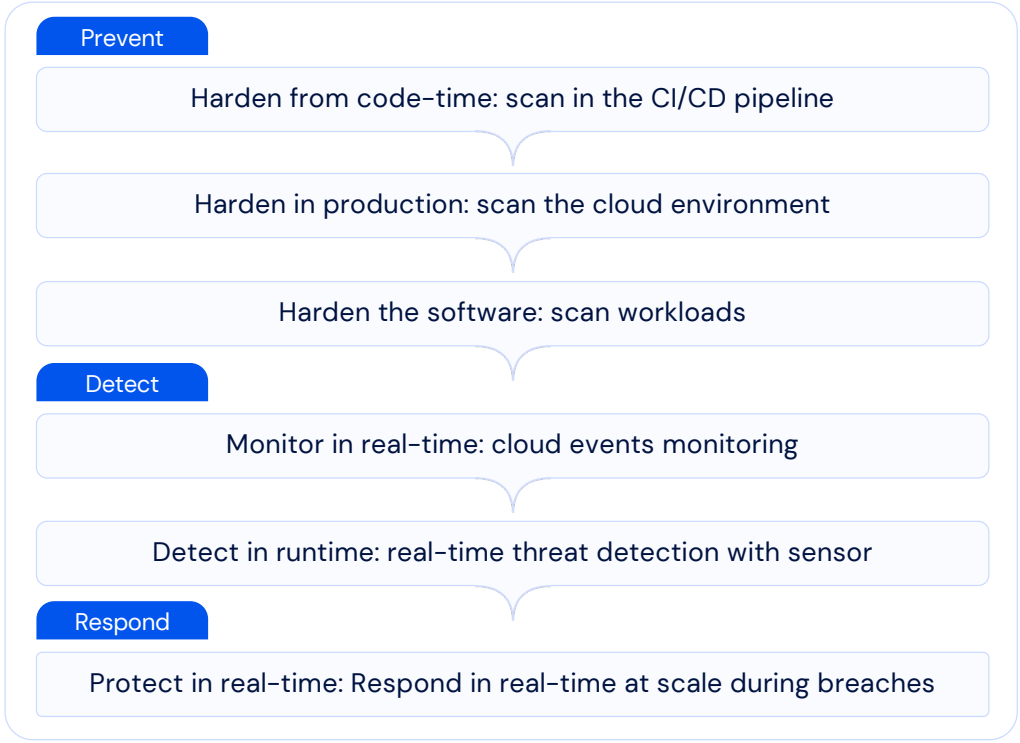
Nurture a risk-based approach to prioritize risks for remediation



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



WIZ

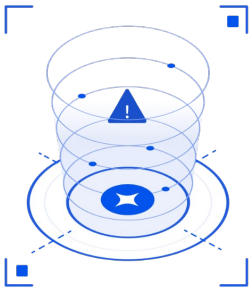
Introducing the Wiz Runtime Sensor: Unified cloud security from prevention to real-time detection and response

Prevention

Agentless visibility & risk prioritization that proactively reduces the attack surface

