KubeCon CloudNativeCon North America 2026

#KubeCon #CloudNativeCon

No network? No problem! Running K8s nodes in air-gapped VPCs

Shachar Tal, Palo Alto Networks



> whoami

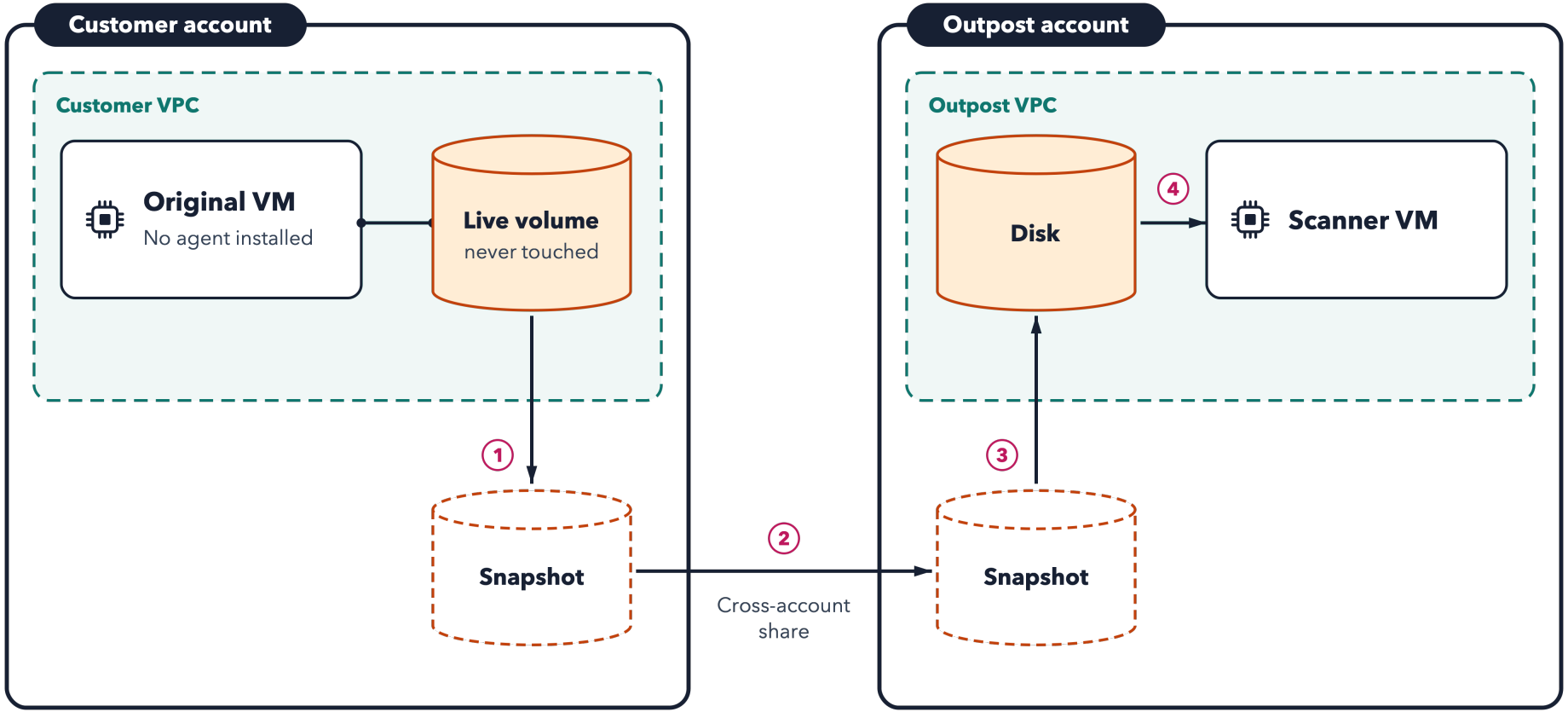


- Sr. Distinguished Engineer at Palo Alto Networks
- Previously: NVIDIA, Cisco
- Actively engaged in Agentic Networking SIG and AI Gateway WG
- Linkedin: https://linkedin.com/in/shachar

