Applying a Zero Trust Security Mindset for Kubernetes, and a Way to Begin Solving the Problem

PRESENTED BY: Bill Kalogeros, Nav Sagoo, Dave Ayoub
Nutanix Cloud Native - Modern Applications and Data
bill.kalogeros@nutanix.com
Nav.sagoo@nutanix.com
David.Ayoub@nutanix.com

BLUF (Bottom Line Up Front)

NUTANIX

Kubernetes is Not Easy: Kubernetes adoption creates new cybersecurity challenges

- **Zero Trust at the Container Level is Not Zero Trust at the Network/Application Level**
- **Researchers identified 350+ API servers that could be exploited by attackers**
- **Exposed Dashboard and API Endpoints**
- **Insecure Container Images and Registries**
- **Default Privileges and Permissions**
- **Unpatched Nodes and Components**

Limited Resources Create Ops Challenges Without Automation

- Managing Container Drift & Container Security
- Managing and Securing the SBOM
- Maintaining the ATO
- Maintaining Day-2 Operations
- Maintaining a Zero Trust Container Environment
- Mitigating Zero-Day Container Attacks
- **Protecting the Vault – Securing your Secrets**

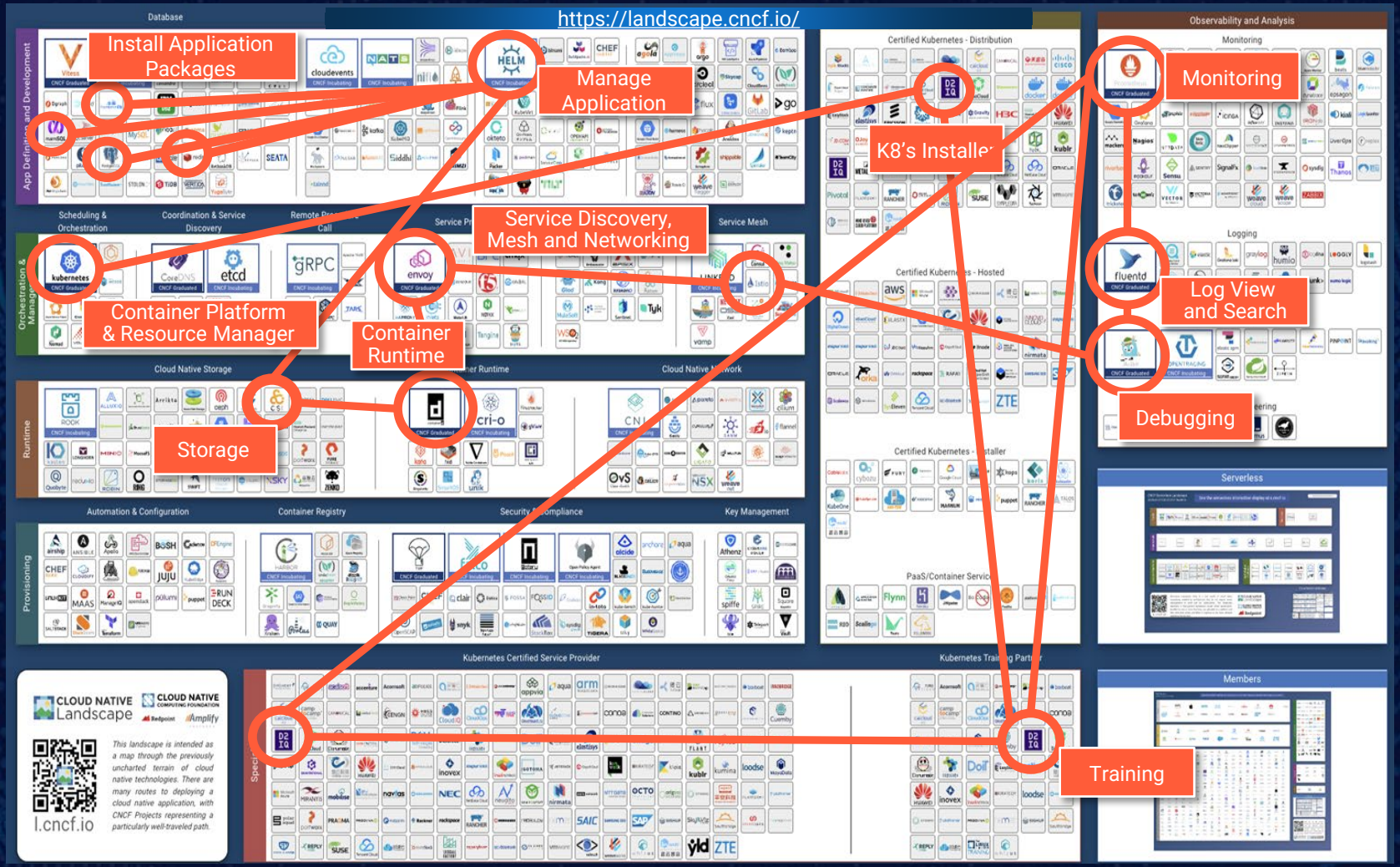
Ops teams struggle with growing complexity of Kubernetes environments