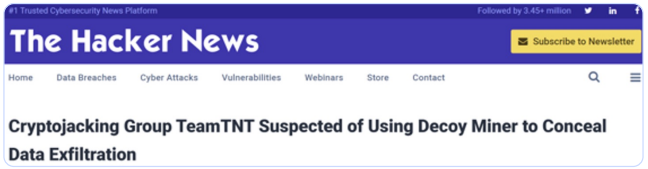
Real-time detection and response

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

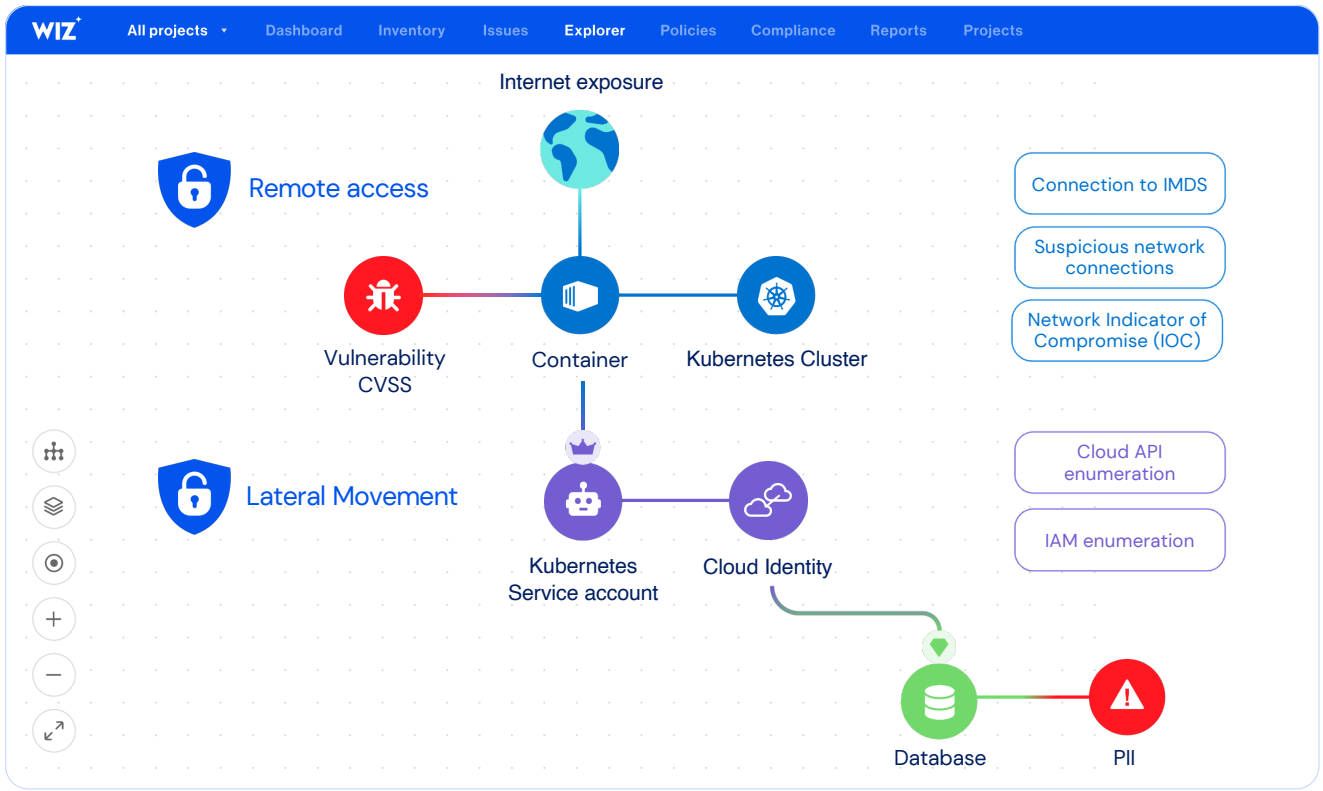
- Unknown and known threats
- Network activity
- Malicious behavior

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



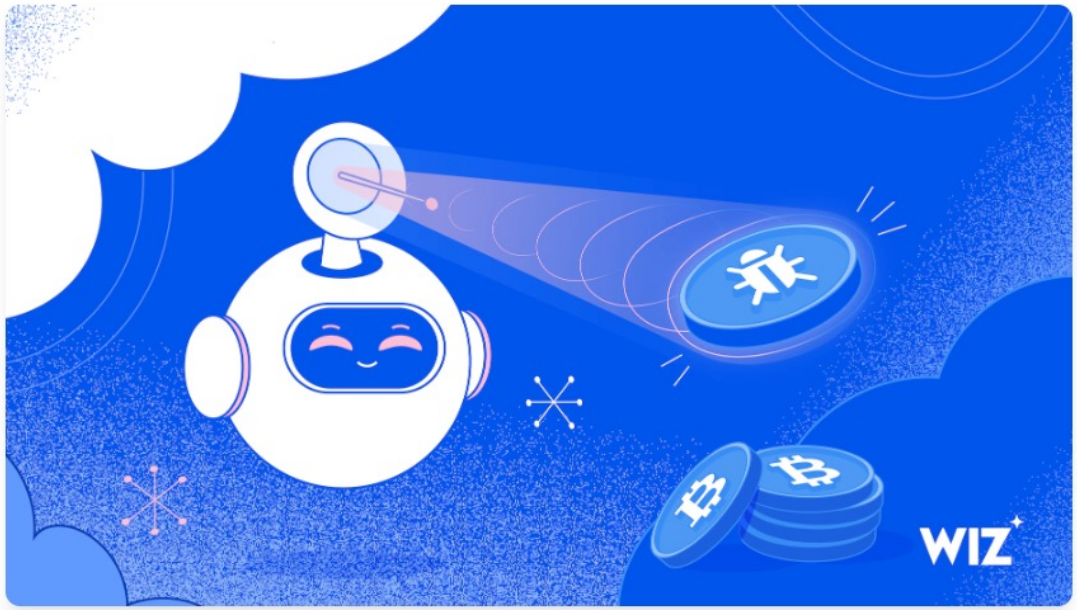
PyLoose: Python-based fileless malware targets cloud workloads to deliver cryptominer

