

Container Security at Scale:

Lessons Learned from the Front Lines



Today's speakers



Wiebe de Roos
CI/CD Consultant
ABN AMRO and Flusso



Keith Mokris
Technical Marketing Engineer
Palo Alto Networks

What we'll cover today

- Latest trends in container adoption, touching on the latest CNCF survey results
- Security best practices when using containers
- ABM AMRO's success in securing their containerized stack across their organization

CNCF Survey 2019 Stats

Key takeaways

- **Containers are here to stay:**

84% of respondents are using containers in production, a jump of more than 15% from 2018

- **Kubernetes use is UP, especially managed K8s!**

78% of respondents are using Kubernetes in production, a huge jump from 58% last year

- **Serverless gaining relevancy:**

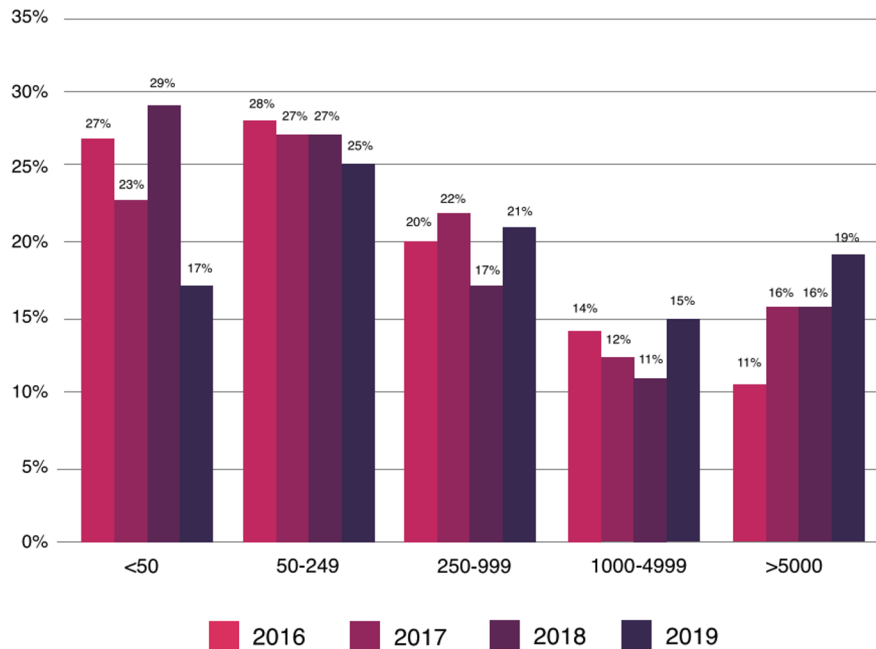
At least 41% of respondents are using serverless technologies

Source: CNCF Survey 2019 - Deployments are getting larger as cloud native adoption becomes mainstream | [LINK](#)

Number of containers in production

- Growth trending left to right to greater numbers
- According to CNCF: the number of respondents using 250 or more containers **increased by 28%**, to **more than half**.

