NUTANIX

TechNet Pacific Northwest

PACIFIC NORTHWEST CHAPTER AFCEA

Nutanix Kubernetes Platform

DevSecOps to the Tactical Edge

Delivering Kubernetes, AI, and Zero Trust Security to the Tactical Edge and Beyond

From Garrison, to IL6 and DDIL Training & Simulation Operations

March 2026

PRESENTED BY: Bill Kalogeros
Nutanix Cloud Native - NKP Modern Applications and Data
bill.kalogeros@nutanix.com

NUTANIX

CNCF Annual Cloud Native Survey: The infrastructure of AI's future

CNCF ANNUAL CLOUD NATIVE SURVEY

66% of organizations use Kubernetes to host generative AI workloads.

CNCF ANNUAL CLOUD NATIVE SURVEY

82% of container users deploy Kubernetes in production, up from 66% in 2023.

CNCF ANNUAL CLOUD NATIVE SURVEY

Cloud native adoption reaches 98% across surveyed organizations.

CNCF ANNUAL CLOUD NATIVE SURVEY

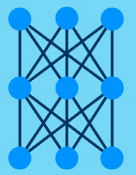
Cultural changes with the development team ranks as the #1 challenge for deploying containers (47%), surpassing technical concerns.

CNCF ANNUAL CLOUD NATIVE SURVEY

Container usage in production applications increased from 41% (2023) to 56% (2025).

CNCF ANNUAL CLOUD NATIVE SURVEY

47% of organizations deploy AI models occasionally, with only 7% deploying daily.



CNCF ANNUAL CLOUD NATIVE SURVEY

52% of organizations don't build or train their own AI models - they're consumers.

CNCF ANNUAL CLOUD NATIVE SURVEY

GitOps adoption jumps from 0% among cloud native explorers to 58% among cloud native innovators.

CNCF ANNUAL CLOUD NATIVE SURVEY

CI/CD adoption reaches 91% among mature organizations, making it the most fundamental practice.

CNCF ANNUAL CLOUD NATIVE SURVEY

74% of cloud native innovators check in code multiple times daily vs. 35% of explorers.

CNCF ANNUAL CLOUD NATIVE SURVEY

59% of organizations use cloud native for much or nearly all development (up from 54% in 2023).

CNCF ANNUAL CLOUD NATIVE SURVEY

Infrastructure sustainability emerges as a critical concern with machine-driven automated usage.

Copyright © 2026 The Linux Foundation | January 2026. This report is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International Public License.

Please cite this research report when using the infographics. See guidance on the report's back page."

KUBERNETES

NUTANIX

Kubernetes can be complicated… Kubernetes adoption creates new challenges if automation is not included in the deployment strategy

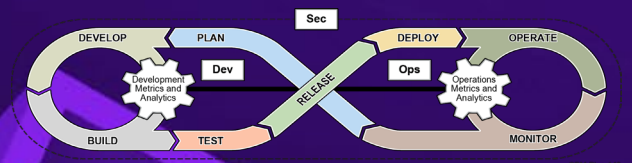
Limited Resources Create Ops Challenges Without Automation – Adding VMs makes it more challenging

- Managing Container Drift & Container Security
- Maintaining the ATO
- Maintaining Day-2 Operations
- Maintaining a Zero Trust Container Environment
- Mitigating Zero-Day Container Attacks

Example:

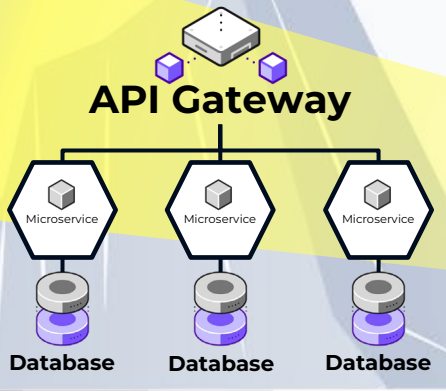
PEO-STRI Mission Focus in Modern Warfare

- Advanced Modeling & Simulation (M&S)
- Synthetic Training Environments (STE)
- Live-Virtual-Constructive (LVC) Integration
- Cyber-secure, scalable DevSecOps pipelines
- Multi-Domain Operations (MDO) & JADC2
- IL6 + DDIL environment readiness



NUTANIX

Unmasking the Complexity: The Hidden Challenges of Microservices



Developer

RBAC | Hardening
Image Scanning | Multi-Tenancy

Security Engineer

Scalability | Reliability
Performance | Observability

SRE

Kubernetes | DevEx
Self-Service | Automation | CI/CD

Platform Engineer

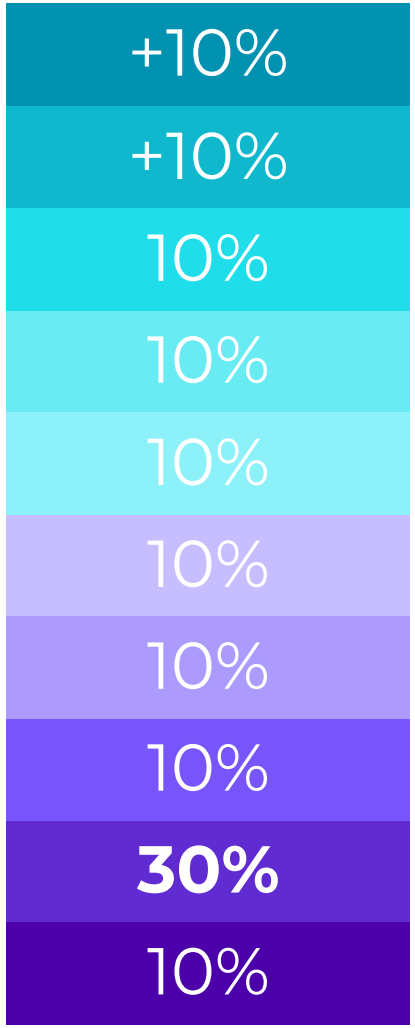
SQL | NoSQL | Performance
Self-Service | Patching | Data Protection

Database Admin

Location | Hardware | Storage
Scalability | Resource Optimization | Performance

Cloud Admin

What Does It Take to Build a Kubernetes Platform?



Container Registry

DevEx (Software Factory)

Application Networking

Security & Compliance

Observability

Multicluster & Multicloud Management

Distributed Storage & Data Services

Cluster Networking

Kubernetes

Infrastructure

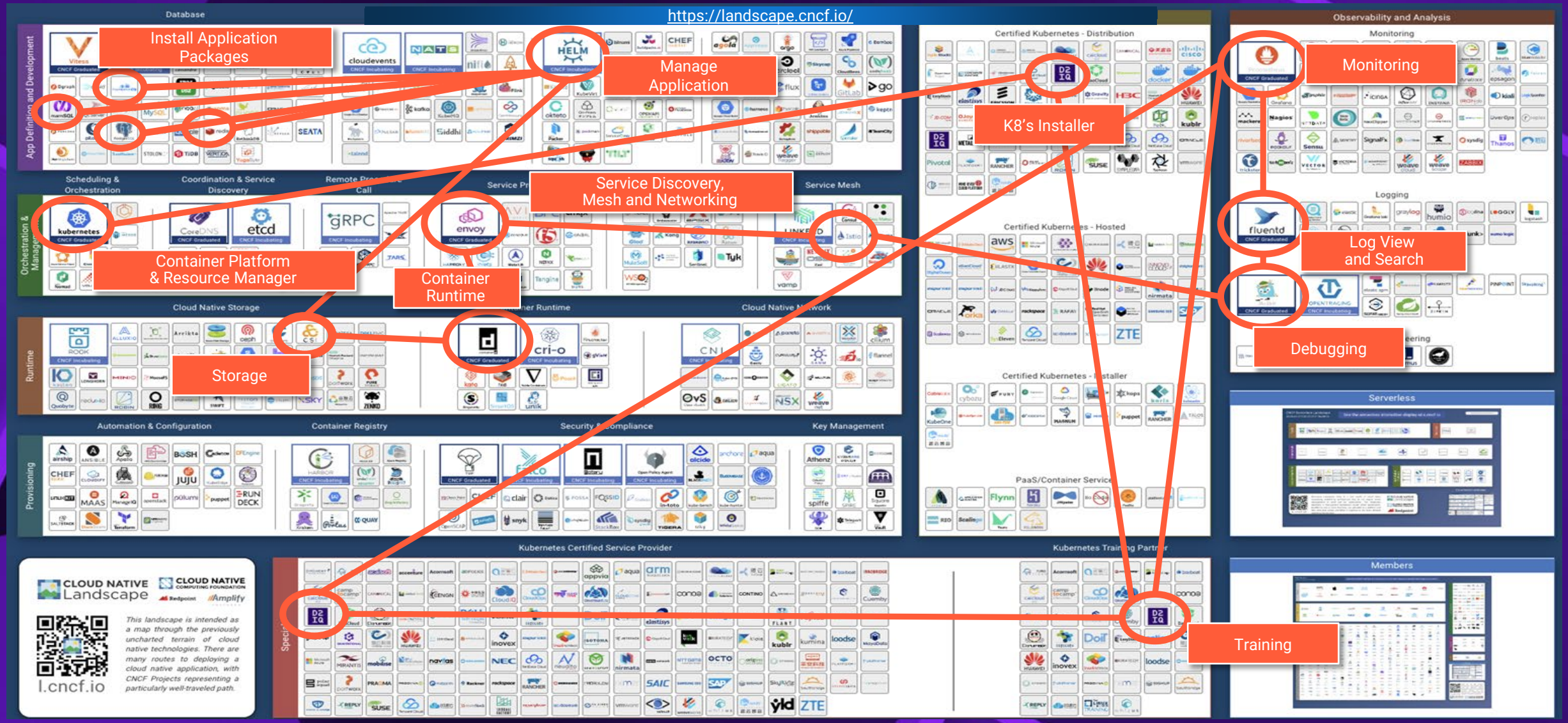
WHAT'S A KUBERNETES?

