WIZ Research

Kubernetes Security 2030

Lessons From 50% of Fortune 100
and the Next Big Challenge

Shay Berkovich
Wiz Threat Research
shaybbc

Nico Ehrman
Product

What if I tell you..

That Kubernetes will be dead by 2030

Gitpod Leaves Kubernetes' 'Dead-End Failures', Adopts Home Grown Tool

November 26, 2024 application development, cloud, cloud-native applications, containers, devops, kubernetes, open source, virtual machines

Medium · Alistair Grew
700+ likes · 1 year ago

Are Kubernetes days numbered?

Circling back around to the original question I posed at the beginning of this post: **Are Kuberr numbered**? The simple answer is "no", ...

DevOps Paradox Backstage Contact Subscribe

DOP 62: Kubernetes Is Dead, Long Live Serverless

Posted on Wednesday, Jul 1, 2020

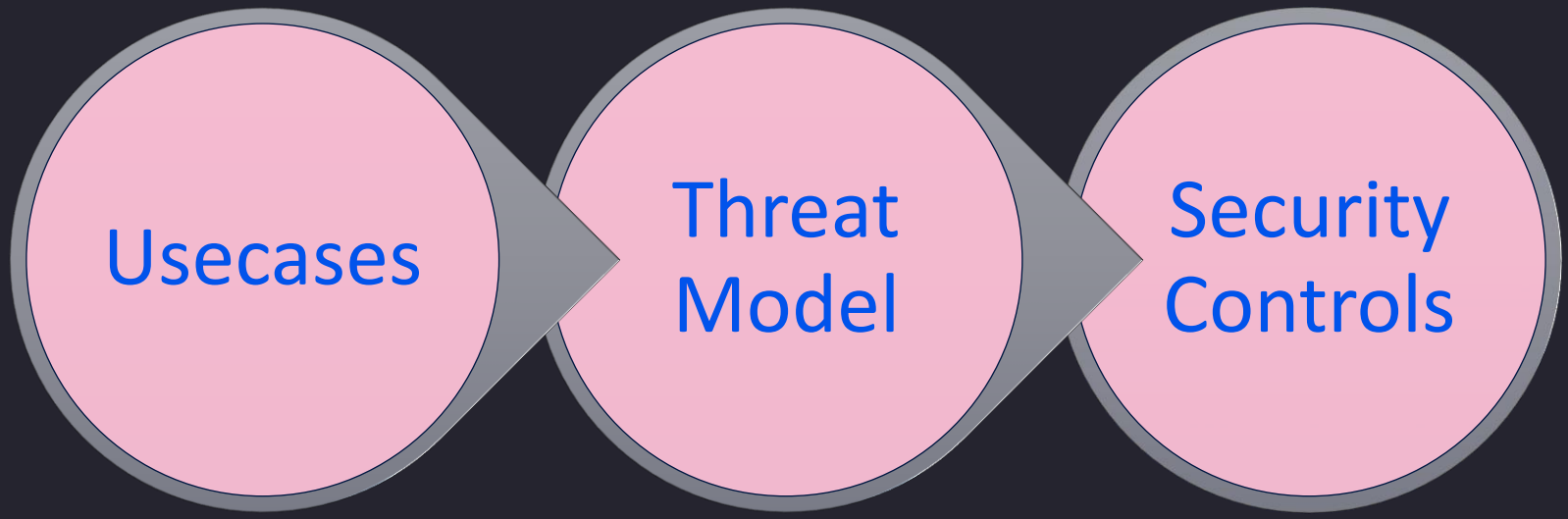
NEW OPERATION MODEL

“Kubernetes has matured to the point where it’s like Linux – its just there, does what it does, and gets out of the way”

Kelsey Hightower

But is this true for security?