Number of Containers in Production

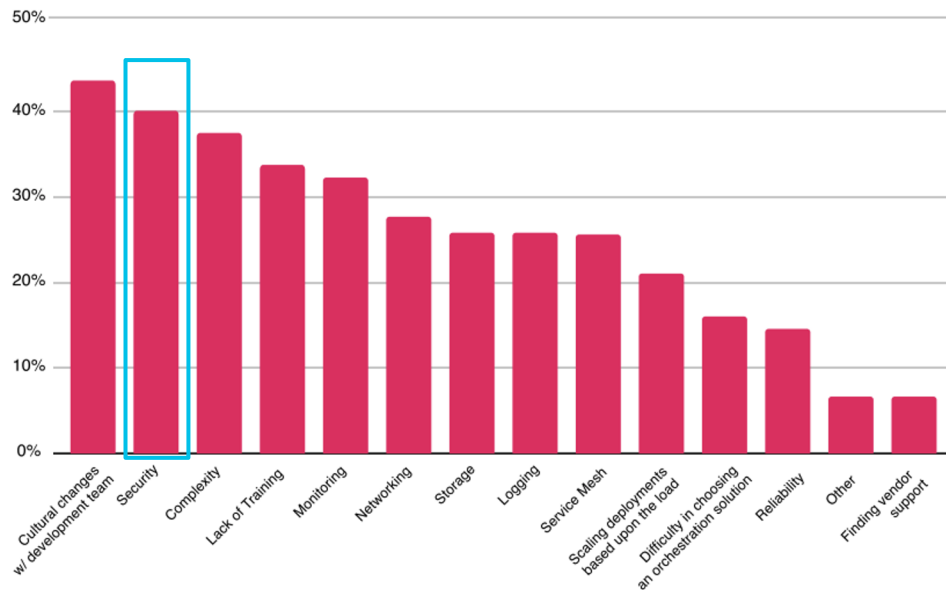


Source: CNCF Survey 2019 - Deployments are getting larger as cloud native adoption becomes mainstream | [LINK](#)

Security is a top challenge for using/deploying containers

- **40%** of respondents report security as a top challenge
- At the same time, cultural changes, complexity, lack of training, and monitoring also above **30%**

What are your challenges in using/deploying containers?
Please select all that apply.



Source: CNCF Survey 2019 - Deployments are getting larger as cloud native adoption becomes mainstream | [LINK](#)

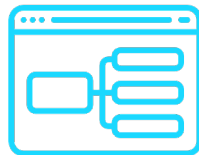
Container Security Best Practices: The Palo Alto Networks View

Container Characteristics



Minimal

Typically
single process
entities



Declarative

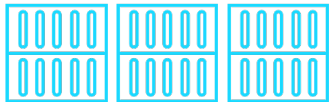
Built from
images that
are machine
readable



Predictable

Do exactly the
same thing
from **run** to
kill

What's Difficult About Securing Containers?