NUTANIX

© 2023 AccuKnox

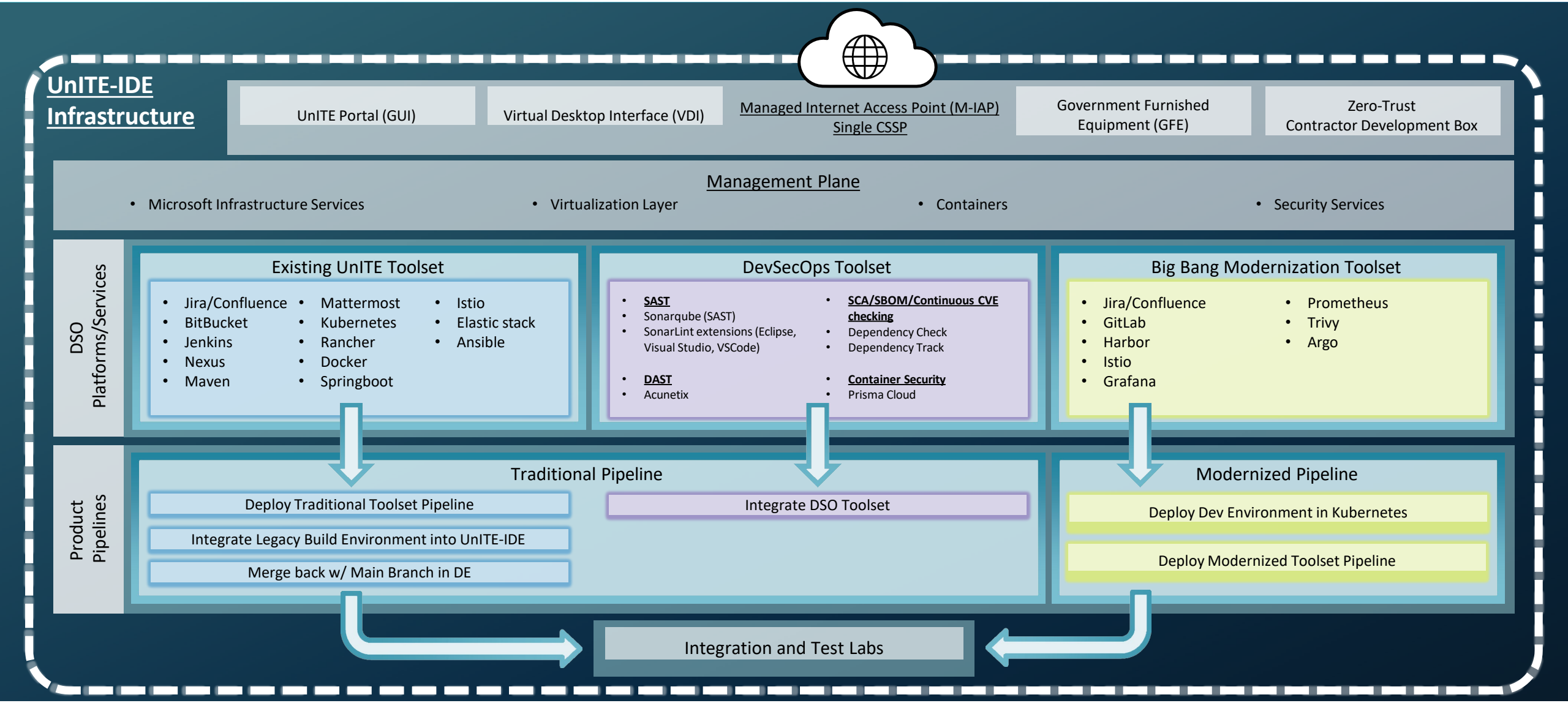
It’s really like building a Kit Car – If You don’t know how to build it, there’s going to be issues. You may be a great transmission mechanic, but that doesn't mean you can build a car.

Kubernetes Is Complex—And It's More Than Just Kubernetes

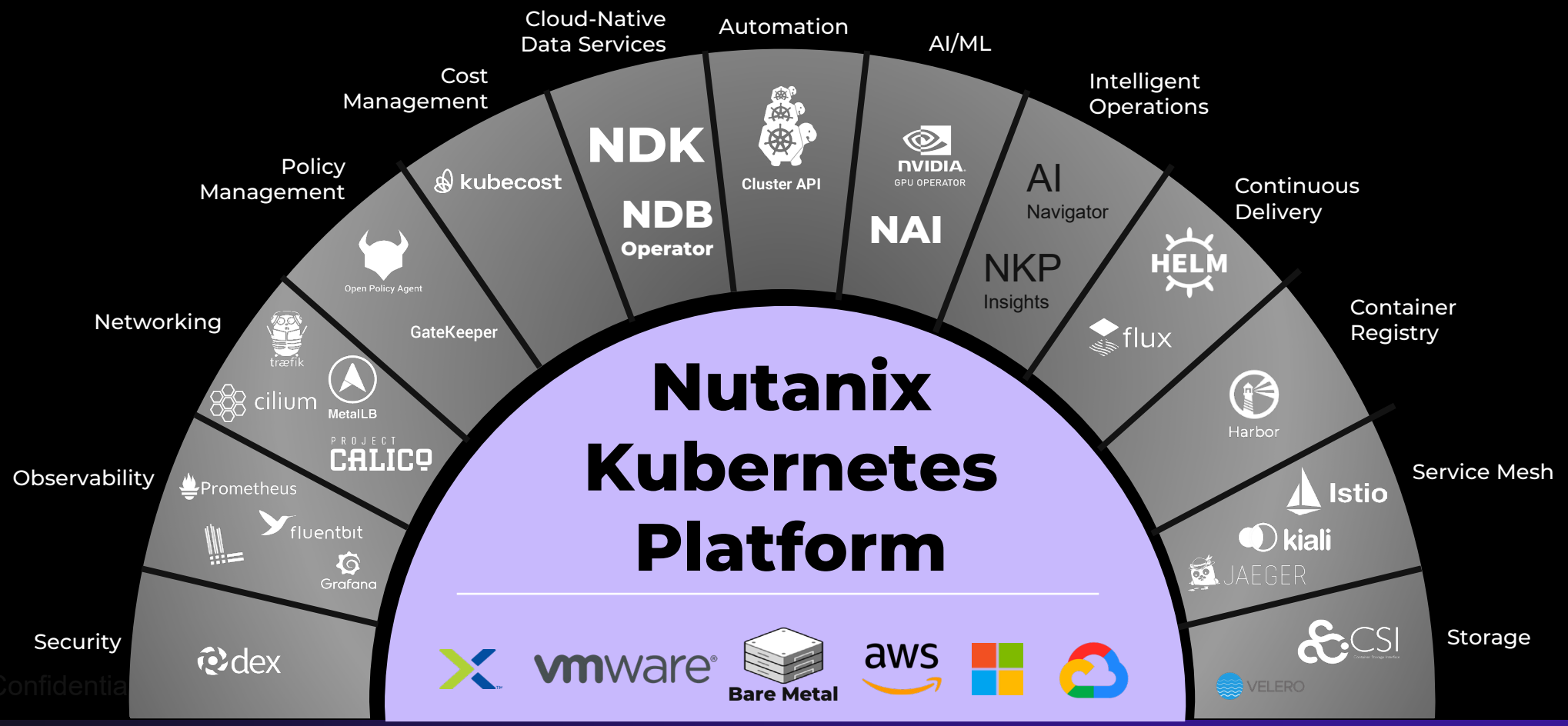


And building that stack can be overwhelming…
More projects are being added all the time!