Security evolution model



The Past

A look into the past

Security challenges of the early days

- **Core K8s vulnerabilities**

  Reviewing Critical and High vulns in K8s in the official CVE feed:

```
sshayb@PC-PF30LAFG:/mnt/c/Users/ShayBerkovich/git/k8s-sve-feed$ curl -sL https://k8s.io/docs/reference
/issues-security/official-cve-feed/index.json | jq '.items[] | .id + " " + .content_text' | grep criti
cal | wc -l
1
```

```
sshayb@PC-PF30LAFG:/mnt/c/Users/ShayBerkovich/git/k8s-sve-feed$ curl -sL https://k8s.io/docs/reference
/issues-security/official-cve-feed/index.json | jq '.items[] | .id + " " + .content_text' | grep **Hig
h** | wc -l
12
```

A look into the past

Security challenges of the early days

- **Core K8s vulnerabilities**

Did not materialize - K8s API is one of the most robust code bases out there

A look into the past

Security challenges of the early days

- Core K8s vulnerabilities
- **CRI escapes**

Liz Rice keynote at KubeCon EU 2018

Symlink-based escapes

Manifestation: Leaky vessels

A look into the past

Security challenges of the early days

- Core K8s vulnerabilities
- **CRI escapes**

Overall tamed / movement towards the solution: image verification, quick patching, hypervisors and sandboxes where needed

A look into the past

Security challenges of the early days

- Core K8s vulnerabilities
- CRI escapes
- **Image vulnerabilities**

- Inconsistencies across the scanners (UBCIS publication)
- Issues with package and metadat identification