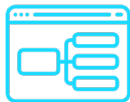
Many more entities



High rate of change, much more ephemeral



Security is largely in the hands of the developer

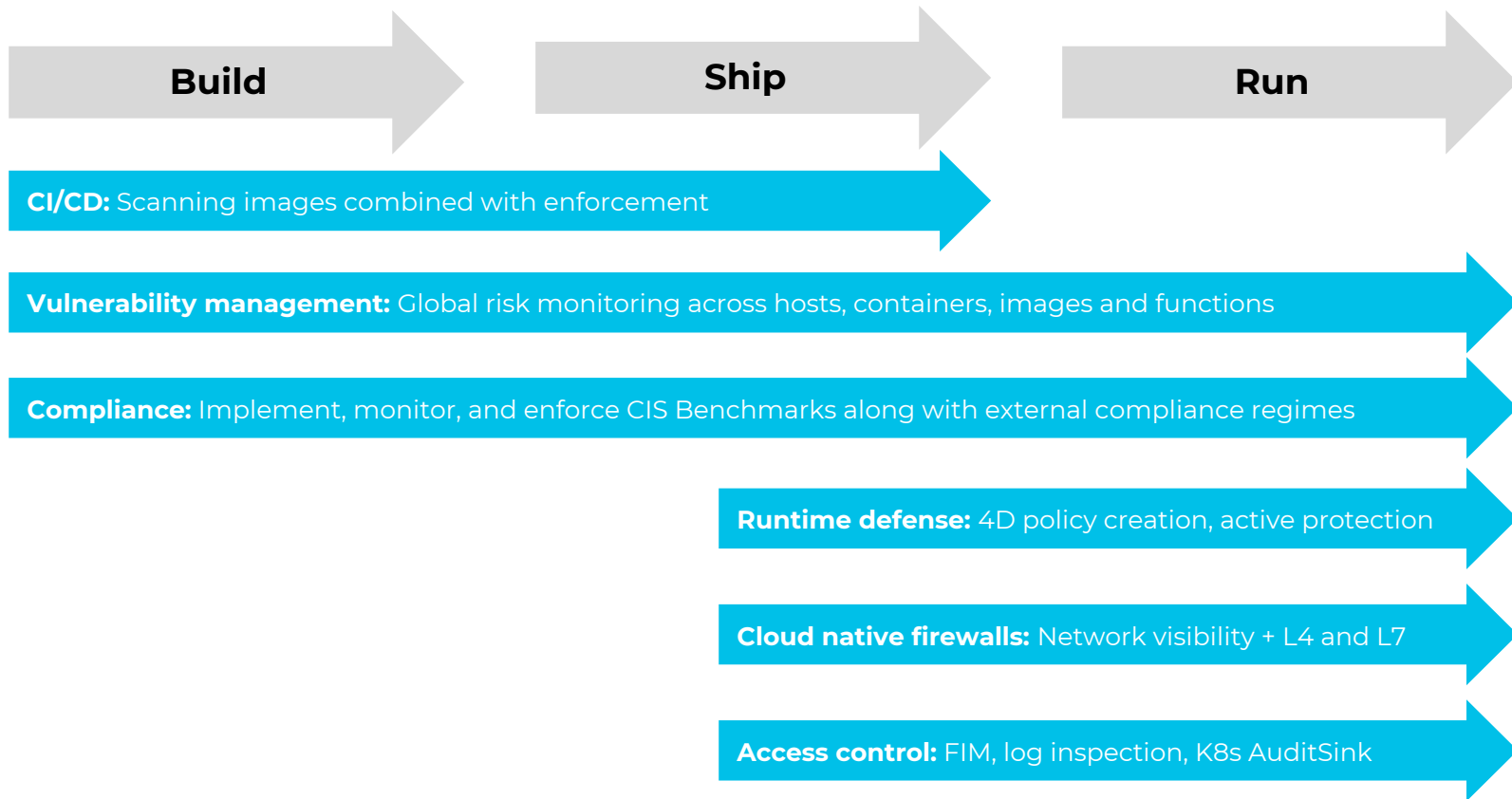


Security must be as portable as the containers itself

Securing container deployments--the Palo Alto Networks view:

- Prioritize risk in production environments
- Implement CIS Benchmarks across your entire stack
- Protect applications at runtime using automated application whitelisting, including the network layer
- Integrate security into DevOps workflows

Key Steps to Secure Containers Across the Application Lifecycle





Container adoption at enterprise scale *status so far and lessons learned*

ABN AMRO Bank

Wiebe de Roos - CI/CD
Consultant & Engineer

Topics for today

- Container journey - quick overview
- The managed container platform
- Positioning of Prisma Cloud Compute
- Challenges and solutions
- Some notes about the future

