How can you scale it if you don’t trust it?

Start At the End

• Production environments are all about trust
  • What does a workload contain?
  • Where does a workload run?
  • Are the right resources in play for the right workload for the right people?
  • Can information flow only in a secure manner?
• Bigger the deploy, harder it is to maintain the trust
• Super hard with multi-clouds
policy

policy
It’s 2am, and I’m sure more memory will make it work better.
Lots more.

Malware in a public Docker image?
What malware?
My container is talking to who on the Internet?
It shouldn’t be taking up any bandwidth at all.

The newest OpenSSL exploit is called what?
Are we vulnerable?
What version of Java are we using?

Really? That new/old?

Who has the database credentials?

What can those credentials do?
Where’s Your Policy Now?
What Would Be Better?

- Pervasive
- Explicit
- Automatically Enforced

Let’s talk about enforcement points...

Pervasive means

Resource limits
- CPU
- Memory
- Disk space
- Network usage
- Per instance/total
- Object counts

www.flickr.com/photos/tannershek/7188249991
Pervasive means.

**Workload-to-workload connections**
- Per port, not per container/vm
- Per protocol, not per c/vm
- Automatic bidirectional trust is less secure

Pervasive means...

- Ingress/Egress
- External connectivity and routing
  - (multi-cloud...)

Pervasive means...

- Software components version control
- Deployment

Pervasive means....

- Log access
- Policy editing
- Permissible operations between frontend and backend
What did I leave out?

1. affinity
2. Exception handling
3. Policy for changing policy
4. Compliance state
5. Cleaning policy
Not from your cloud provider

- EC2 instance parameters, network firewall control, network topologies
- RBAC with 3 set roles

“If team members have edit permission, then they can modify instances and also access the instances using ssh. If team members are authorized as an owner, they are also able to create Google Compute Engine resources in the project.”

- checkboxes, oh so many checkboxes

Hopefully your platform?

- nope.
- not yet.
- a few.
- bring it on!
Container Management Systems, The Morning After
Birds-of-a-Feather Session

Wednesday 9:00 pm–10:00 pm
Lincoln 3
Get in Touch!

www.apcera.com

dnb@apcera.com