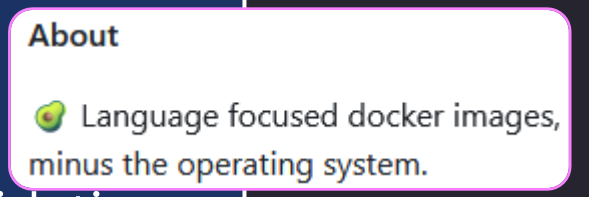
A look into the past

Security challenges of the early days

- Core K8s vulnerabilities
- CRI escapes
- **Image vulnerabilities**

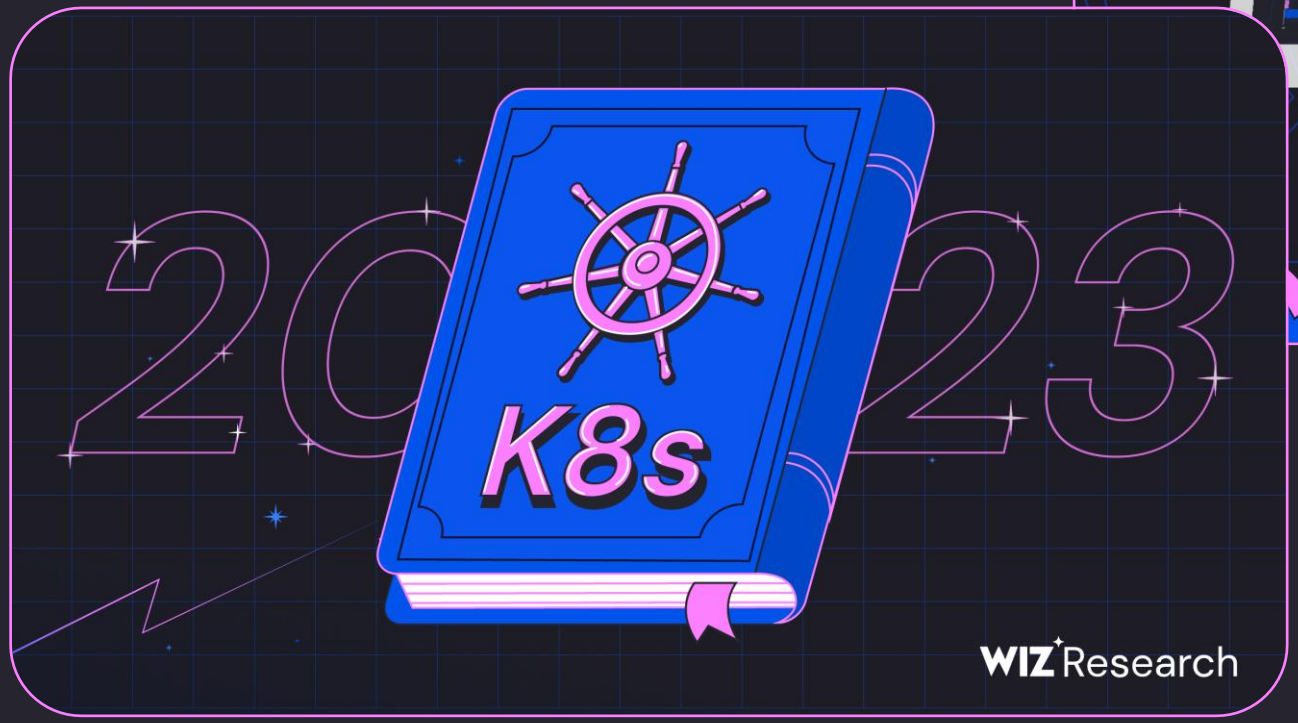
Overall tamed by

- SBOM and image scanners, not unique to this domain
- Minification of the images (Distroless anyone?)
- Movement towards the contextual and runtime vuln validation