Financial sector

Enterprising bank

18,830

Total # of employees

Amsterdam

Headquarter

400+

Development Teams

Agile organization

DevOps / Hybrid cloud

3,000+

Applications

Container journey so far

Jenkins Core in AWS



Container platform EKS



The big shift



2017/2018

2019 Q1

2019 Q2

2019 Q3

2019 Q4

2020 Q1



First Docker PoCs



Twistlock

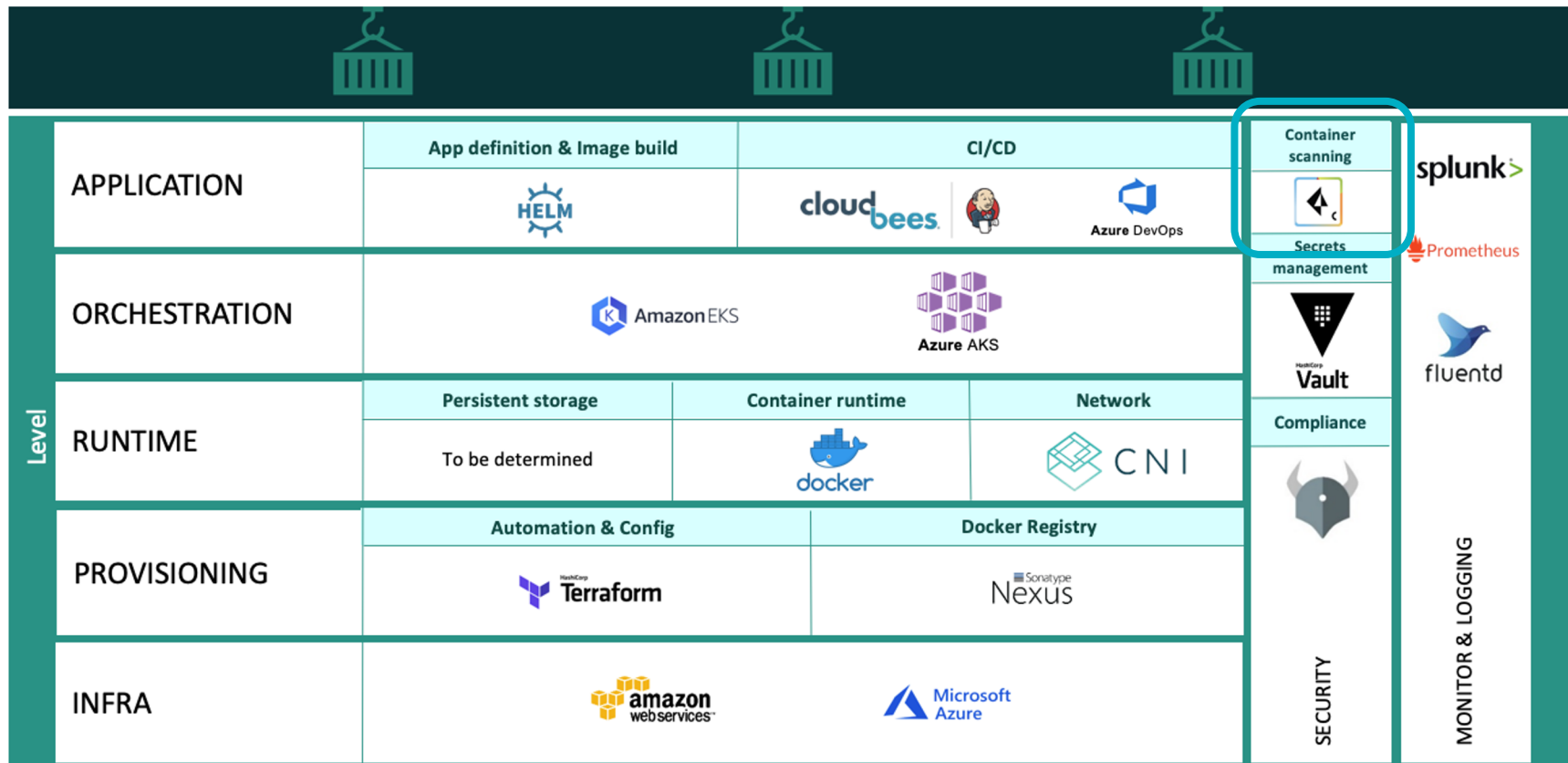


Open Policy Agent



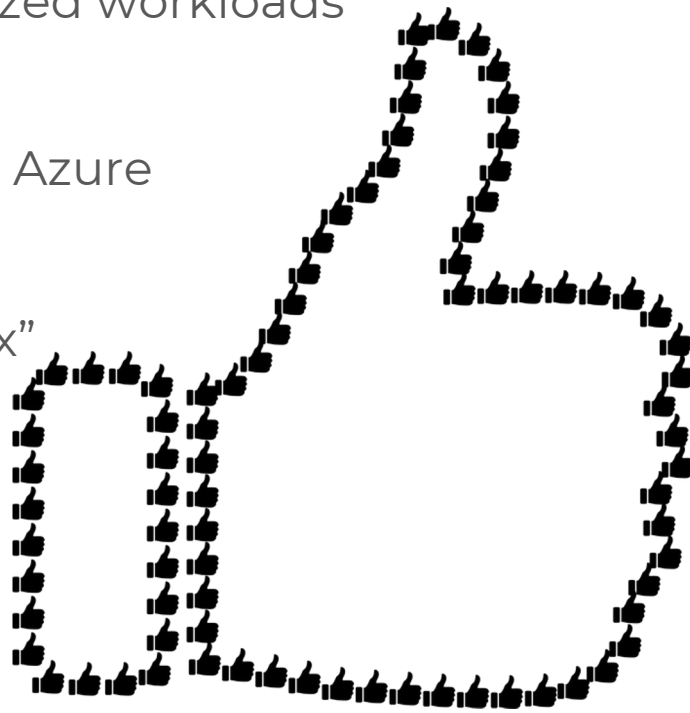
Container platform AKS

Managed Container Platform



The six most important goals of the MCP

1. One K8S based solution for all containerized workloads
2. CI/CD processes are standardized
3. Support the company-wide migration to Azure