Given this complexity, it is not surprising that almost all stakeholders (98%) reported they face challenges when using Kubernetes in production.

For 2023, one challenge is at the top of the list — putting in needed guardrails for enterprise production environments (48%)

Help Net Security
November 10, 2023

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



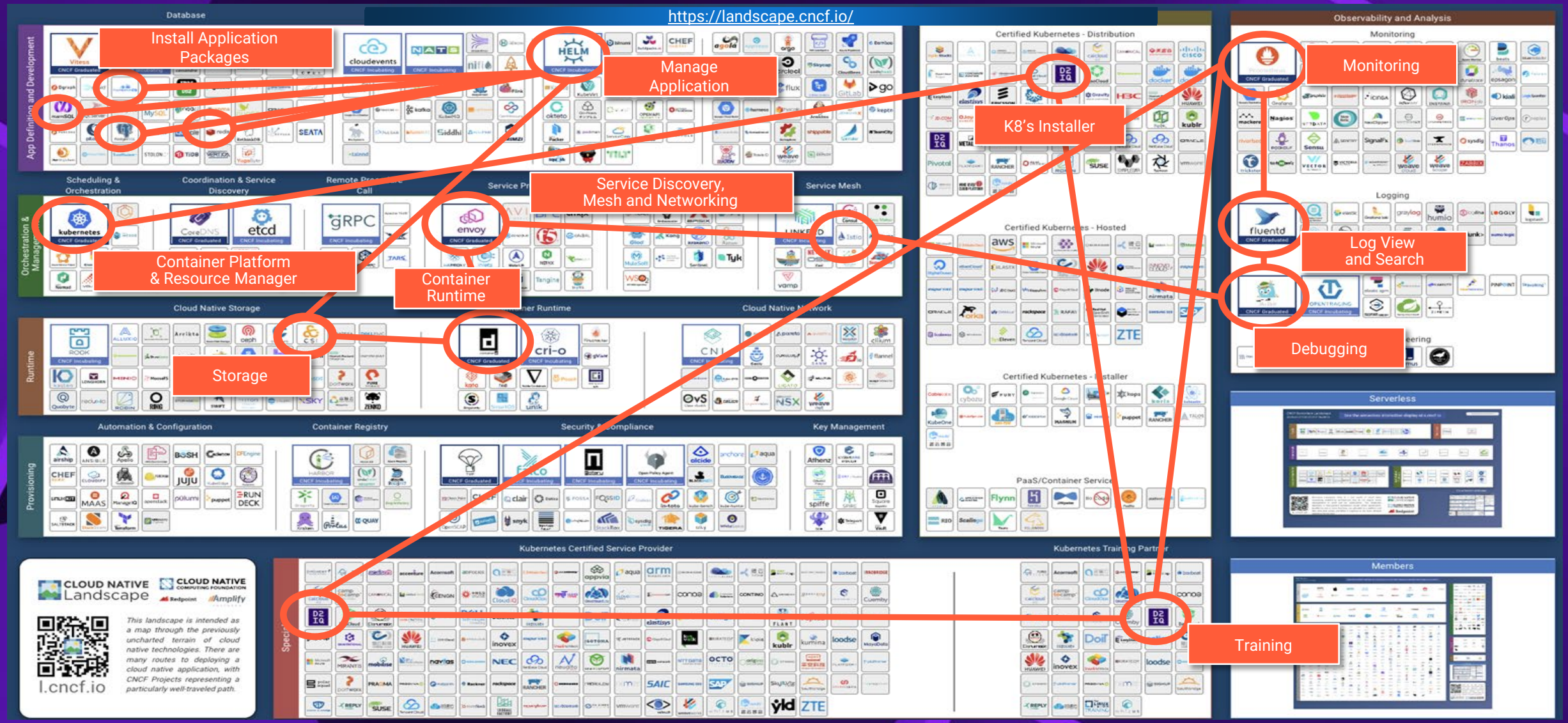
NUTANIX

WHAT'S A KUBERNETES?

