Deploying Kubernetes in Classified Environments

Palantir

Speakers

Ali Monfre

Senior Architect, Federal

Vlad Ungureanu

Engineering Lead

Agenda

- Palantir Overview
- Challenges
  - Security & Compliance
  - Infrastructure Constraints
  - SDLC + Incident Response
- Solutions
- Q/A

Introducing Palantir

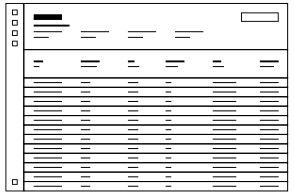
Overview

Palantir builds leading software platforms for data-driven operations and decision-making. We empower government institutions to deliver on their mission and duty for the benefit of the people they represent.

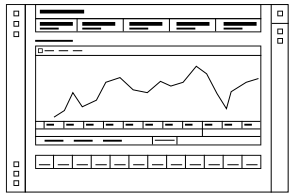
Our Mission

- → Support the world's most critical institutions — in their daily operations and in times of crisis.
- → Deploy data ecosystems that empower users, enhance collaboration, and compound value.
- → Preserve fundamental principles of privacy and civil liberties while using data.

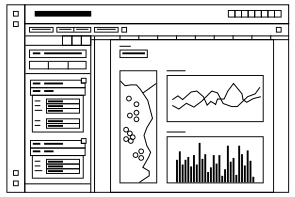
Platform capabilities



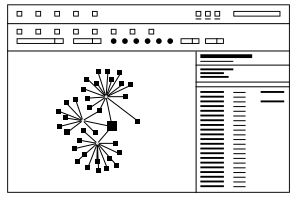
Data Integration, Management, & Security



Analytics, Modeling, & Exploration



Investigative & Case Management Applications



Operational Decision-Making Applications

Our Clients Include

ARMY	AIR FORCE	SPACE FORCE	HHS	NCATS & NC3
CDC	DHS	PEPFAR	NCI	FDA

Challenges

Terminology Overview

- Highside
- Secure Space
- ATO – Authority or Authorization to Operate
- NIST Controls – National Institute of Standards and Technology
- STIG - Security Technical Implementation Guide
- DISA - Defense Information Systems Agency
- SIPR
- JWICS
- SCIF
- CDS
- DTO
- ITAR
- NNPI
- UCNI
- CUI
- NSS
- CMMC
- RMF
- BCAP
- CC SRG
- TS/SCI
- NIPR/SIPR/JWICS

Compliance Challenges

/ 01 **STIGs –** There are many DISA STIGs required if you want to use k8s – OS, k8s, and things that run in the cluster.

/ 02 **Continuous compliance** – It's not enough to satisfy STIGs at accreditation time; STIG scans must be conducted regularly.

/ 03 **Operating System**
- Ex: Logging failed login attempts
- Major vendors have different STIGs published (Canonical / RedHat)
- Lag in STIGs for latest OS versions

/ 04 **Kubernetes**
- Ex: kube-apiserver anonymous auth disabled
- Ex: kubelet readonly port disabled
- k8s distro STIGs available with nuanced checks

Infrastructure Challenges

/ 01 **Overview**
- Hyperscalers have classified regions
- Physically in USA
- Exist for both Secret and Top Secret classifications

/ 02 **Feature Lag –** Features deployed high-side last (~24-36 months)

/ 03 **Capacity Constraints**
- HW capacity errors more frequent highside
- Specialized HW is scarce
- Longer VM lifecycle operation times

/ 04 **No SaaS**
- NO GitLab / GitHub offering
- NO centralized public container image registry
- NO observability provider available
- NO centralized Identify Provider
- Options limited to cloud provider services / DIY

/ 05 **PKI Management**
- Highside regions are air-gapped
- No public DNS registrar
- CAs not included in OS bundles
- All services need access to the CA bundle for TLS connections

COMMERCIAL

New features land in commercial cloud

Secret

New features available

Top Secret

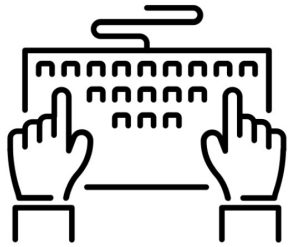
New features available

Palantir

Software Development Lifecycle / Incident Response

/ 01 **SDLC**

- Vulnerability management and virus scanning
- How to transfer software to classified networks
- How to deploy, configure, upgrade software highside
- Running high-side fleet with cleared human operators