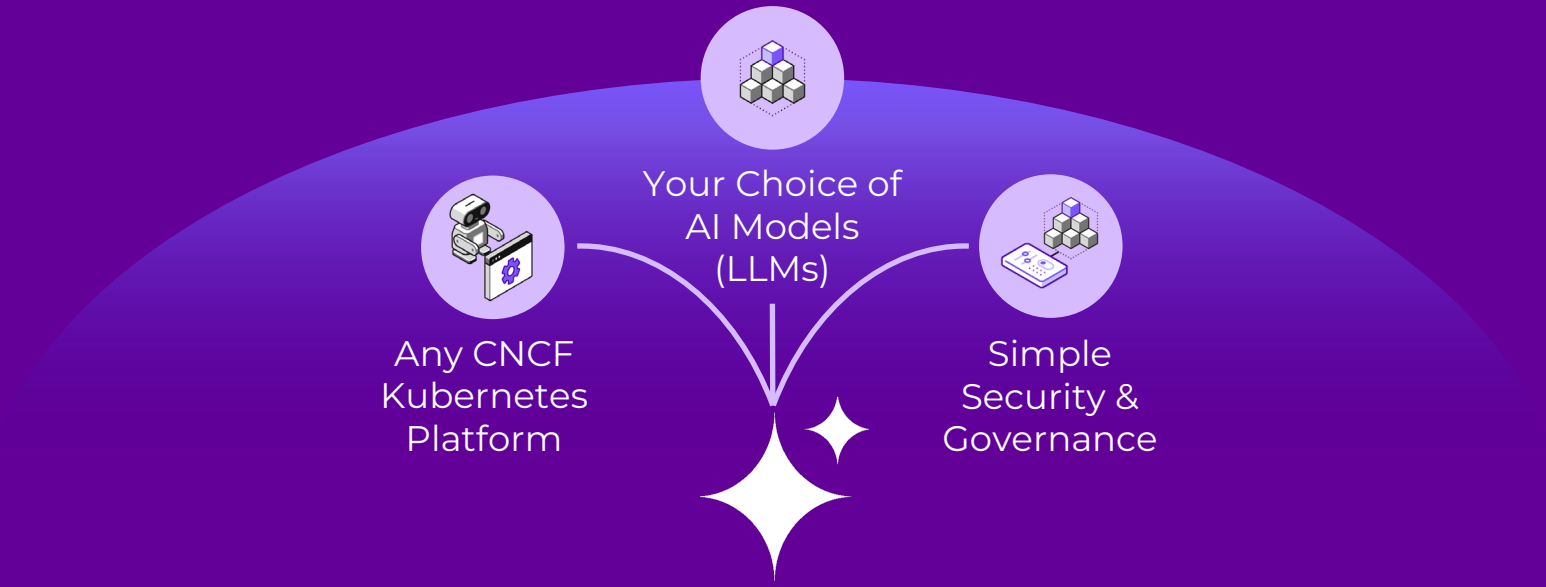
UnITE Platform Conundrum:
3 Separate Environments – Redundant Toolsets & Inefficiencies



Consolidate and master your cloud native operations Deploy, Secure, Manage and Upgrade: Cloud Native Stack at Scale. Infrastructure Agnostic – Deploy on existing infrastructure (Compute, Storage, Network). Works with existing vanilla K8s — no rip-and-replace



Nutanix Enterprise AI Delivers Key Benefits



Simplicity

A clean, easy interface for AI model selection and deployment for running GenAI applications.

Control

IT admins are enabled for AI operations to control application access, endpoints, and AI models.

Cost

Ensure predictable total cost or ownership (TCO) from running AI on-premises, or in public clouds.

AI Factory with Nutanix Enterprise AI

AI and Modern Apps

Core Infrastructure

Deploy & Build GenAI Apps

NVIDIA AI Enterprise & NIM

Nutanix Enterprise AI

Enterprise Model Repository | Choice of LLMs | Secure Endpoints

Nutanix Kubernetes Platform

Simplified Operations | Flexible Deployment | Consistency

Hardware Platform + Storage

Secure Infrastructure | Resilient Storage | Hyperconvergence

Nutanix Agentic AI Solution

Platform Eng

Data Scientist

Model aaS | Agentic Apps | Physical AI

NVIDIA AI Enterprise (Nemotron / Omniverse / OpenShell)

AI Services & Kubernetes Platform

Nutanix Kubernetes Platform, AI Catalog
Nutanix Enterprise AI, Nutanix Database Service, Nutanix Data Hub