The Present

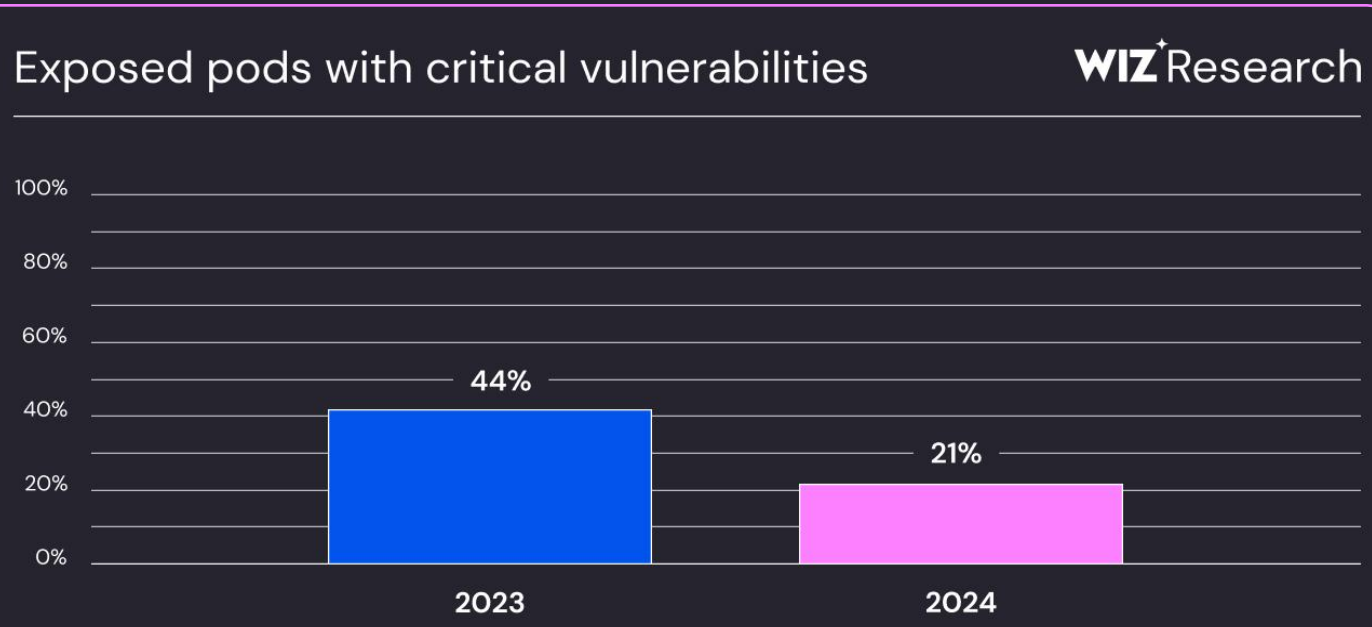
A look at the present



A look at the present

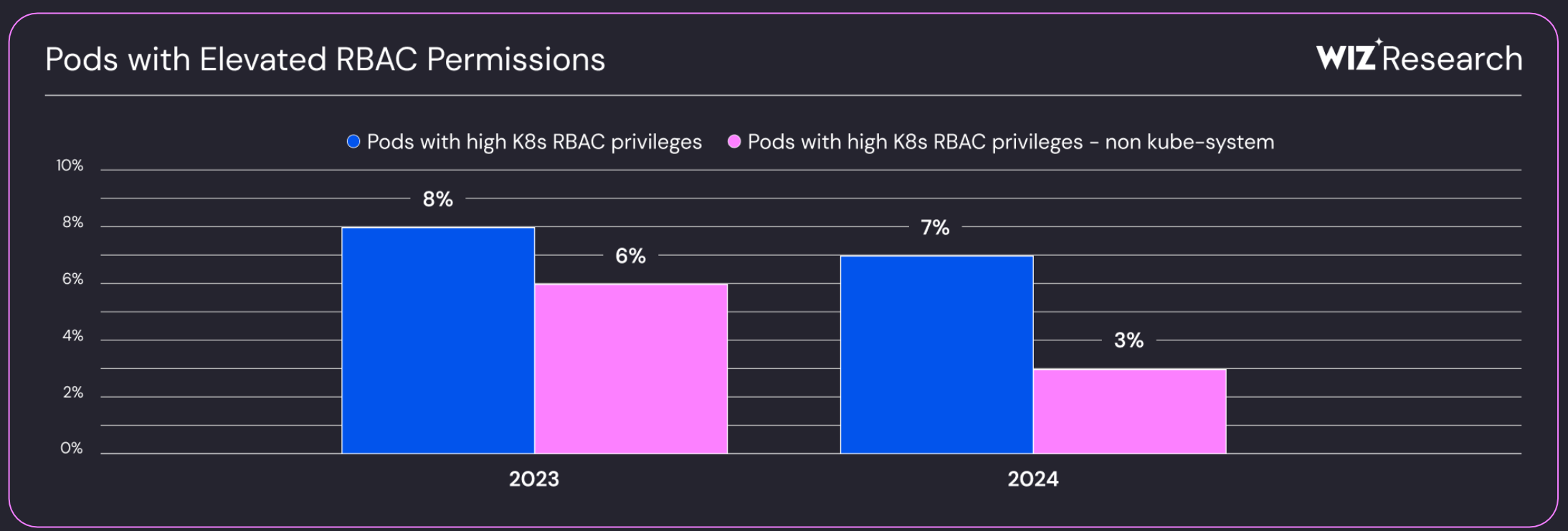
Positives – **better vulnerability management**

The proportion of critical vulnerabilities in exposed pods decreased by 50% between 2023-2024.