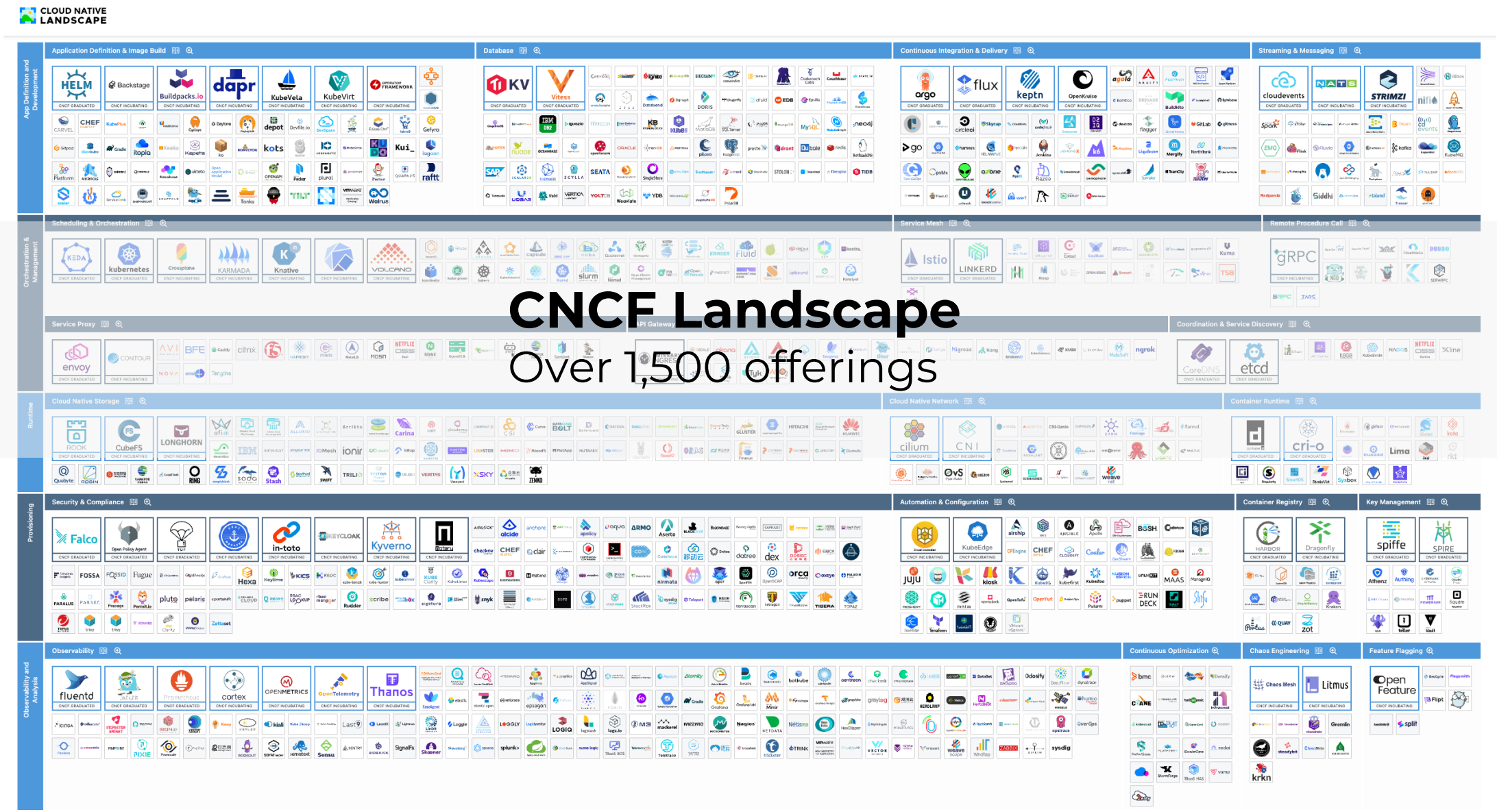
NUTANIX

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

https://landscape.cncf.io/



And building that stack can be overwhelming



CNCF Landscape

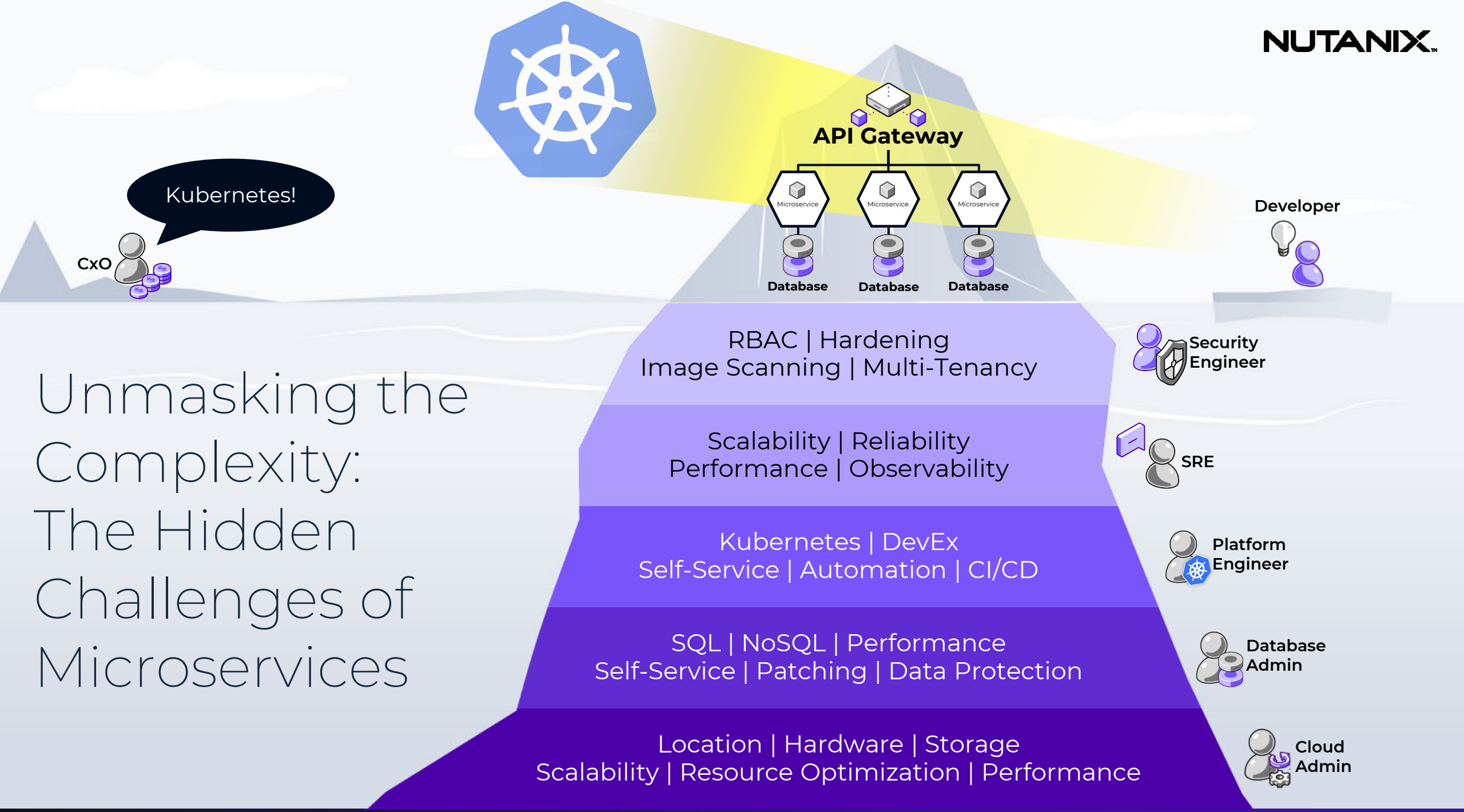
Over 1,500 offerings


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

NUTANIX

NUTANIX

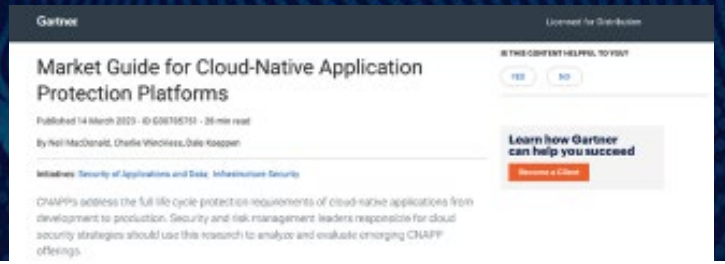
Unmasking the Complexity: The Hidden Challenges of Microservices



What Does It Take to Build a Kubernetes Platform?

+10%	Container Registry
+10%	DevEx (Software Factory)
10%	Application Networking
10%	Security & Compliance
10%	Observability
10%	Multicluster & Multicloud Management
10%	Distributed Storage & Data Services
10%	Cluster Networking
30%	**Kubernetes**
10%	Infrastructure

Market Guide for Cloud-Native Application Protection Platforms



- ✓ **Optimal security of cloud-native applications requires an integrated approach that starts in development and extends to runtime protection.**