4. Compliance for all components
5. Container & k8s security is “out of the box”
6. Supports (controlled) team autonomy



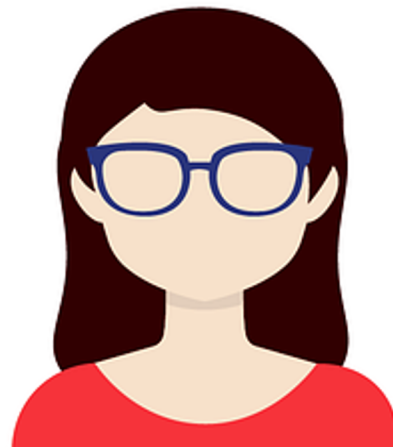
Positioning of Prisma Cloud Compute

Use Prisma Cloud for containers in:

- Azure
- AWS
- On prem
- Local systems

Prisma Cloud is a “standard building block” in pipelines

Future state:
block issues before the security risks become a *real* problem



Containers at scale - 5 enterprise grade challenges



Source:
<http://pixabay.com/>

Challenge #1: overcome the knowledge gap

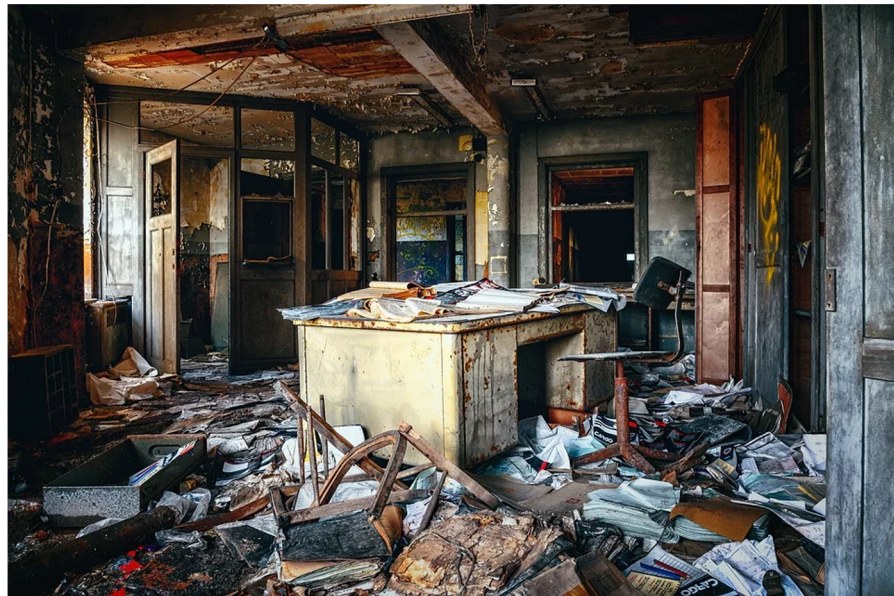
“Everyone is running containers now, but how to run them secure across the enterprise?”