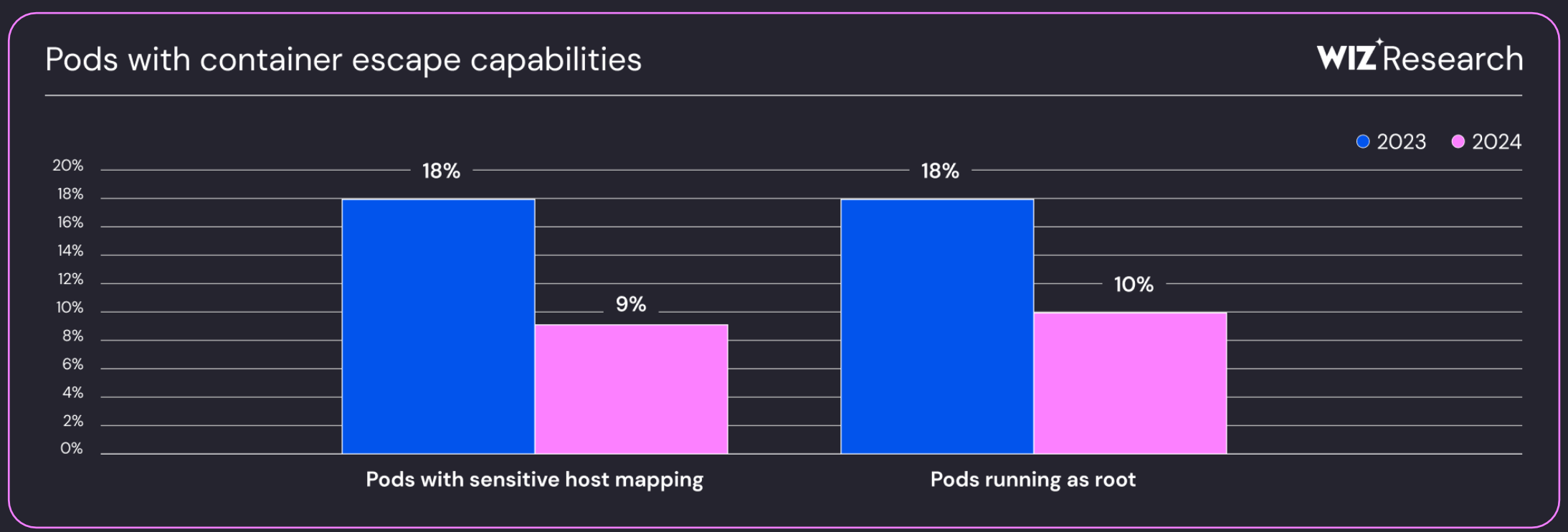
A look at the present

Positives – **better permission management**



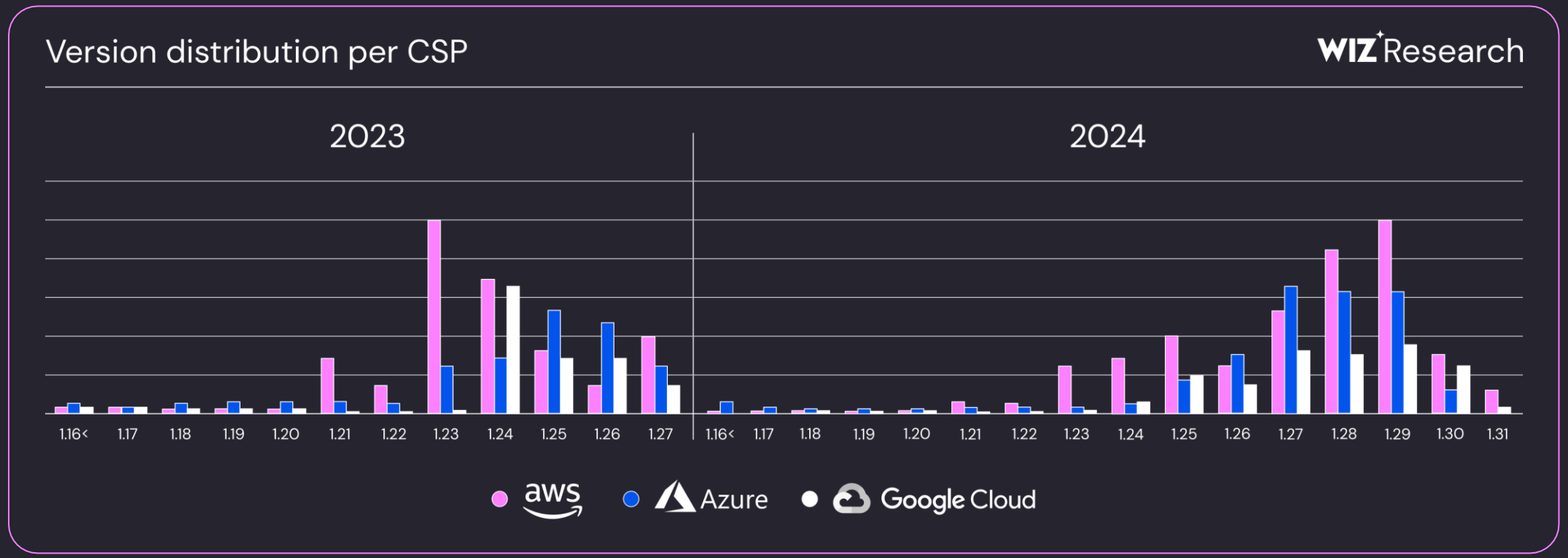
A look at the present

Positives – **better workload security**

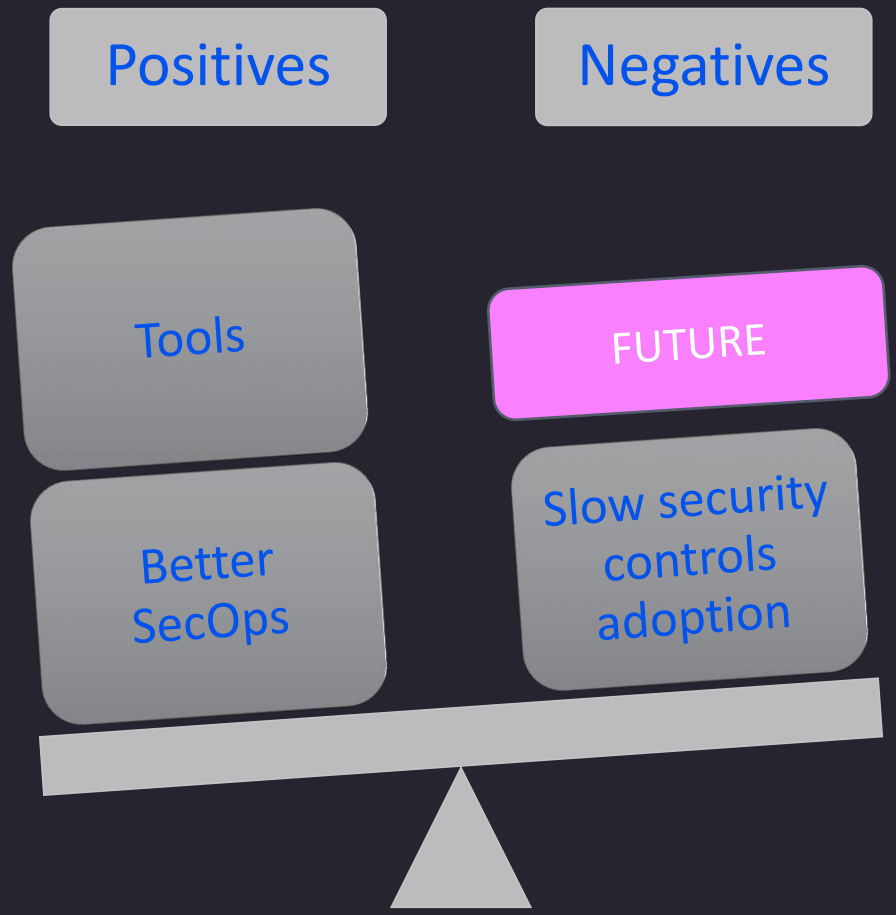


A look at the present

Positives – **better version management**



A look at the present



The Future

Wait, so what now?

K8s == OS for modern workloads

- By operation type: from academy to industry
- By workload type: from Webapps to H

WIZ Research

Device Plugins

Device plugins let you configure your cluster with support for devices or resources that require vendor-specific setup, such as GPUs, NICs, FPGAs, or non-volatile main memory.

FEATURE STATE: Kubernetes v1.26 [stable]

What's next

- Learn more about infrastructure extensions
  - Device Plugins
  - Network Plugins
  - CSI storage plugins
- Learn about kubectl plugins
- Learn more about Custom Resources
- Learn more about Extension API Servers
- Learn about Dynamic admission control
- Learn about the Operator pattern

Extensibility

Network Plugins

Kubernetes (version 1.3 through to the latest 1.32, and likely onwards)

Dynamic Admission Control

In addition to compiled-in admission plugins, admission plugins can be developed as extensions

Extend kubectl with plugins

Extend kubectl by creating and installing kubectl plugins.