Infrastructure Optimization & Security

NVIDIA Topology Aware AHV Hypervisor,
Flow Virtual Networking & Security on DPUs

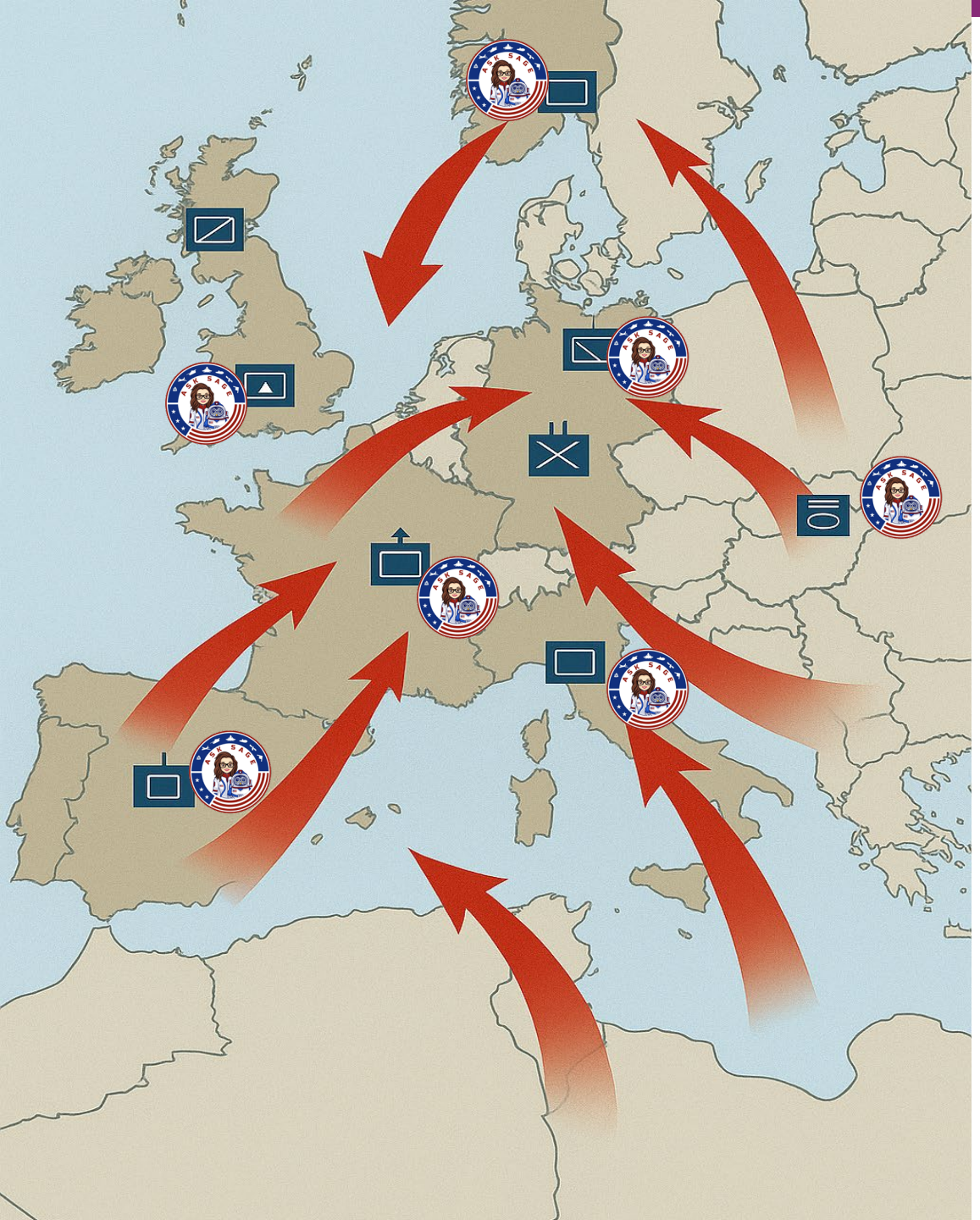
Infra Admin

Agentic AI Dev

CPUs, GPUs, DPUs, Networks

Data Infra
Nutanix Unified Storage

Soldier Digital AI Assistant - Powered by DDIL Ask Sage Appliance



Ask Sage: GenAI at the Edge

The Ask Sage Edge solution is a turnkey field-deployable offering specifically developed for military operations in DDIL and disconnected environments such as FOB's, Vessels/Craft/Mobile Units, or Remote Command Centers. **Powered by Nutanix NKP,** Nvidia and HPE, Ask Sage can now deliver Enterprise grade Gen AI on the go or at the edge empowering the soldier and automating tasks.

- Fully Functional Disconnected Generative AI in a box model
- Utilize local data and data tied to specific commands
- Reap the benefits and efficiencies of LLM tuned to edge operations and functions
- Automate mundane soldier tasks for optimized and standardized output
- Utilize all localized records, manuals, maintenance, logs, images to a single secure appliance for Ask Sage to utilize in its GEN AI models

Accelerating AI: Edge to Multicloud on NKP

Nutanix at the Core: AI-ready infrastructure for training models or for customizing cloud-built LLMs – with data sovereignty **running on NKP**

Nutanix in Public Cloud: Consistent infrastructure with public cloud to access LLMs – with data sovereignty **running on NKP**

Retrain across cores

Retrain to cloud

Retrain with core

Retrain with core

Retrain to cloud

Core

Core

Public Cloud

Edge

Edge

Edge

Nutanix at the Edge: Ideally suited to run compact, customized AI inferencing in small, untethered edge locations **deployed on NKP**

Science and Engineering Challenges

- Multi-functional Sub-systems
- Extensible Architectures
  - New modalities
  - Interoperability with on-orbit systems
  - Commercial / Dual-use systems
- Technology Refresh
  - Software-upgradeable systems
  - Backward compatibility
- Distributed Intelligence
  - Autonomous operations
  - On-board AI/ML
- Life-cycle Management
  - Space-hardened systems
  - Rapid maneuvering for exigent operations
  - De-orbit and replenishment


SOFTWARE FACTORY
NUTANIX
NKP
GROUND CONTROL STATION
PRYON AI
AI
ACCUKNOX
ZERO TRUST SECURITY
ZERO TRUST SECURITY
TACTICAL EDGE
DDIL / DISCONNECTED ENVIRONMENT

USE CASES

NUTANIX

Nutanix Confidential

Mission Context

NUTANIX

System Integrator and Government Objectives:

- Accelerate DevSecOps delivery across IL5/IL6 environments
- **Rapid Prototyping for new program development**
- Enforce Zero Trust security from development through deployment
- Ensure continuity from software factory to tactical edge
- Achieve unified management across domains and platforms
  - Unified, multi-domain operations: lab, cloud, tactical

Examples of Key Programs Supported:

- F-35, C2BMC, GWS, CHIL, THAAD, SBX, 1LMX, MQ-9

Field-Proven IL6 & Tactical Deployments

Why NKP is Built for Mission Assurance:

- Operational in IL6 classified environments and forward-deployed edge
- Integrated with Dell, and any ruggedized tactical compute
  - NKP is Hardware Agnostic
- Hardware/Infrastructure independent
- Supports disconnected, air-gapped lifecycle workflows
- Deployed in support of ISR, missile defense, and joint C2 operations

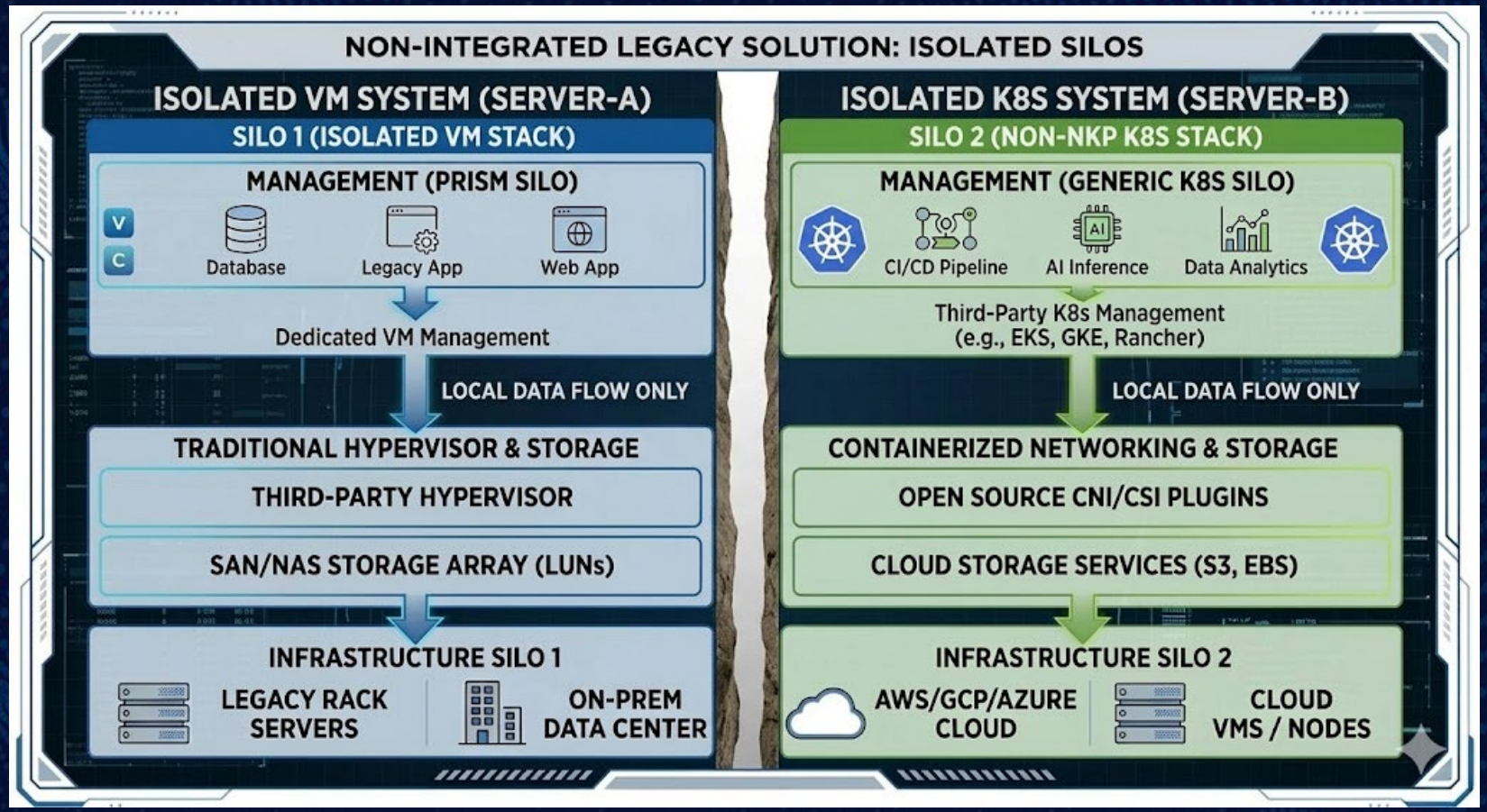
Zero Trust with Built-in Runtime Enforcement - NKP & AccuKnox KubeArmor:

- eBPF-based process-level runtime policy enforcement
- Kubernetes-native identity, RBAC, and system call controls
- Full STIG alignment with real-time audit telemetry
- Supply chain SBOM validation and drift detection