Business Case

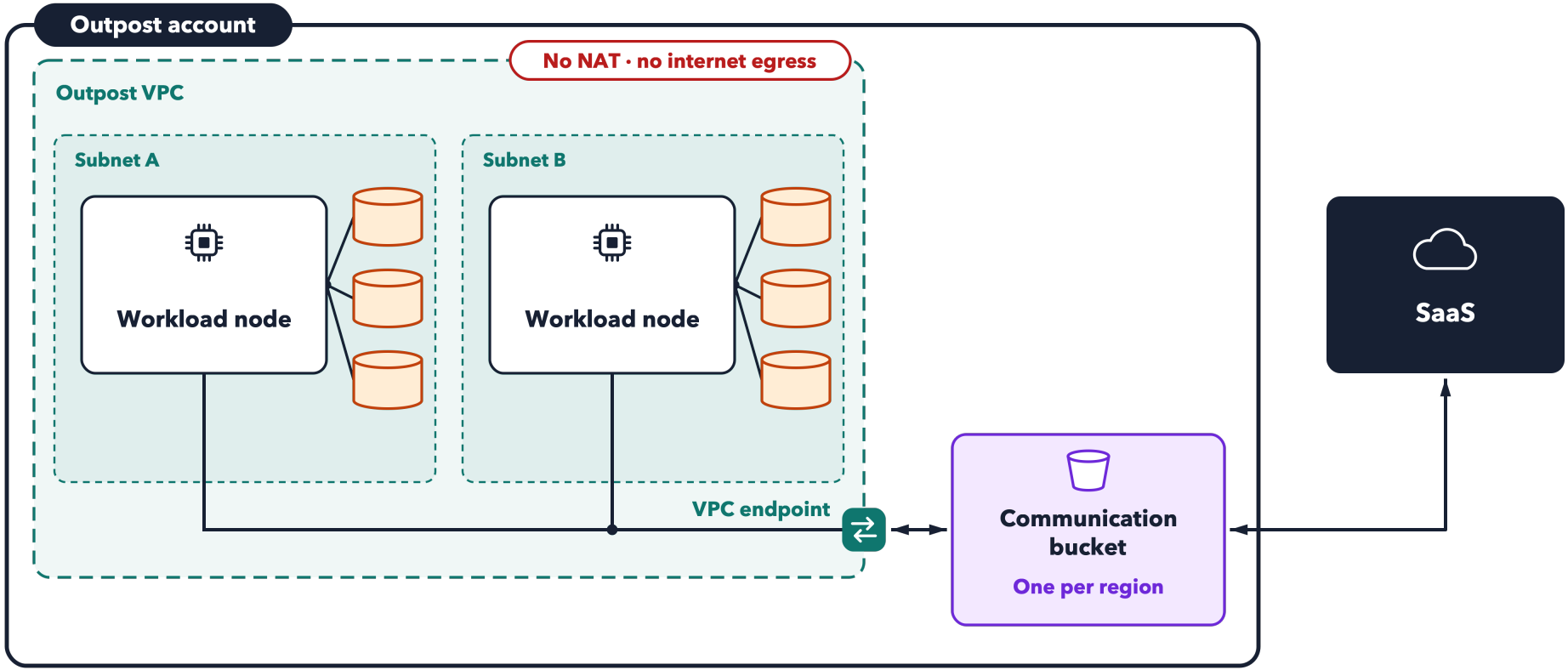
- Scanning Cloud Block Storage
- Operating on VM-attached disks and K8s PVs
- Extracting:
  - SBOM, Vulnerabilities in host OS and container images
  - Malware
  - Compliance issues and misconfiguration
  - Detection and content classification for self-managed databases
  - All things AI:
    - Detection of agent harnesses
    - MCP servers and tool analysis
    - Self-hosted models
    - Prompt/inference/tool logs
    - …