- ✓ **Implement an integrated security approach that covers the entire life cycle of cloud-native applications, starting in development and extending into production.**
- ✓ **Integrate security into the developer's toolchain so that security testing is automated as code is created and moves through the development pipeline, reducing the friction of adoption.**
- ✓ **Acknowledge that perfect apps aren't possible and focus developers on highest severity, highest confidence and highest risk vulnerabilities to avoid wasting developer's time.**
- ✓ **Scan development artifacts and cloud configuration comprehensively and combine this with runtime visibility and configuration awareness in order to prioritize risk remediation.**
- ✓ **Favor CNAPP vendors that provide a variety of runtime visibility techniques, including traditional agents, Extended Berkeley Packet Filter (eBPF) support, snapshotting, privileged containers and Kubernetes K8s integration to provide the most flexibility at deployment.**

While Zero Trust is a security model that emphasizes a "never trust, always verify" approach, applying it to Kubernetes environments comes with some challenges and shortfalls.

While Zero Trust is a security model that emphasizes a “never trust, always verify” approach, applying it to Kubernetes environments comes with some challenges and shortfalls.

Here are some potential issues and considerations:

1. Complexity of Microservices
2. Network Overhead
3. Granular Policy Definition
4. Identity Management
5. Service Mesh Integration
6. Dynamic Nature of Kubernetes
7. Logging and Monitoring
8. Dependency on Network Policies
9. User Experience and Productivity
10. Resource Intensive

NUTANIX

Potential issues and considerations:

Complexity of Microservices

Kubernetes environments often consist of numerous microservices, each with its own dependencies and communication patterns. Implementing and managing a Zero Trust model in such a complex architecture can be challenging, requiring careful configuration, and monitoring.

Potential issues and considerations:

NUTANIX

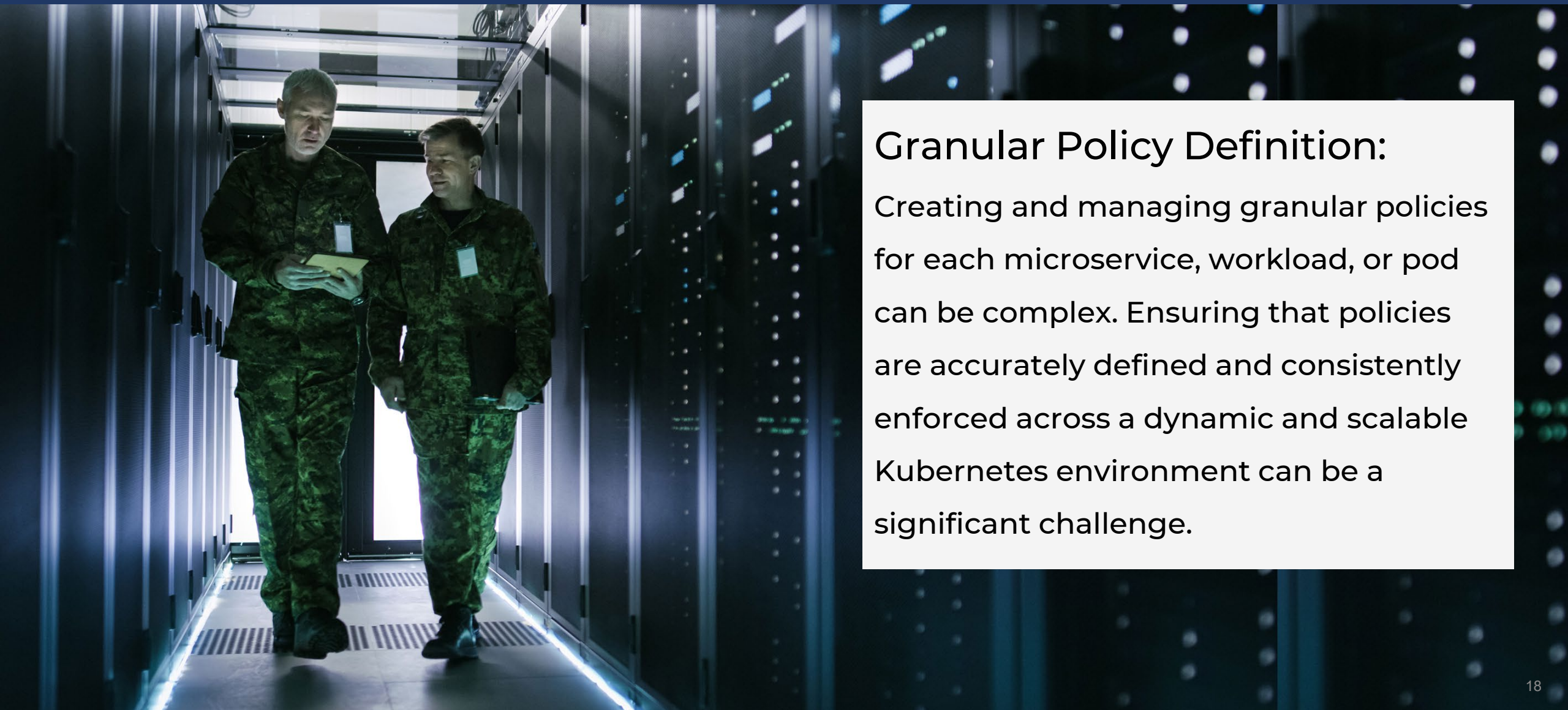
Network Overhead:

Zero Trust involves continuous verification of entities and strict access controls.

This can introduce additional network overhead, especially in large Kubernetes clusters, potentially impacting performance.