Problem Set: Running VM Application & K8s Forward Deployed

Non-Integrated Systems:

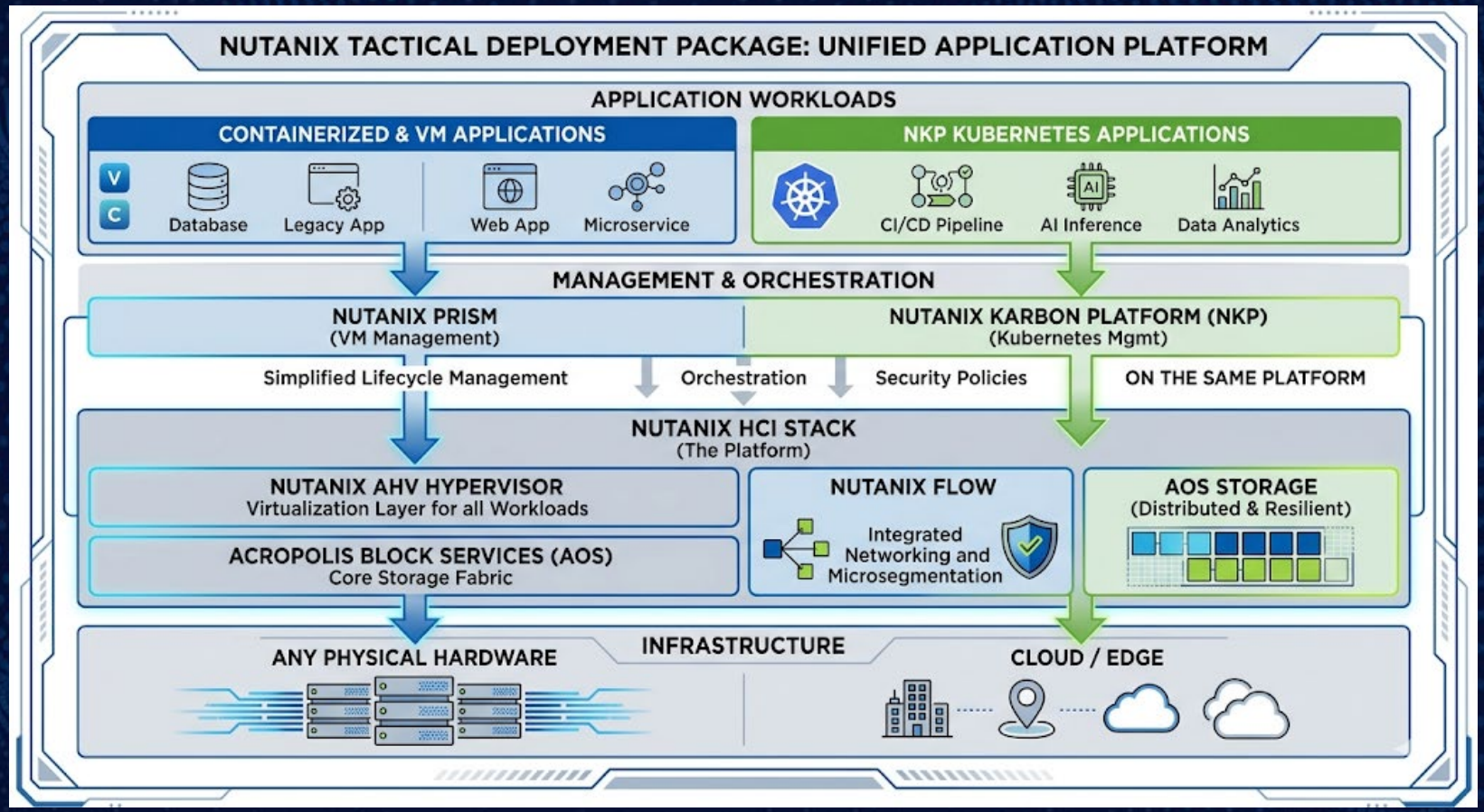
- VM Applications have to run in an isolated silo/platform
- K8s must run on a separate server
- Doubles the HW resources and storage



Problem Set: Running VM Application & K8s Forward Deployed

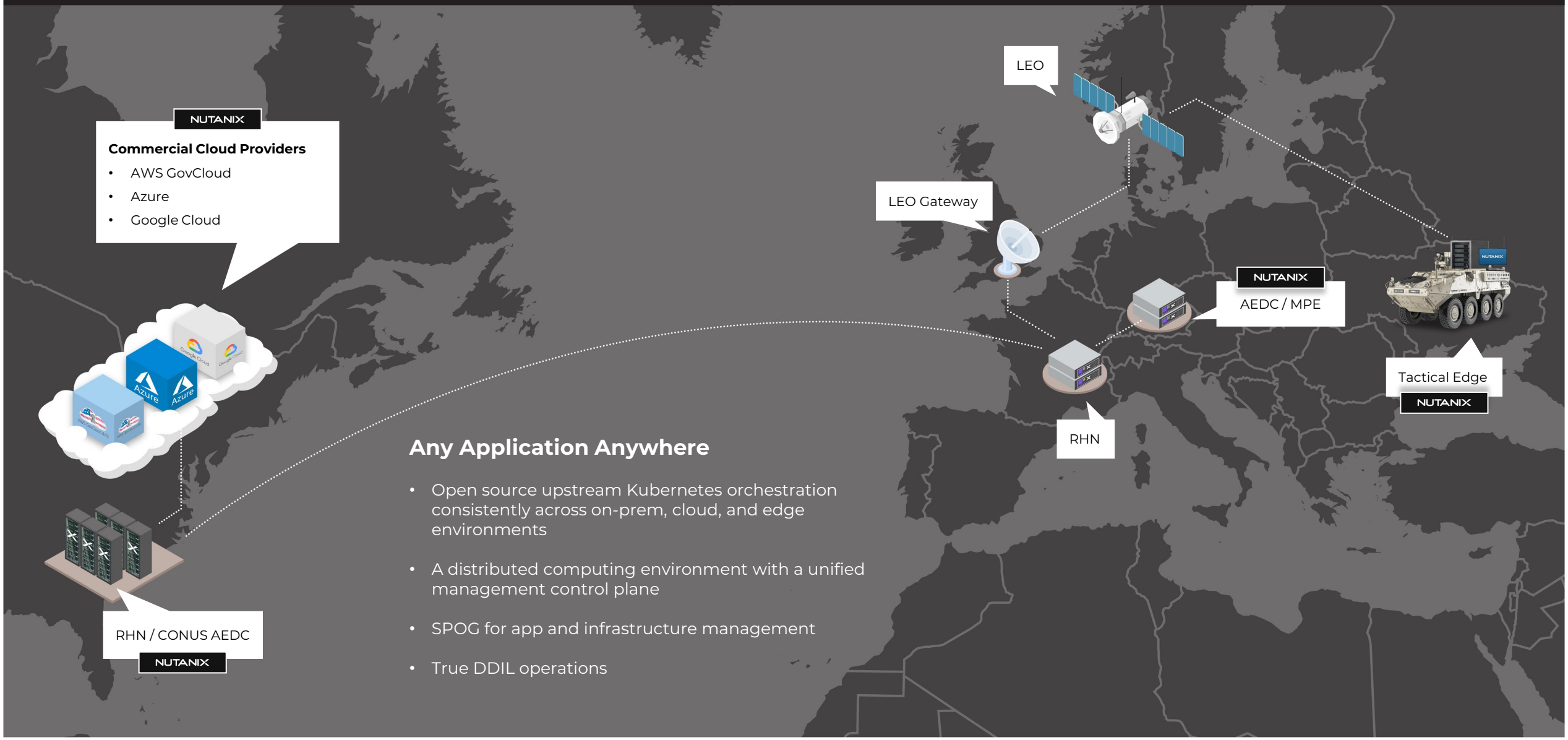
Fully Integrated Nutanix System:

- VM Applications and K8s are running on the same deployed HW package
- Storage and services can be shared, saving power, and SWAP
- **Hardware agnostic**