Disk Side-Scanning Workflow

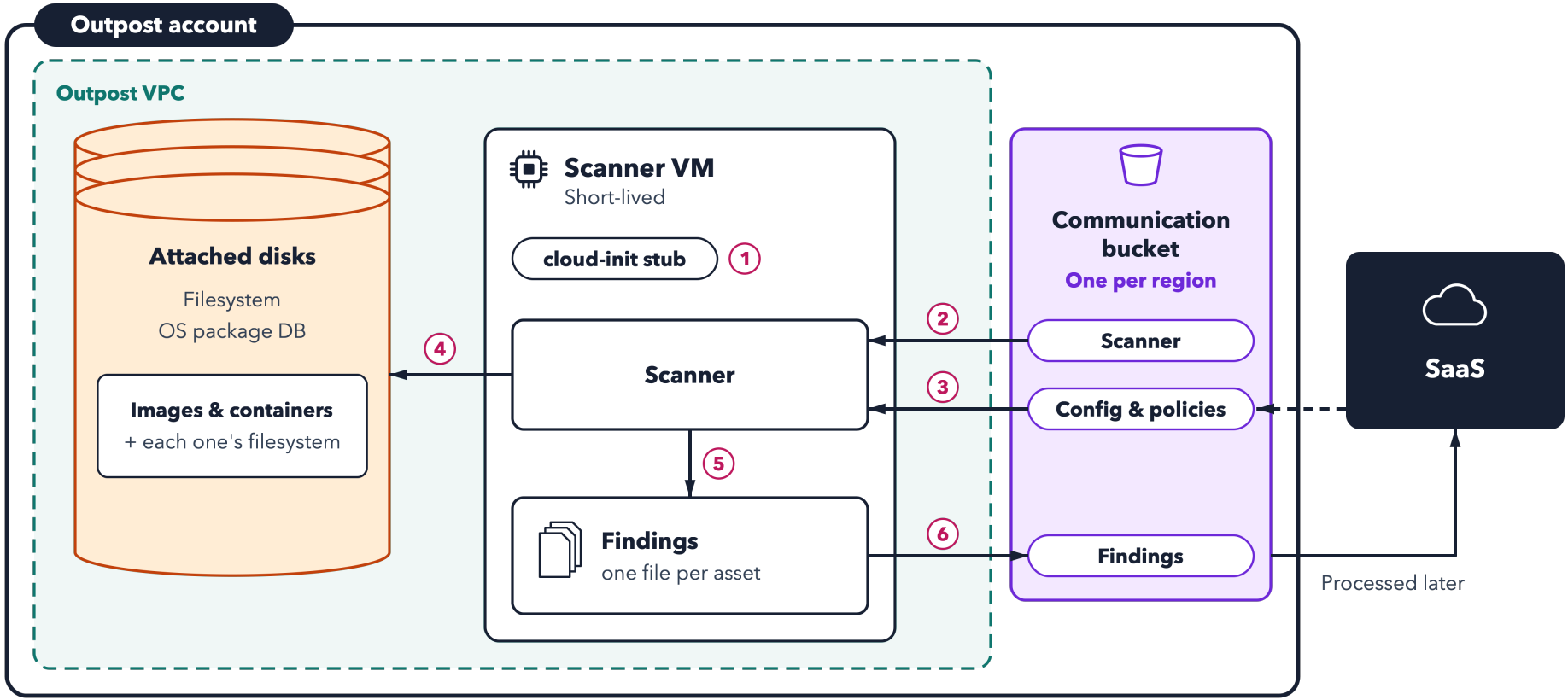


Anatomy of an Outpost

KubeCon CloudNativeCon North America 2026



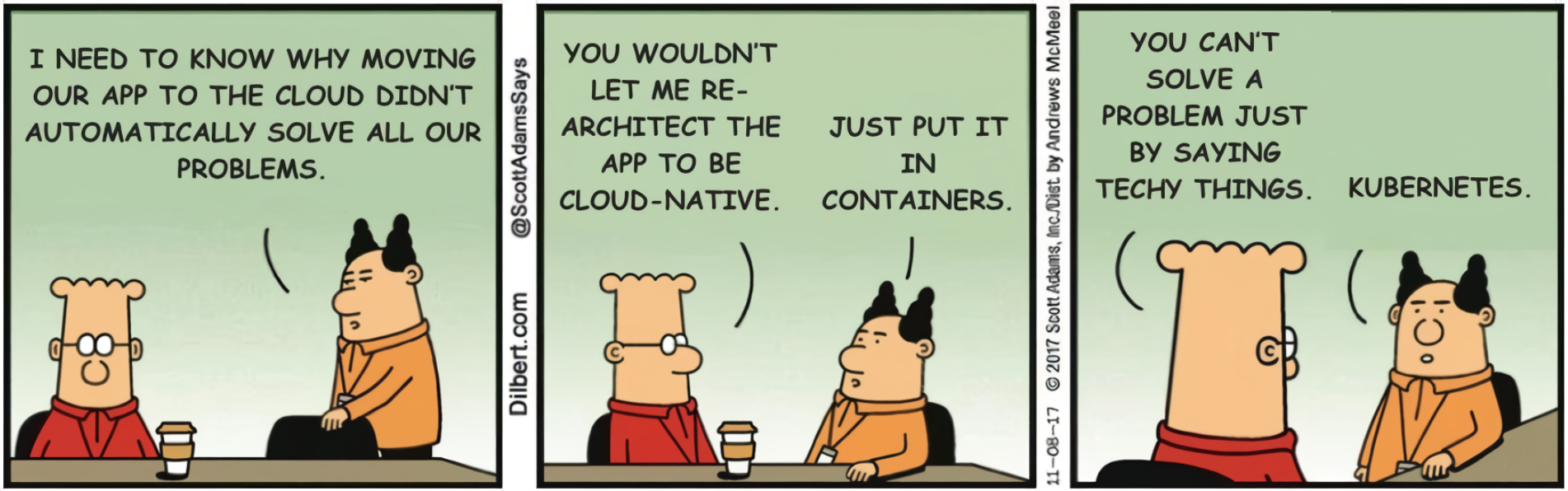
Scan Workflow: How It Started