NUTANIX

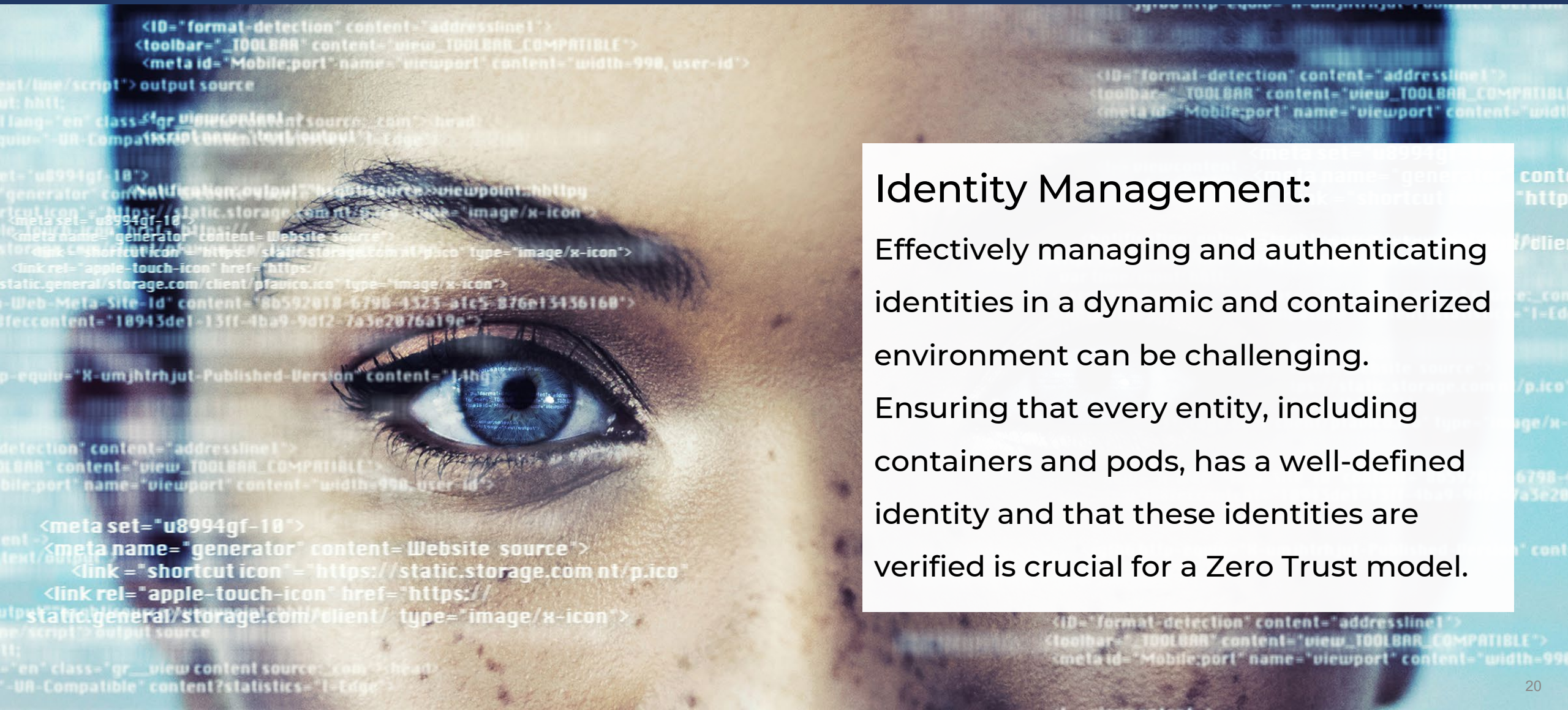
Potential issues and considerations:



Granular Policy Definition:

Creating and managing granular policies for each microservice, workload, or pod can be complex. Ensuring that policies are accurately defined and consistently enforced across a dynamic and scalable Kubernetes environment can be a significant challenge.

Potential issues and considerations:



Identity Management:

Effectively managing and authenticating identities in a dynamic and containerized environment can be challenging. Ensuring that every entity, including containers and pods, has a well-defined identity and that these identities are verified is crucial for a Zero Trust model.

NUTANIX

Potential issues and considerations:

Service Mesh Integration:

Many Kubernetes environments use service mesh technologies like Istio for managing microservices communication. Integrating Zero Trust principles within a service mesh architecture may require additional considerations and configurations.

NUTANIX

Potential issues and considerations:

Dynamic Nature of Kubernetes:

Kubernetes is inherently dynamic, with pods and services scaling up or down based on demand. Adapting a Zero Trust model to the dynamic nature of Kubernetes, where workloads are constantly changing, can be a continual challenge.

NUTANIX

Potential issues and considerations:

Logging and Monitoring:

Zero Trust relies on comprehensive logging and monitoring to detect and respond to potential threats. Setting up effective logging and monitoring solutions within Kubernetes and ensuring that security events are appropriately logged and analyzed, can be demanding.