Next-Generation Command & Control with Nutanix: From Cloud to the Tactical Edge

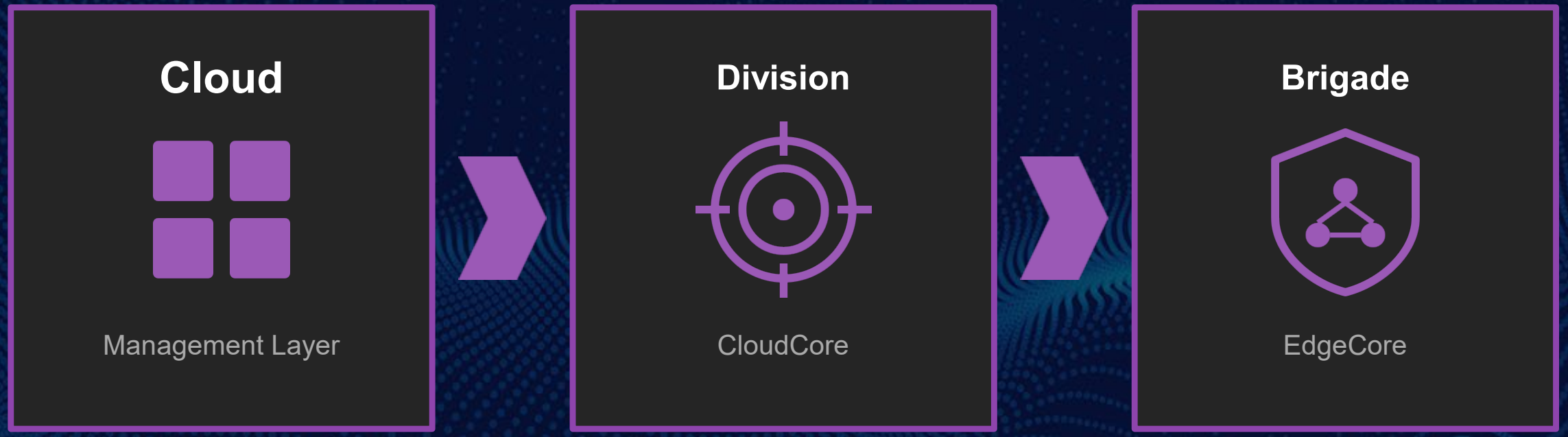
NUTANIX



Any Application Anywhere

- Open source upstream Kubernetes orchestration consistently across on-prem, cloud, and edge environments
- A distributed computing environment with a unified management control plane
- SPOG for app and infrastructure management
- True DDIL operations

Normal Operations – All Connected



HQ OPERATIONS

- Central policy management
- Global orchestration
- Fleet visibility

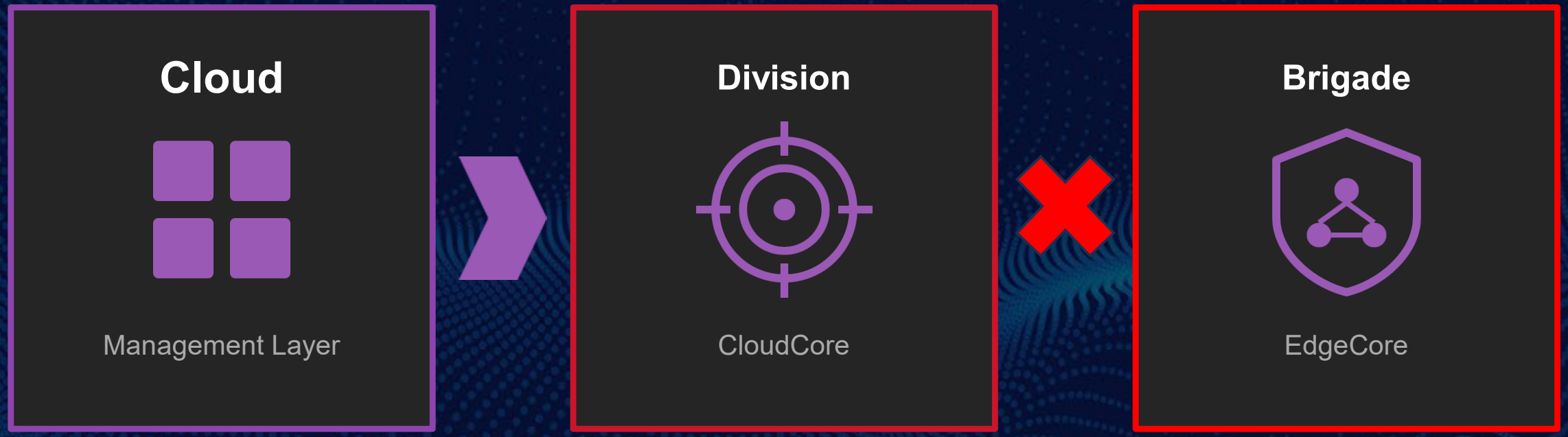
COMMAND POST

- Regional control plane
- Edge cluster management
- Bidirectional sync active

EDGE NODES

- Receives configuration updates
- Sends telemetry upstream
- Workloads running normally

DDIL Scenario 1 – Edge Disconnected



HQ OPERATIONS

- Maintain HQ-Command link
- Aware of edge disconnect
- Policy updates queued

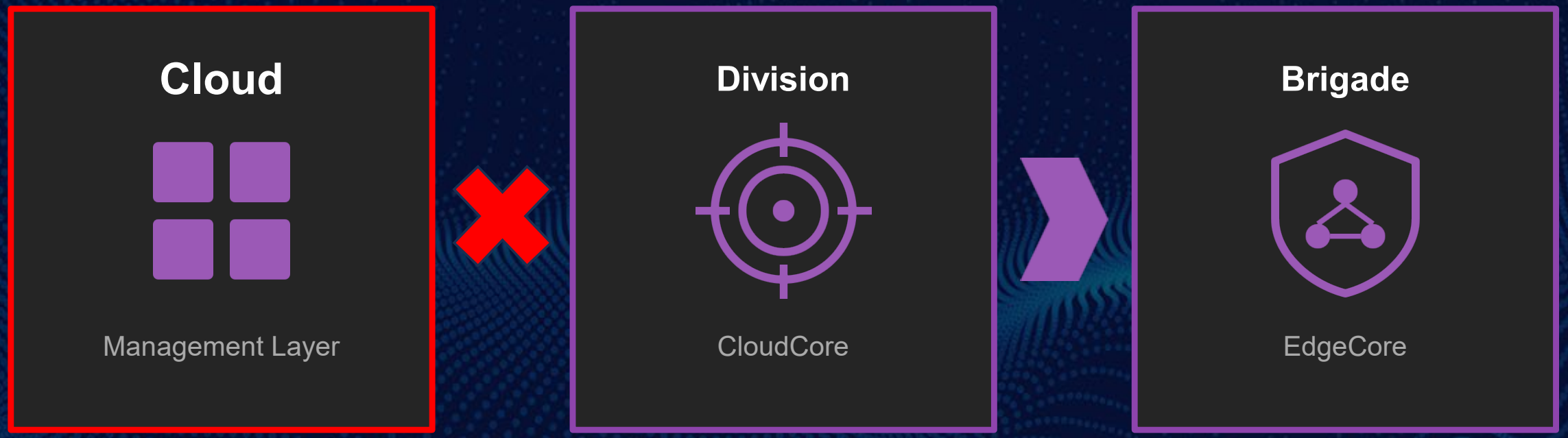
COMMAND POST

- Connected to cloud only
- Cannot update edges
- Queues configuration changes
- Monitors for reconnection

EDGE NODES

- Workload continue running
- No new deployments possible
- Local resource management
- Telemetry queued for sync

DDIL Scenario 2 – Command Post Disconnected



HQ OPERATIONS

- Lost connection to Command Post
- No visibility into edge status
- Central policies on hold