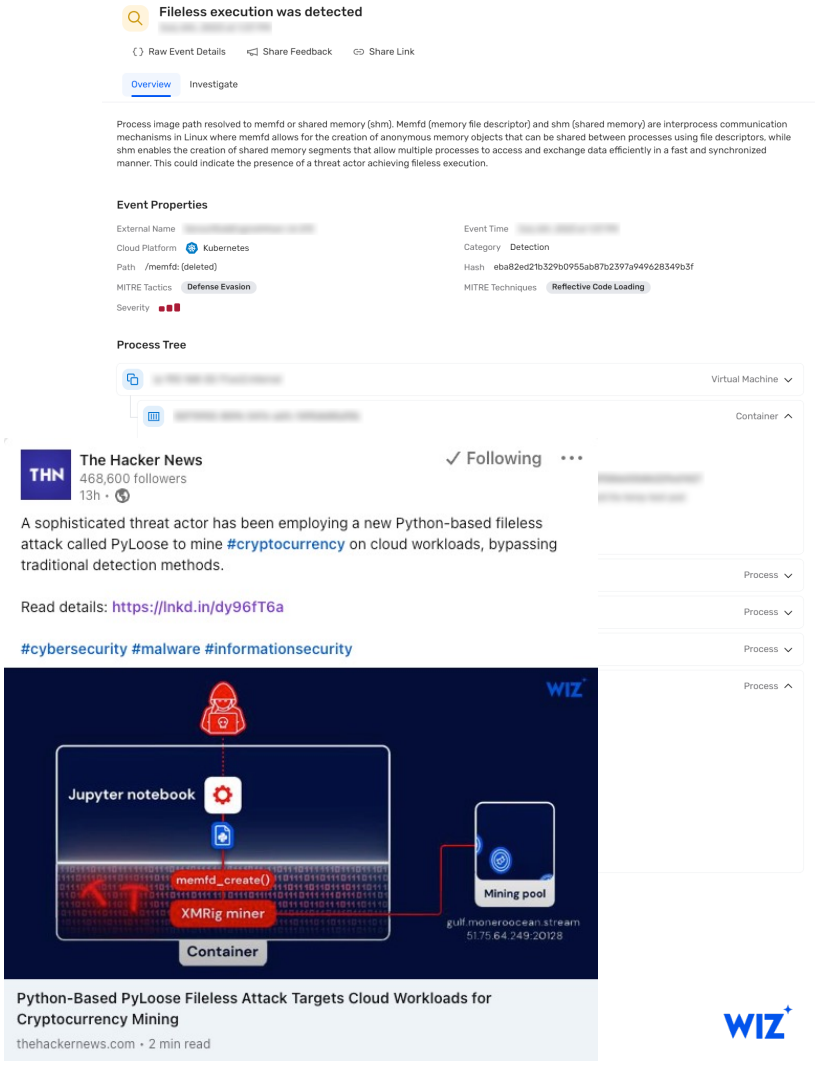
PyLoose is a newly discovered Python-based fileless malware targeting cloud workloads. Get a breakdown of how the attack unfolds and the steps to mitigate it.