/ 02 **Highside Incident Response**

- Operators must share debug info with lowside developers
- No automated mechanism for bringing info lowside
- No SaaS offering highside for observability workflows → bring your own

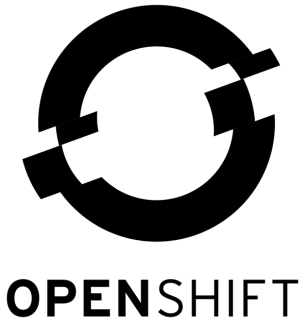
Solutions

Palantir

Compliance Solutions

OpenShift Platform

- Multi-node cluster deployments
- RHCOS (Red Hat Enterprise Linux CoreOS)
- compliance-operator



RKE 2 (Rancher Government)

- Edge / single-node clusters deployments
- RHEL 8

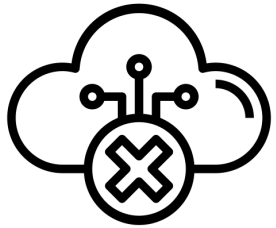
Infrastructure Solutions

PKI management

- Pre k8s we configured the OS CA bundle on every machine
- Built an API that allows pods to request CA material
- Mutate pods during admissions with initContainer + emptyDir
- Solutions like cert-manager can be also used

No reliance on SaaS

- No git / CI system highside -> strongly believe in not developing highside
- Became good at deploying OSS for SaaS highside
- OSS Prometheus
- OSS Keycloak as IdP
- Minimize components needed highside



Software Development Lifecycle Solutions

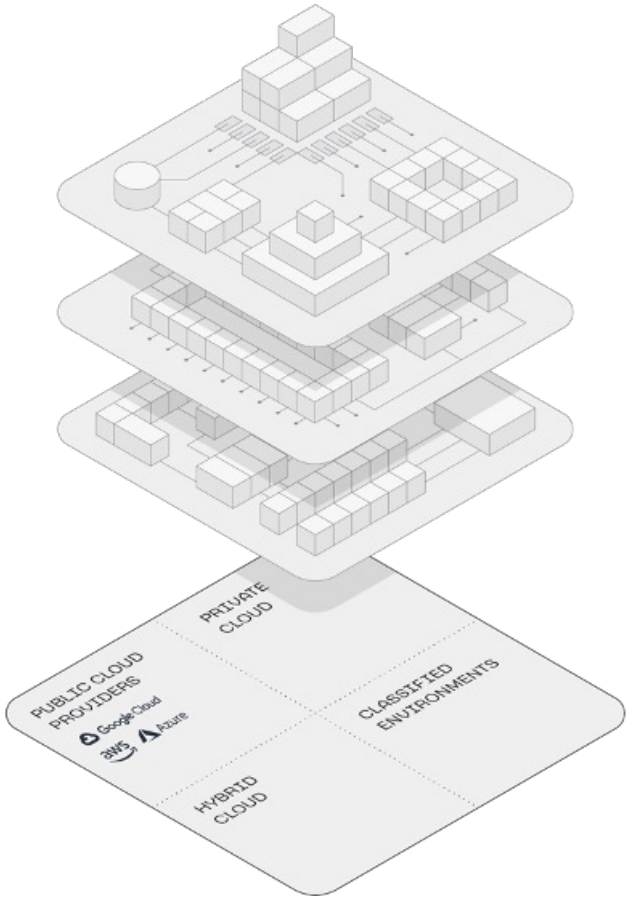
Security & Compliance

- Build software that continuously passes security & compliance requirements
- A strong vulnerability management story is critical
- Maintain internally a golden container image that all software uses
- OCI Artifacts

Cross Domain Solution

- Automated one way data transfer
- Hyperscalers offer CDS as a managed service
- Can be included in ATOs with caveats (e.g., integrity of the data in traffic)
- Reduced transfer times from multiple hours to multiple minutes
- Managing the end-to-end process highly challenging

End-to-End Management and Automation



Apollo

- Configure the environment lowside, mirror it highside
- Intelligent change management controls
- Integration with vulnerability management and scanning infrastructure
- Highside-specific overrides
- Fleet-wide changes, even highside
- Standardized monitoring and alerting

Q&A