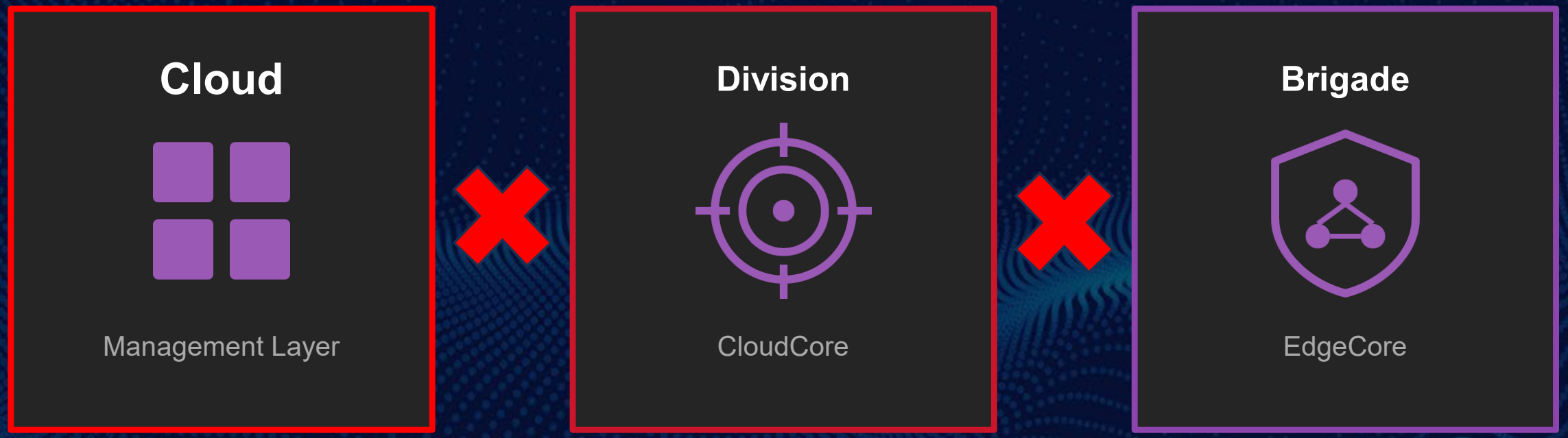
COMMAND POST

- Still manages edge nodes
- Independent operation continues
- Full edge functionality
- Local decision-making active

EDGE NODES

- Receives configuration updates
- Sends telemetry upstream
- Workloads running normally
- Unaffected by HQ disconnect

DDIL Scenario 3 – Complete Isolation



HQ OPERATIONS

- No connectivity to infrastructure
- Zero visibility into operations
- Awaiting reconnection

COMMAND POST

- Isolation from HQ and edges
- Cannot update edge nodes
- Maintain local state
- Operates independently

EDGE NODES

- Workloads continue running
- Full autonomous operations
- Local resource management
- Self-healing active

AI-Enabled ATO Acceleration & DevSecOps Alignment

NKP, NAI, and Pryon AI Integration:

- Natural language access to SBOMs, STIGs, policies
- Streamlined ATO generation through AI-augmented workflows
- Developer knowledge assistant for classified environments
- AI supports compliance documentation and audit traceability

DevSecOps Alignment for Software Factories - NKP Advantages:

- GitOps-native: integrates with FluxCD, Terraform, and Ansible
- Seamless integration with Platform One, Iron Bank/Big Bang
- Full lifecycle management of clusters, volumes, and infrastructure
- Seamless container orchestration, persistent storage, and monitoring
- Validated in partner software factories

Multi-Cloud & Edge Federation & Enabling GenAI at the Tactical Edge

Unified Command & Control:

- Prism Central manages IL4–IL6 clusters from a single pane
- Native CSI for Nutanix Volumes and Files in classified clouds
- VDI and Thin Client integration with Nutanix Frame
- Supports GovCloud, Azure Government, on-prem, and bare metal

Enabling AI at the Tactical Edge - NKP + Nutanix AI:

- Secure inference for ISR, C2, logistics, and predictive analytics
- GPU-enabled edge clusters for real-time AI/ML operations
- Supports confidential compute and zero trust data pipelines
- Complements DevSecOps with automated anomaly detection and AI assistants

Mission Context Accomplished

NUTANIX

Objectives for Programs Met:

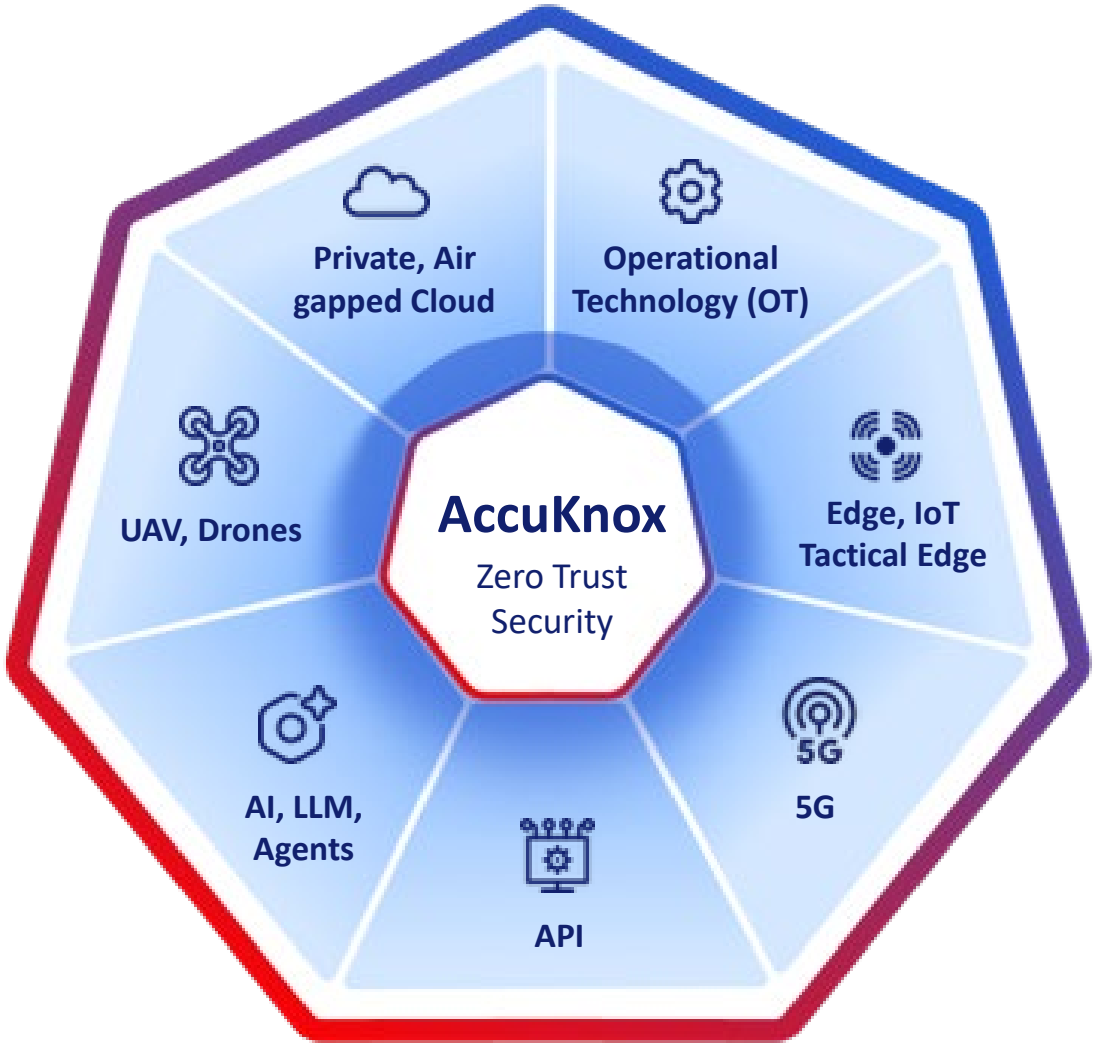
- Accelerate DevSecOps delivery across IL5/IL6 environments
  - Rapid prototyping and deployment to any environment
- Enforce Zero Trust security from development through deployment
- Ensure continuity from software factory to tactical edge
- Achieve unified management across domains and platforms
  - Unified, multi-domain operations: lab, cloud, tactical

