# Streamlining FedRAMP Compliance with CNCF Technologies

Palantir

# Speakers

Ali Monfre

Senior Architect, Federal

Vlad Ungureanu

Engineering Lead

# Agenda

- Palantir Intro
- Challenges
  - Vulnerability management
  - FIPS validated crypto
  - Ingress / Egress controls
  - K8s intrusion detection system
- Solutions
- Q/A

# Introducing Palantir

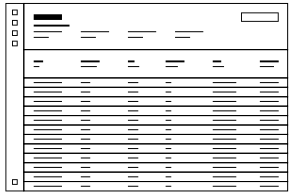
## Overview

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.

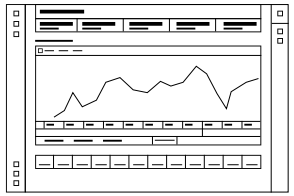
## Our Mission

- → 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.

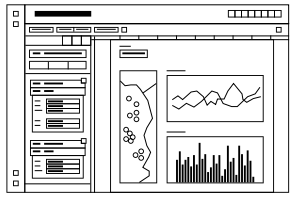
## Platform capabilities



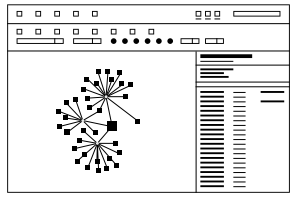
Data Integration, Management, & Security



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 |

# FedRAMP Overview

## 01 Preparation

### Readiness Assessment

*(Optional, but highly recommended)*

- RAR Development
- FedRAMP PMO Review of RAR
- Remediation (if needed)
- FedRAMP Marketplace Designation – Ready

### Pre-Authorization

- Partnership Establishment
- Authorization Planning
- Kickoff Meeting
- FedRAMP Marketplace Designation – In Process

Source: fedramp.gov October 7, 2023

## 02 Authorization

### Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)*

### Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- FedRAMP Marketplace Designation - Authorized

## 03 Continuous Monitoring

### Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment

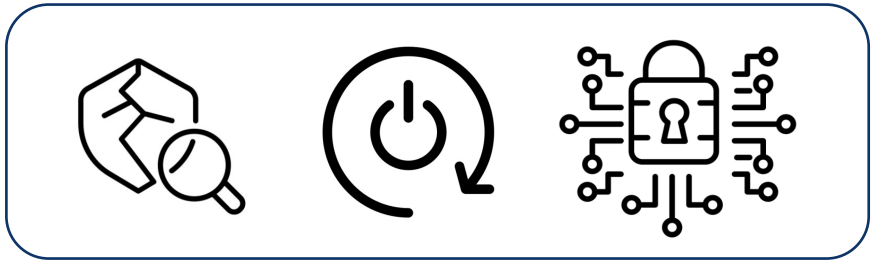
** The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.*

Palantir

# Challenges

# Challenges Pre-Kubernetes

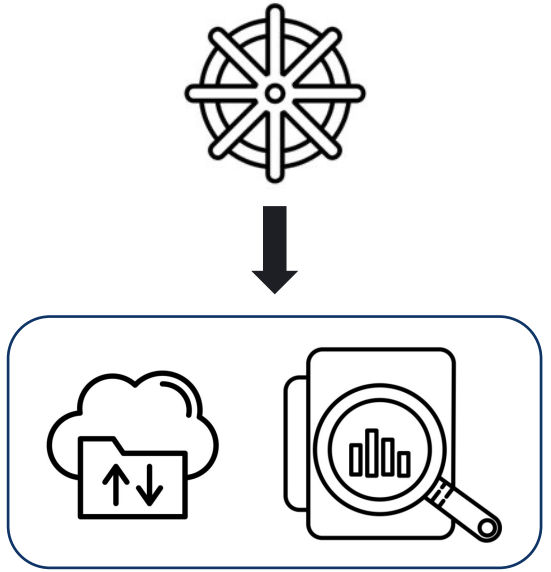
/ 01 **Scanning Requirements**
- Vulnerability scans
- Virus scans
- STIG scans
- Dynamic web application scans



/ 02 **Patching Requirements → constant host reboots**

/ 03 **FIPS Encryption challenging for microservices architectures**

/ 03 **Architectural updates *with* k8s**
- Ingress/egress controls
- Monitoring and incident response



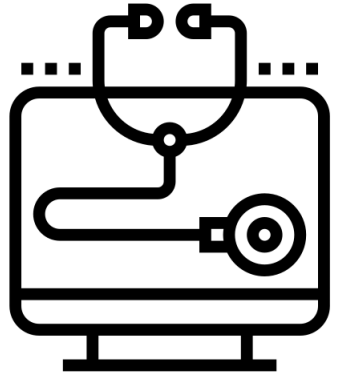
# Solutions

Palantir

# Vulnerability & Compliance Scanning

/ 01 **Operating System**

- Major vendors have different STIGs published (Canonical / RedHat)
- Lag in STIGs for latest OS versions
- Immutable machine image compliance scanned in CI
- 72h host lifecycle



/ 02 **Container Images**

- Internal golden container image used by all products
- Automation to build all downstream images
- Embedded Trivy to run in our SDLC (software development lifecycle)

# FIPS Encryption & Network Security

/ 01 **FIPS**

- Kernel + crypto libraries (e.g., Ubuntu Pro, RHEL, etc)
- NIST long processing times

/ 02 **Cilium**

- CNI of choice in all k8s clusters
- IPSec encryption for pod <-> pod traffic
- Powerful network policy primitives
- Deny by default

# Ingress / Egress traffic

/ 01 North-south traffic encrypted with FIPS validated libraries

/ 02 NGINX+ FIPS validated, but just as commercial offering

/ 03 Envoy is designed for cloud-native applications

/ 04 BoringSSL as TLS provider, FIPS configurable (--define boringssl=fips)

/ 05 Running as forward / reverse proxy

# Incident Response in Kubernetes

/ 01 Host Intrusion Detection System

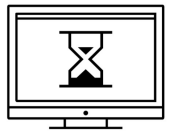
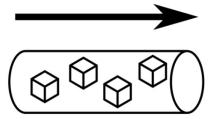
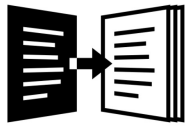
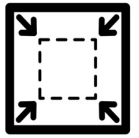
/ 02 osquery – endpoint visibility tool

/ 03 No k8s integration → chaos with multiple pods on the same node

/ 04 Isovalent Tetragon – eBPF visibility natively integrating with k8s & Cilium

/ 05 Process 'malware.out' accessing ‘maliciousurl.com’; which service account launched the pod?

# Continuing Challenges: Apollo and FedStart

| | | | |
|---|---|---|---|
| Change Management |  Feature lag |  |  Policy-based roll-outs |
| Process Controls |  Onerous documentation |  |  Templates |
| Vulnerability Management |  OSS Vulnerabilities |  |  Minimized images |
| Accreditation Process |  Time intensive |  |  Accelerated timeline |

# Q&A