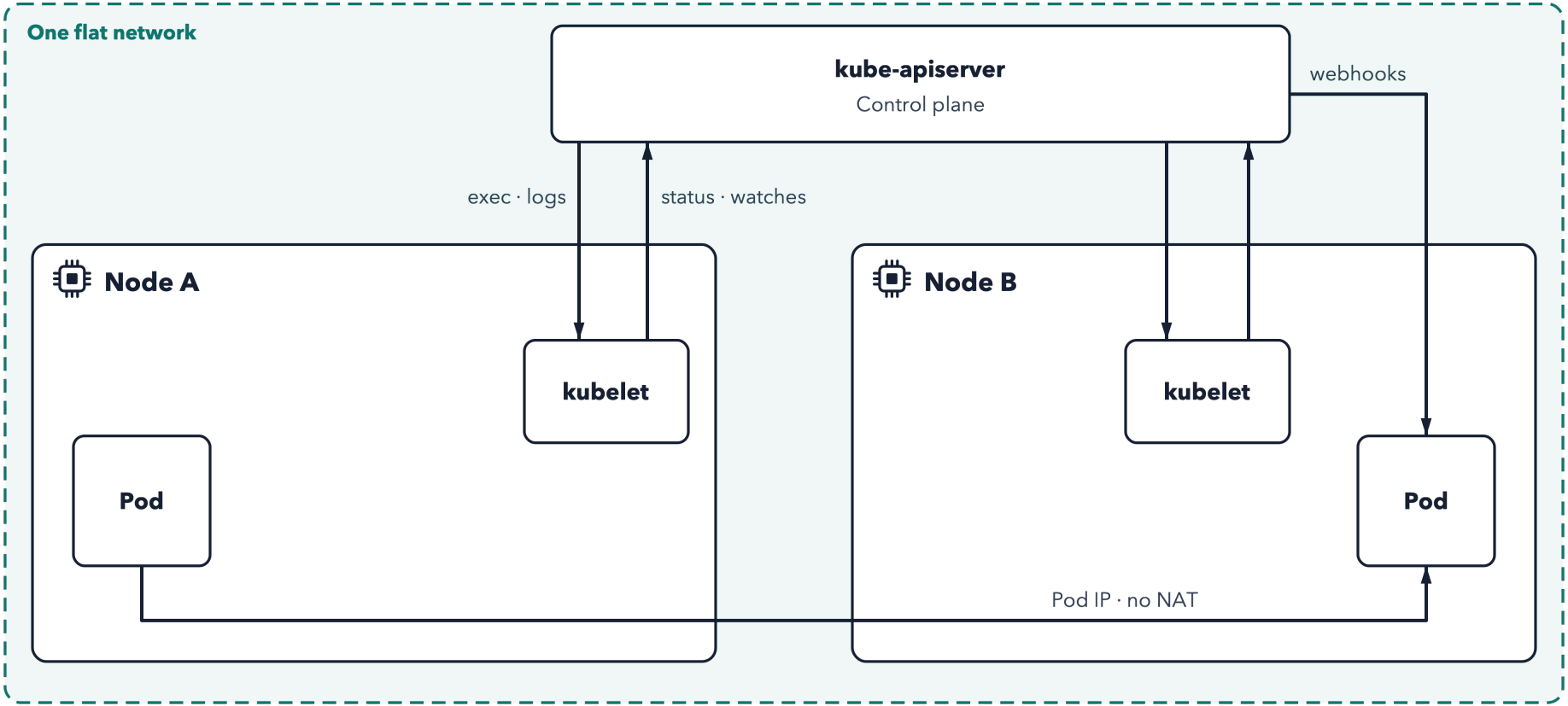
Challenges

- Placement and utilization
- Disk lifecycle
- VM scheduling
- Spot preemption
- Observability delays and gaps
- Troubleshooting

So… What If?