AccuKnox - Unified Security Platform

All advanced attacks are runtime attack

Secure all your assets with AccuKnox runtime security powered CNAPP

- Public Cloud
- Private Cloud
- Private Cloud Air-Gapped



Layered Security

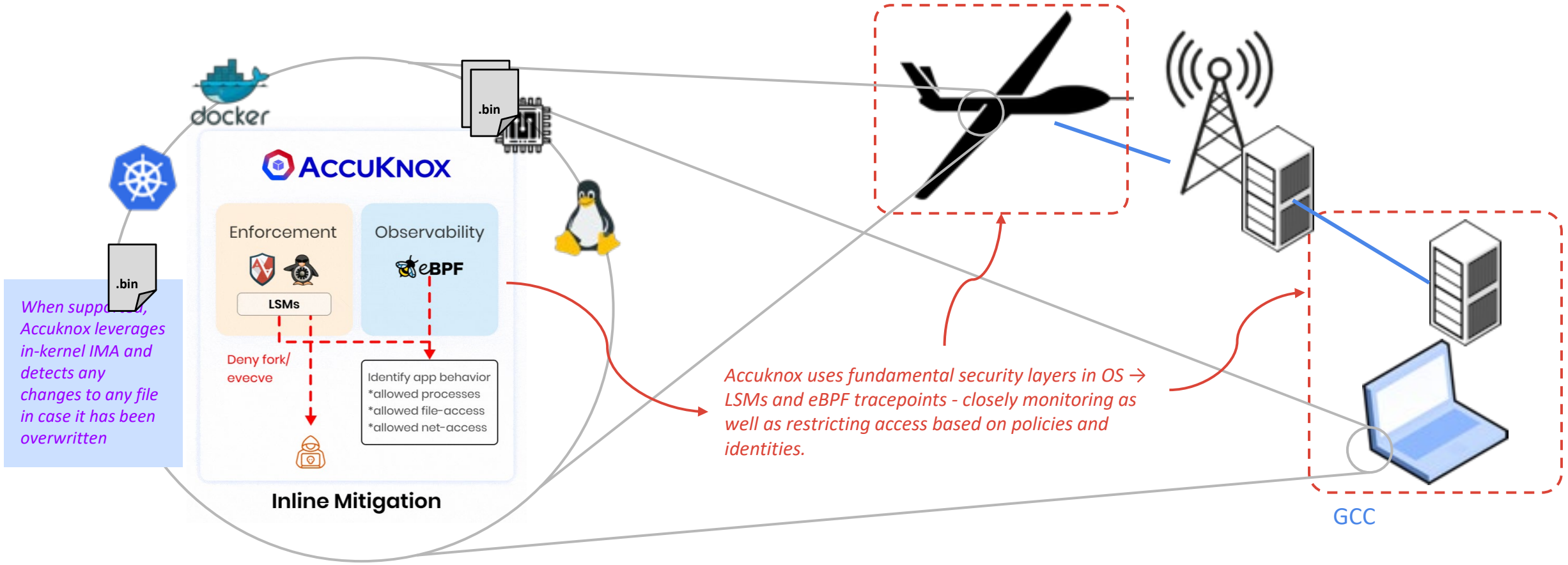
Agentless **CSPM** Cloud Security Posture Management	Basic Security	**Multi-Cloud Security** & **Compliance** Posture Discovery, and protection through the use of native APIs
	Application Security	App Security from **Code to Run**
Lightweight Industry Standard (eBPF) Sensor Agent **CWPP** Cloud Workload Protection Platform	Container Forensics & Auditing	**eBPF** (Extended Berkeley Packet Filter) based Observability with **Auto-Discovery of App Behavior** at process-level granularity
	Workload Hardening, Zero Trust Security	Comply with NSA Kubernetes Hardening Guide. - **Application Firewalling** - **Micro-segmentation** - **Kernel Hardening** to defend against zero-day attacks. Use eBPF for observability and **LSMs** (Linux Security Modules) to move from observability (audit) to enforcement (block) mode

© 2023 AccuKnox

Runtime Protection & Monitoring

ACCUKNOX

Building a Zero-Trust Identity-Aware network between all layers of computing on the Ground Control Center (GCC) and on the UAS side.



Why AccuKnox with Nutanix? Orchestrated & Open Source Driven

Misconfiguration Detection

Scan for misconfigurations in IaC templates. Auto-remediate at the source with a pull request

- Misconfigurations in Multi-Cloud
- Proactive Monitoring on Sensitive Assets

Runtime Security

Detect threats leveraging KubeArmor and get auto-recommended Behavioral & Hardening Policies and get in-line remediation

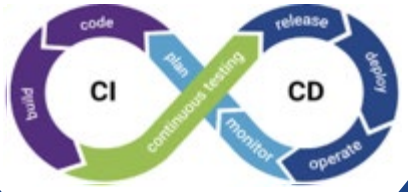
- Auto Policy Recomm.
- LSMs Enforcement
- Activity audit
- Micro-segmentation
- Custom Alert

Troubleshooting

Accelerate troubleshooting with a single source of truth

- Kubernetes Context
- eBPF backed telemetry
- Logs Aggregation

AccuKnox CNAPP



NUTANIX

Image Scanning

Scan for vulnerabilities and misconfigurations across static code, containers and hosts

- Registry/ Image Scan
- Static Code Analysis
- Host scanning

CSPM, KSPM & Compliance

Most comprehensive security posture by leveraging different security scanning tool. Custom Playbooks to cover all kind of Environments

- Security Tool Integration
- Compliance frameworks
- Risk Based Prioritization

Drift Detection

Get customized alerts based on deviation from baseline

- Custom Baseline
- Baseline Comparison
- Alerts on Drift

SE-UAS

For UAS Resilience and Autonomy in Highly Contested Peer-Adversary Ecosystems

Lead Organization: SRI International; Technical Point of Contact: Phillip.Porras@sri.com

Peer Nation-State Threats Are Outpacing UAS Swarm Defenses

The key challenge is not autonomous flight in benign conditions—it is mission survival under coordinated attack.

- Peer adversaries conduct integrated attacks, *not isolated disruptions.*
- Mission failure occurs when swarm trust, coordination, and integrity collapse together.
- Future UAS resilience requires system-level defense across autonomy, software, communications, and mission data.

Operational Imperative:

Defend the swarm as a system—not just the platform, the link, or the payload.

Capabilities Envisioned

Security-Enhanced UAS (SE-UAS) is a Best-of-Breed Open Vendor Platform For Defending Emerging Software-Defined UAS Platforms:

- AI-driven multi-agent peer-to-peer collective intelligence
- Automated ATO validation
- post-quantum data protection
- Zero-trust runtime enforcement
- GPS-independent swarm navigation intelligence,
- Unified situational awareness across distributed assets

System Impact and DoD Benefit

- Mission completion under adversarial pressure
- Bounded degradation rather than catastrophic swarm failure
- Reduced operator burden with AI-LLM mission validation
- Post-Quantum coalition-secure data protection
- Tactical-edge execution without cloud dependence
- Stronger transition potential for U.S. military use

Phase I Execution and Demonstration

Q1	Q2	Q3	Q4
System Design	**Core-Capability Development**	**Prototype & Evaluation Plan**	**Prototype Test Range Demonstration**
•Architecture •Interfaces •Mission scenarios •Adversarial plan •Integration plan	•AI command layer •APNT/swarm layer •UAS Zero-trust •Post-quantum data protection •UAS Test Range prep	•Interface validation •UAS Lab development •Prototype initiation •Test generation •Contested scenarios	•Final SE-UAS prototype demon •Adversarial test evaluation •Transition plan with target users

GPS Denial/EW Attacks | Comms Degradation | Cyber Espionage | Supply Chain Malware | ATO Compliance | AI Mission Resilience | Post-Quantum Threats

End-to-End Security Across All Environments

Nutanix Private Cloud Infrastructure, Nutanix Kubernetes Platform (NKP) + AccuKnox Zero Trust Security Overlay Delivers Comprehensive & Resilient Autonomous Security to the Tactical Edge

Land

Patriot systems, new radars, and a common launcher for current and future interceptors.

Under Layer

Air

Next Generation Interceptors (NGI), THAAD, and Aegis systems with a new missile field in the American Midwest.

Upper Layer

Sea

For communications and targeting.

Undisclosed Geosynchronous Earth Orbit

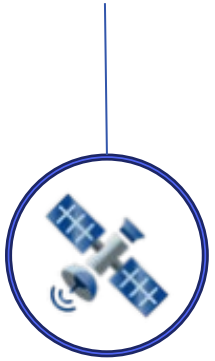
Space

Dedicated to detection and interception

Low Earth Orbit (LEO)

Cyber

Satellites for missile warning, tracking and boost-phase intercept.



Space Layer

Build, Deploy & Secure Any Application, Anywhere: From Core to Cloud to Edge

Questions...

NUTANIX

Nutanix Confidential

Thank You

PRESENTED BY: Bill Kalogeros
Nutanix Cloud Native - NKP Modern Applications and Data
bill.kalogeros@nutanix.com

NUTANIX

Nutanix Confidential