- The right knowledge should be centrally available
- Map Prisma Cloud policies with detailed info
- Create real world examples based on sample code
- Let teams experiment in a sandbox
- Share the agenda to start **breaking** builds
- Practice the “**WET** principle” (**W**e **E**njoy **T**elling) ;-)

Challenge #2: a big mess of issues

“How to deal with all of the security issues and violations?”

- Do the ultimate shift left!
- Use “collections” in Prisma Cloud to segregate teams
- Don’t just extend the security team → be smart
- Set priorities → use your business units
- Have a **very** good review process in place*.




Source:
<http://pixabay.com/>

* Highly valuable feature request ;-)

Challenge #3a “Shift security left & break stuff fast, BUT...”

Scan details

Image 
ID sha256:f2f352cf387fec91fc797973afdf1de3fabb9dc976ca3e93be26ba66f5490332
OS distribution Alpine Linux v3.9
Scan Status ● Failed
Vulnerability threshold low
Compliance threshold low

- The pain to learn.
- How to collect feedback from security experts?
- How to deal with context-specific situations?
- The long pending discussion on base images.

Vulnerabilities

Compliance

Layers

Package Info

Labels

Risk Factors



Q Search

Id	Type	Highest Severity	Description
47	jar	● critical	com.fasterxml.jackson.core_jackson-databind version 2.9.9 has 17 vulnerabilities. Show details
46	OS	● critical	sqlite (used in sqlite-libs) version 3.26.0-r3 has 3 vulnerabilities. Show details
46	OS	● critical	musl (used in musl-utils, musl) version 1.1.20-r4 has 1 vulnerability. Show details
46	OS	● critical	libbsd version 0.8.6-r2 has 1 vulnerability. Show details
46	OS	● critical	bzip2 (used in libbz2) version 1.0.6-r6 has 1 vulnerability. Show details
46	OS	● high	gcc (used in libstdc++, libgcc) version 8.3.0-r0 has 1 vulnerability. Show details

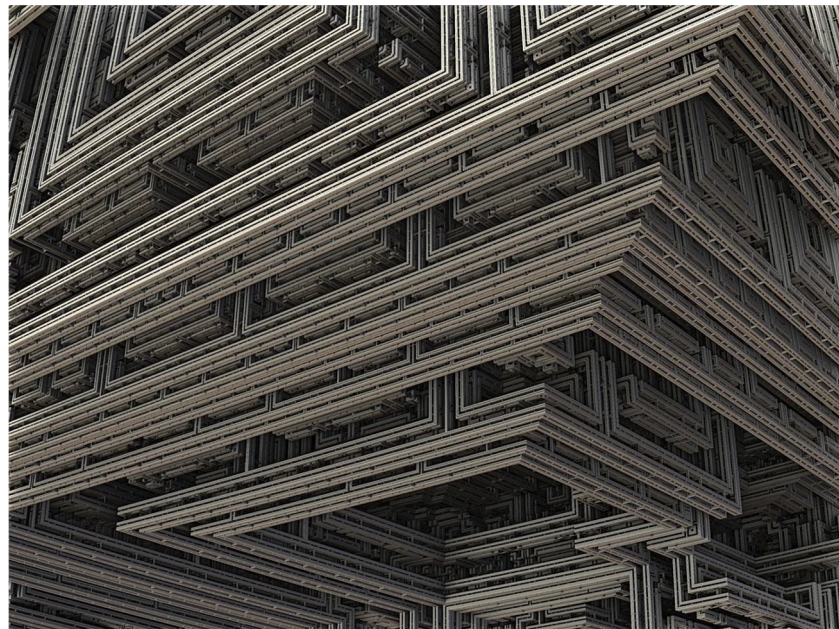


ABN-AMRO

Challenge #3b common patterns to patch images

“How to effectively patch container images?”