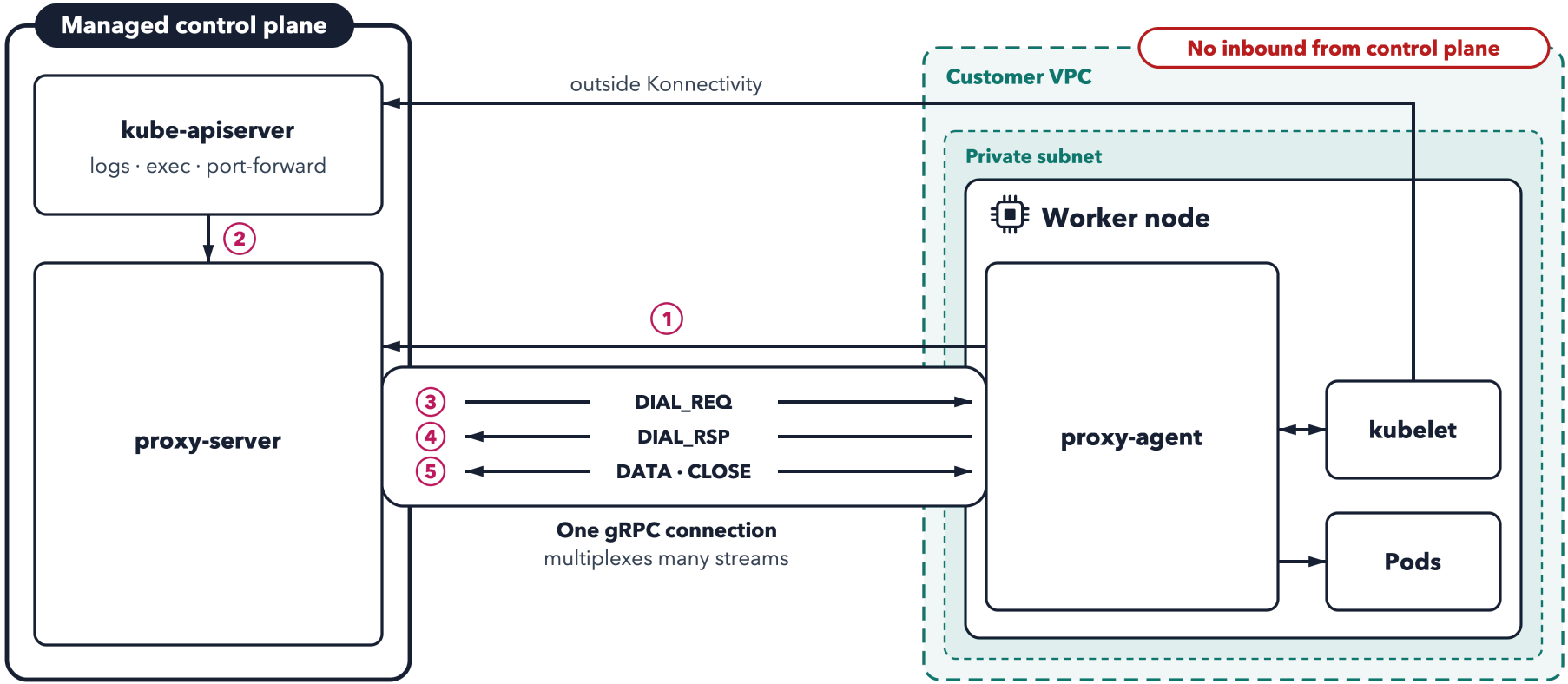

I NEED TO KNOW WHY MOVING OUR APP TO THE CLOUD DIDN'T AUTOMATICALLY SOLVE ALL OUR PROBLEMS.
Dilbert.com @ScottAdamsSays
YOU WOULDN'T LET ME RE-ARCHITECT THE APP TO BE CLOUD-NATIVE.
JUST PUT IT IN CONTAINERS.
11-08-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMeel
YOU CAN'T SOLVE A PROBLEM JUST BY SAYING TECHY THINGS.
KUBERNETES.

