Full Stack DevSecOps

NIST Virtual Workshop on Improving the Security of DevOps Practices
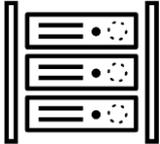21 Jan 2021

John Morello
VP, Palo Alto Networks

3 Dimensions of Cloud Security

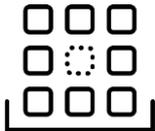Physical - many form factors are used for compute

Spatial - these form factors are present across many different kinds of clouds

Temporal - the apps and infrastructure are continuously looping through lifecycles
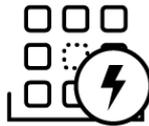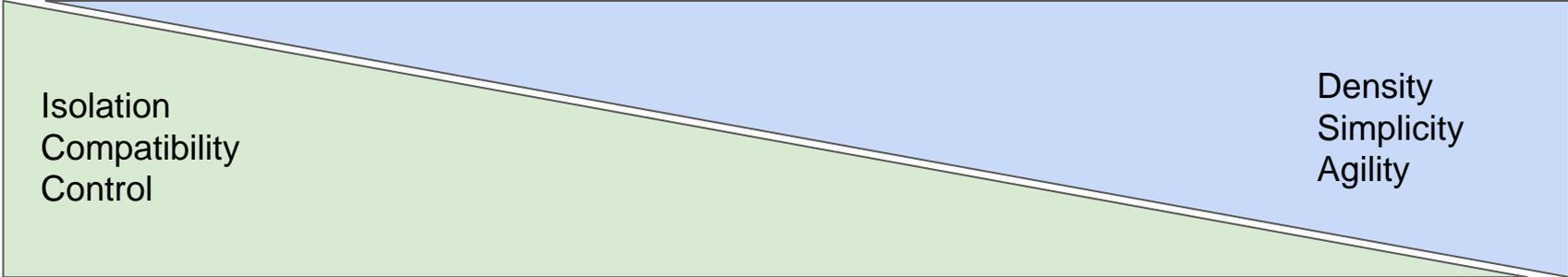
Physical Dimension

VMs

Containers

Containers-as-a-Service

On-Demand Containers

Serverless

Isolation
Compatibility
Control

Density
Simplicity
Agility

Spatial Dimension

Private Clouds
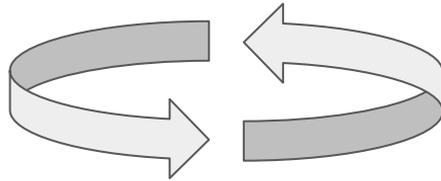
Hybrid Clouds

Public Clouds

Temporal Dimension

BUILD → **SHIP** → **RUN**

Not just the apps - infrastructure as code too

Not linear - a continuous loop

Layered Complexity

Powerful capabilities but potentially extreme complexity as well

Many orgs have an 'all of the above' strategy for choices at each layer, resulting in a nearly infinite set of permutations of app::cloud::lifecycle stage

More important than ever to integrate security into the temporal dimension - make it an inherent part of every build and deployment

NIST's Opportunity

Lots of existing guidance for securing the dimensions… 800-190, 800-144, 800-53

Some guidance can be updated but the biggest need is to tie it together in a deployable pattern reflective of real world architectures

[DevSecOps project](#) can help users navigate this complexity by creating this mapping of guidance

NCCoE can bring the mapping to life by deploying it into labs on common tech stacks and illustrating alignment of the patterns to real world tools