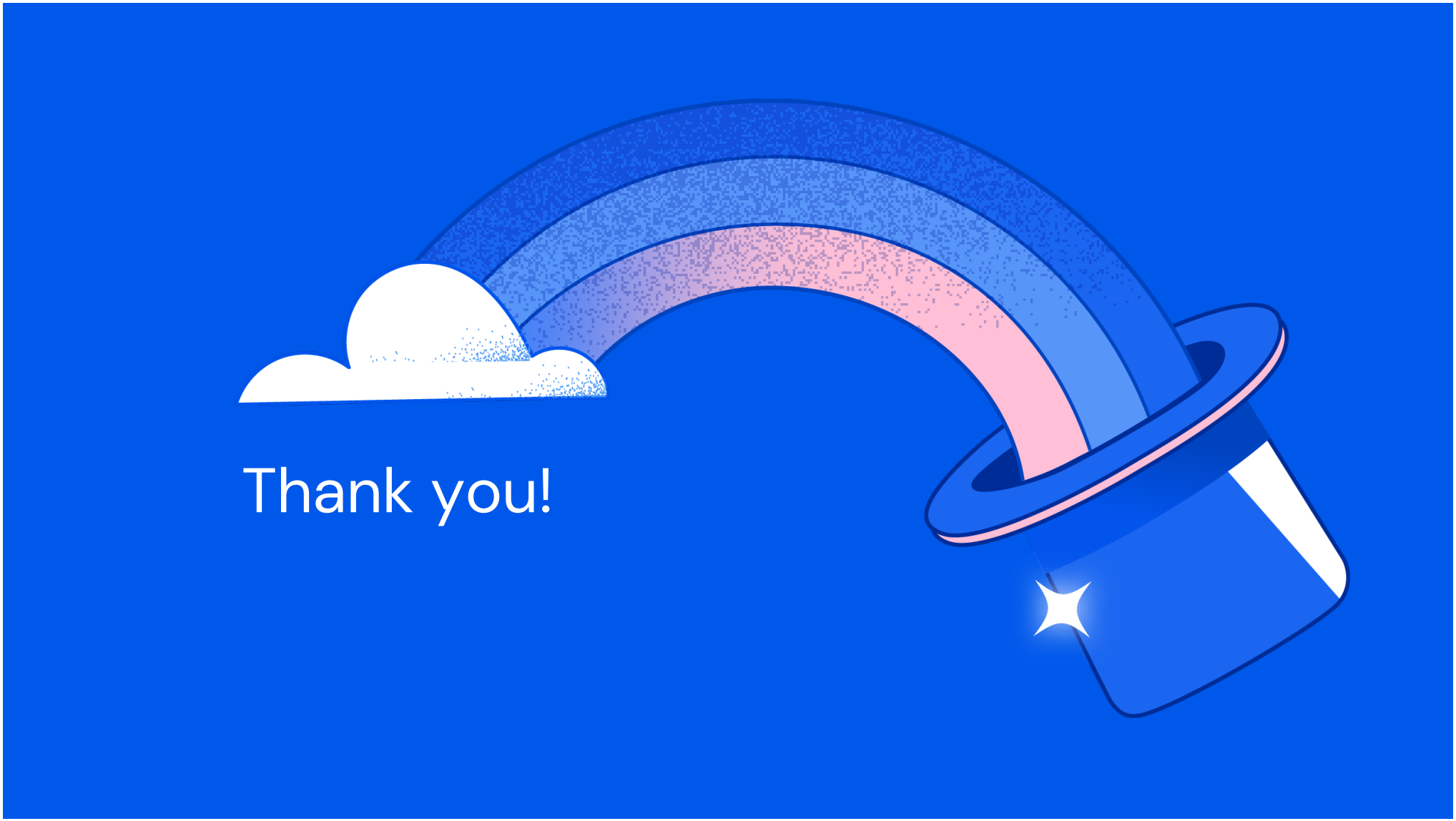
Avigayil Mechtinger, Oren Ofer, Itamar Gilad

6 min read

July 11, 2023






Thank you!