Flat Networking Model



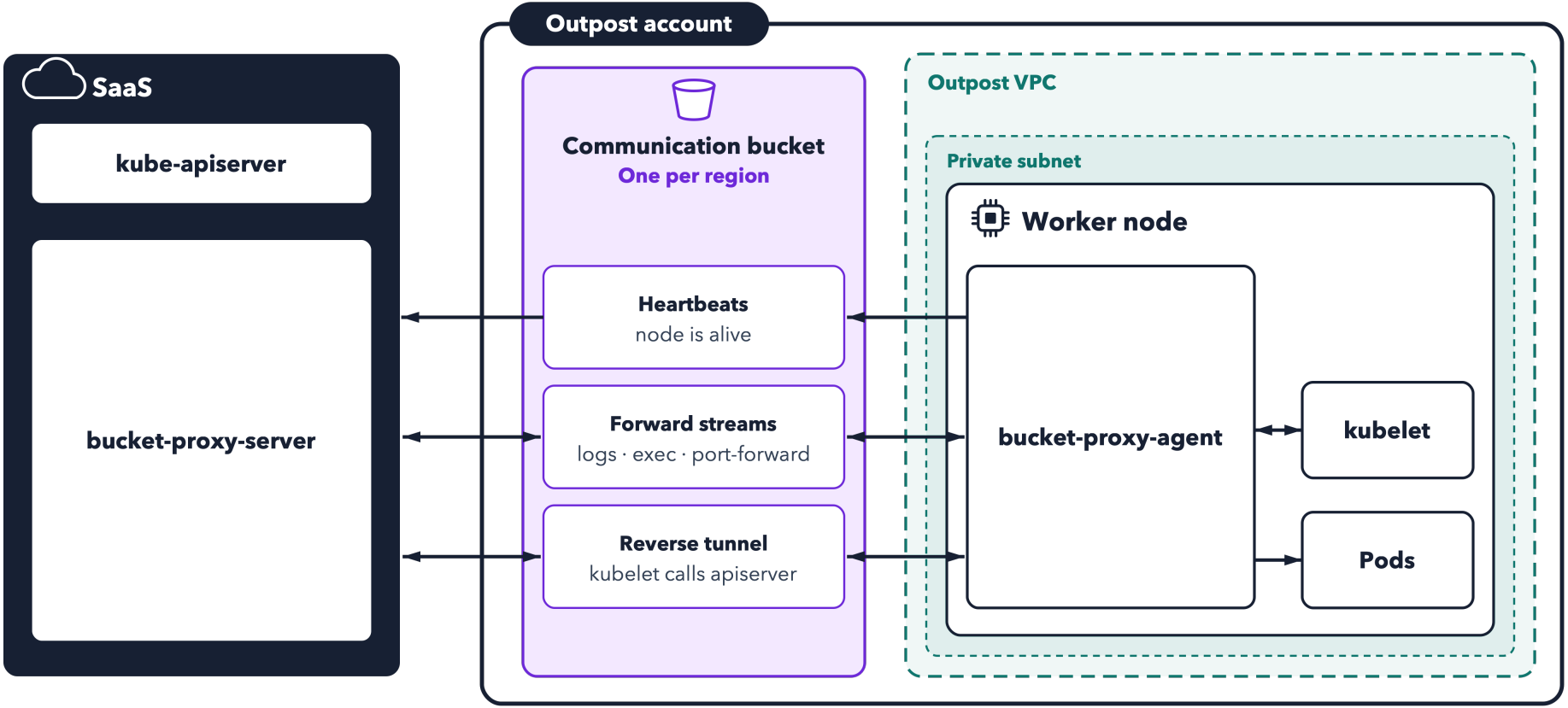
Konnectivity

KubeCon CloudNativeCon North America 2026

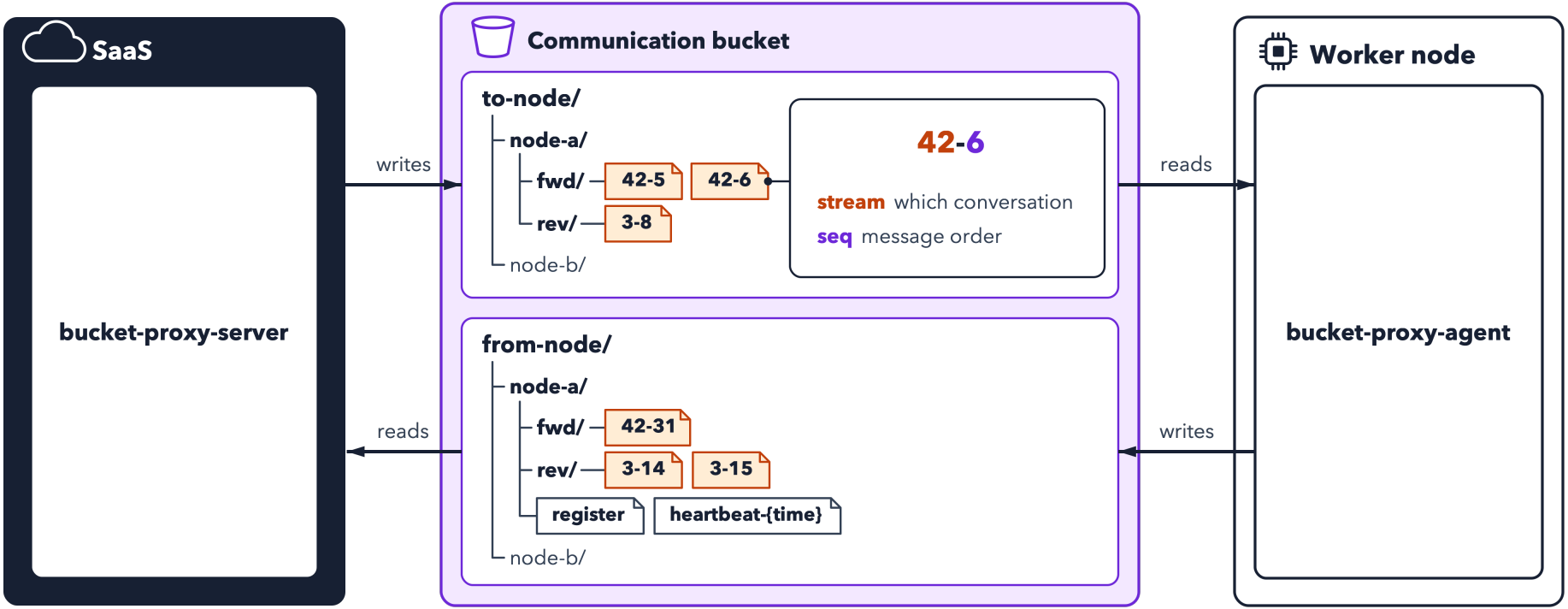


Messaging via Cloud Buckets

KubeCon CloudNativeCon North America 2026

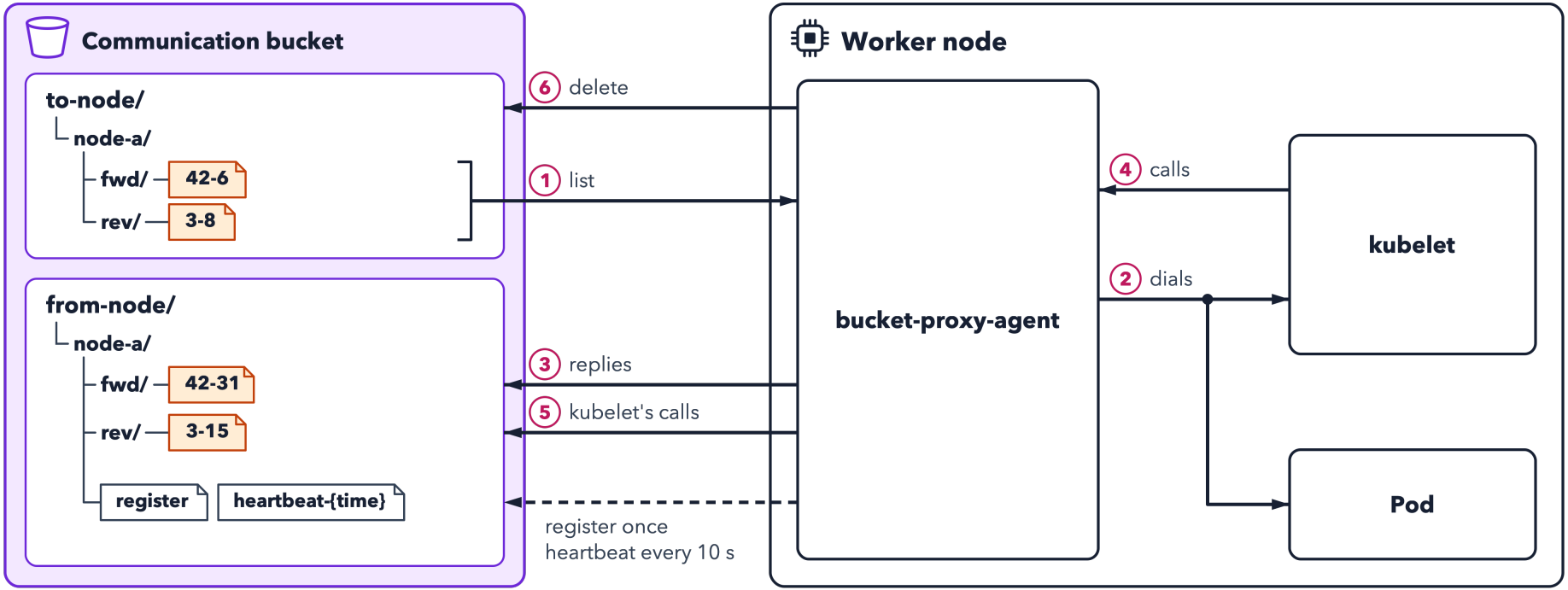


Bucket Layout



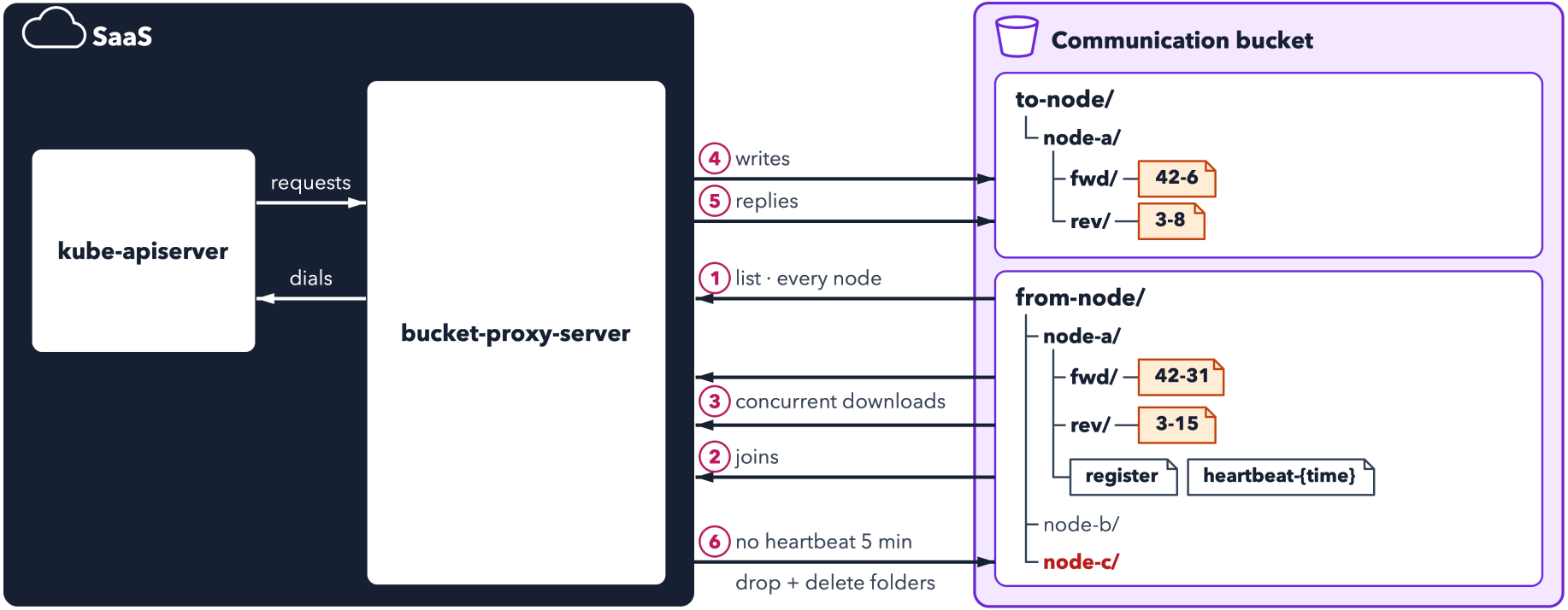
Proxy Agent Flow

KubeCon CloudNativeCon North America 2026



Proxy Server Flow

KubeCon CloudNativeCon North America 2026



Demo

Observations, Costs, Optimizations

- Running control plane as pods (in SaaS cluster)
    - apiserver doesn’t support mixed node topologies via Konnectivity
- CSI plugins remove most application logic around volume lifecycle, placement and snapshot management
- Optimizations:
    - Truncated exponential backoff for polling
    - Server Agent only polls regional buckets where VMs are running
- Cloud bill: ~$5.2 per instance-month
- ~4% of compute resource costs

Project-specific extensions and futures:

- Karpenter for scheduling new VMs based on unschedulable pods
- KEP-6313: Network-Isolated Pod Sandboxes from @aojea (aka “Hermetic Pods”)