WIZ Research

Future – AI Threat Model Support

Training

- Training data
- Model material

Inference

- Compute integrity
- Compute availability
- Confidentiality

Training vs Inference = Protect data vs Protect compute

Threat Model changes

Different security controls are needed

Future – AI and Multi-Tenancy

Execution-as-service and X-tenant vulnerabilities

- Hugging face – breaking out of inference runtime
- Replicate – malicious model + LM
- Sap AI – AI to env takeover
- NVIDIA Container Toolkit – from image to host

Inference

- Compute integrity
- Compute availability
- Confidentiality

Device Plugins

Device plugins let you configure your cluster with support for devices or resources that require vendor-specific setup, such as GPUs, NICs, FPGAs, or non-volatile main memory.

FEATURE STATE: Kubernetes v1.26 [stable]

What's next

- Learn more about infrastructure extensions
  - Device Plugins
  - Network Plugins
  - CSI storage plugins
- Learn about kubectl plugins
- Learn more about Custom Resources
- Learn more about Extension API Servers
- Learn about Dynamic admission control
- Learn about the Operator pattern

Extensibility

Network Plugins

Kubernetes (version 1.3 through to the latest 1.32, and likely onwards)

Dynamic Admission Control

In addition to compiled-in admission plugins, admission plugins can be developed as extensions

Extend kubectl with plugins

Extend kubectl by creating and installing kubectl plugins.

WIZ Research

Future – Peripheral Vulnerabilities

The era of core vulnerabilities is over, next to the perimeter vulnerabilities

- CNI and storage vulns
- Device plugins
- Ingress NGINX controller

Future – Peripheral Vulnerabilities

Ingress NGINX controller

IngressNightmare: CVE-2025-1974 – 9.8 Critical Unauthenticated Remote Code
ress NGINX

over.

CVE ID	Issue Summary
CVE-2025-1974	ingress-nginx admission controller RCE escalation
CVE-2025-1098	configuration injection via unsanitized mirror annotations
CVE-2025-1097	configuration injection via unsanitized auth-tls-match-cn annotation
CVE-2025-24514	configuration injection via unsanitized auth-url annotation
CVE-2025-24513	auth secret file path traversal vulnerability

WIZ Research

Future – Cloud Integration

K8s + Cloud = 

- Bloatware in managed clusters

  (our talks from KubeCon EU 2023 and 2024)