- Swap the container image for the patched one
- Collaborate with a Vendor (if applicable)
- Upgrade packages and their dependencies (hard!)
- Remove the insecure part (be careful!)
- Replace the package
- “I have **bad** news for you”



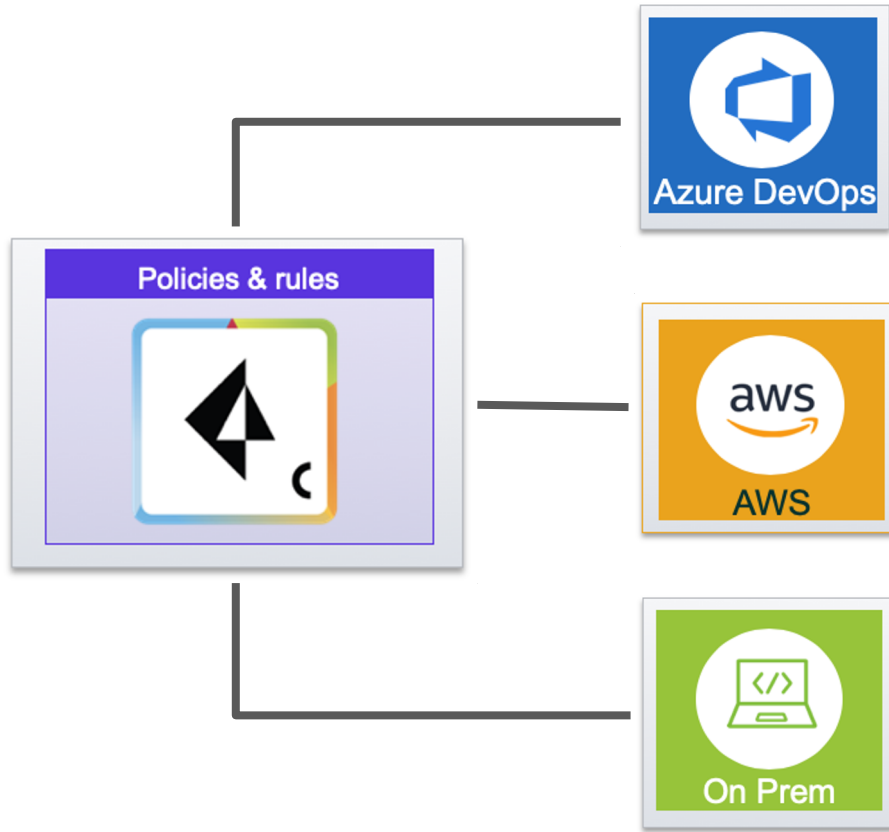
Source:

Keeping the organization “compliant” and in control



Source:
<http://pixabay.com/>

Challenge #4 One Prisma Cloud instance for all



This means:

- Team autonomy versus control & visibility
- AWS VPC: the challenge of defenders
- What if one console instance is not enough?

Challenge #5 enforce and control

“Just 5 considerations to start with...”

- Duration of the “grace period” wrt build breakers in your CI/CD pipelines.
- Who should manage the Defenders*?
- Pure cloud native versus best of tools.
- Traceability of Images, when to really trust it?
- Optimal security versus business benefits

“Our journey continues, security is never done...”

* Another feature request ;-)

A bright future

- All container workloads protected in all environments (multi- & hybrid cloud)
- Review process optimized → scale up
- Containers will be the new “mainstream” → ***on-prem > /dev/null?***
:)

Thank you

Contact:

Wiebe De Roos

wiebe.de.roos@nl.abnamro.com

Keith Mokris

kmokris@paloaltonetworks.com