- Tight integrations with cloud = additional attack surface

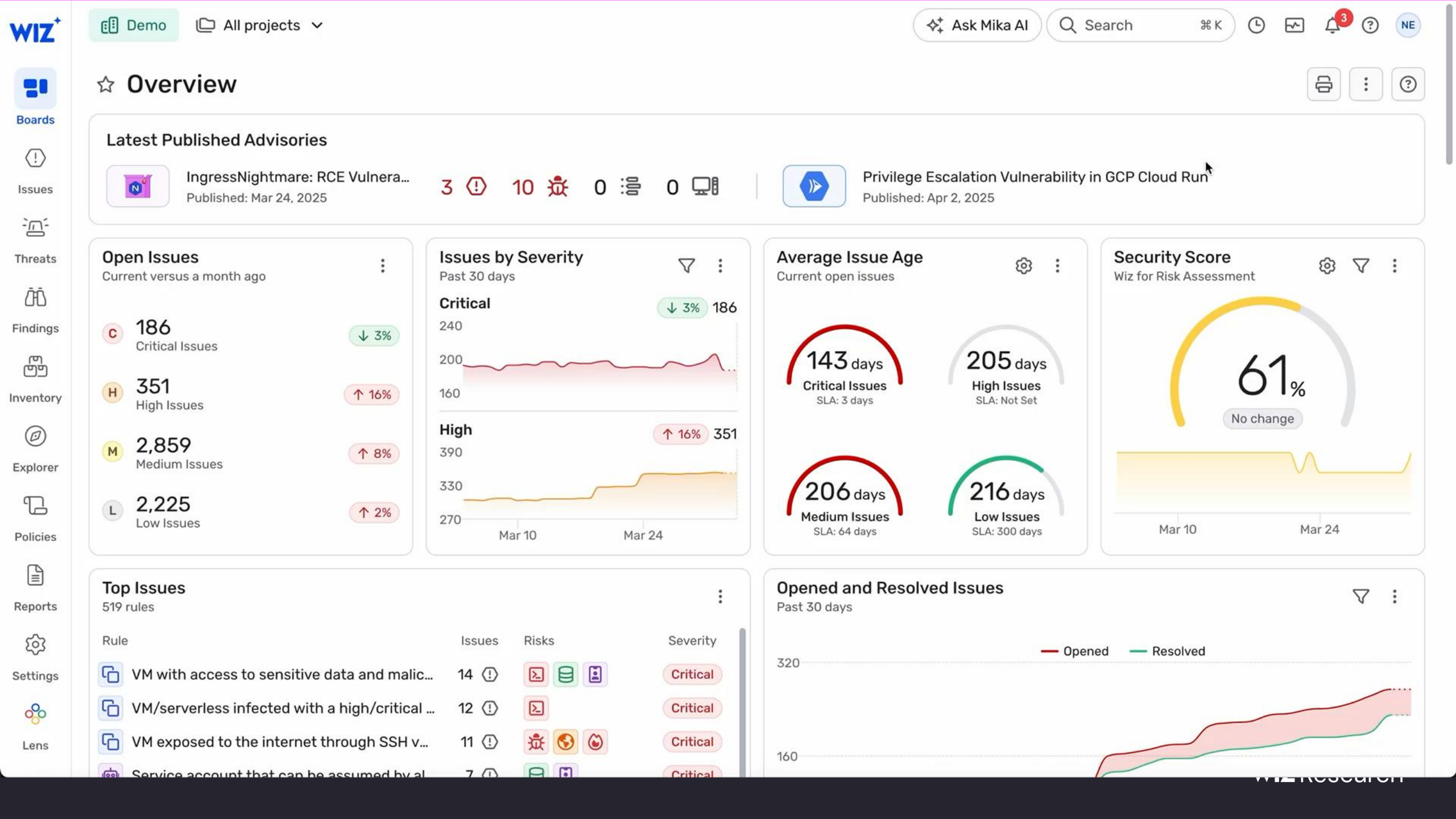
  (Our blog series on security analysis of EKS Access management and EKS pod identity)

Future – Cloud Integration

K8s + Cloud = 

Cloud headaches are now K8s headaches

Product Response


Demo
All projects
Ask Mika AI
Search ⌘K
NE
Overview
Boards
Issues
Threats
Findings
Inventory
Explorer
Policies
Reports
Settings
Lens
Latest Published Advisories
IngressNightmare: RCE Vulnera…
Published: Mar 24, 2025
3
10
0
0
Privilege Escalation Vulnerability in GCP Cloud Run
Published: Apr 2, 2025
Open Issues
Current versus a month ago
C 186 Critical Issues ↓ 3%
H 351 High Issues ↑ 16%
M 2,859 Medium Issues ↑ 8%
L 2,225 Low Issues ↑ 2%
Issues by Severity
Past 30 days
Critical ↓ 3% 186
240
200
160
High ↑ 16% 351
390
330
270
Mar 10
Mar 24
Average Issue Age
Current open issues
143 days Critical Issues SLA: 3 days
205 days High Issues SLA: Not Set
206 days Medium Issues SLA: 64 days
216 days Low Issues SLA: 300 days
Security Score
Wiz for Risk Assessment
61%
No change
Mar 10
Mar 24
Top Issues
519 rules
Rule
Issues
Risks
Severity
VM with access to sensitive data and malic… 14 Critical
VM/serverless infected with a high/critical … 12 Critical
VM exposed to the internet through SSH v… 11 Critical
Service account that can be assumed by al… 7 Critical
Opened and Resolved Issues
Past 30 days
Opened
Resolved
320
160
Wiz Research

Thank you for listening!

Questions?

WIZ Research