NUTANIX

Potential issues and considerations:

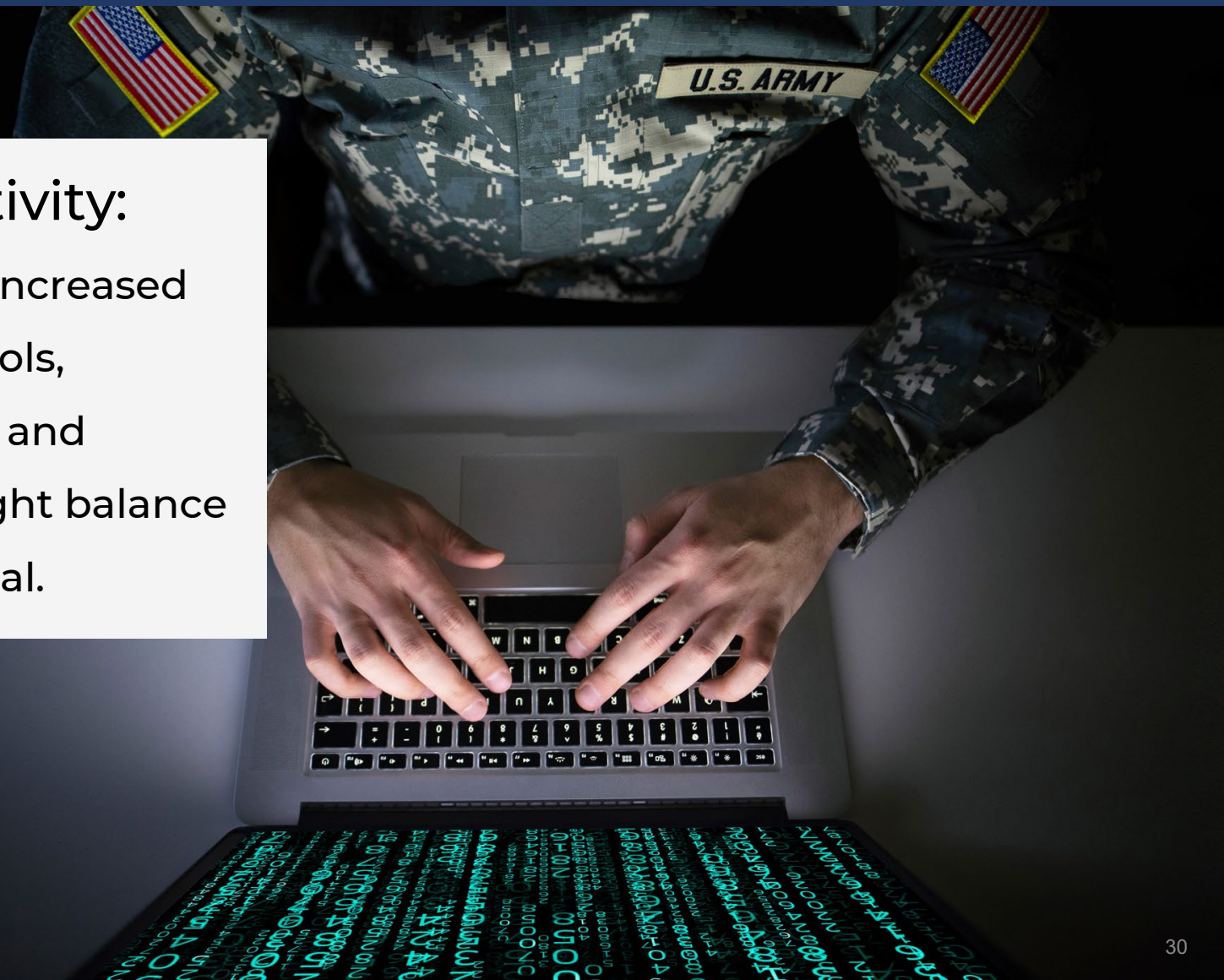
Dependency on Network Policies:

Network policies in Kubernetes define how pods can communicate with each other and other network endpoints. Depending solely on network policies for Zero Trust might not cover all aspects of the security model, especially when considering the diversity of communication channels within a Kubernetes cluster.

Potential issues and considerations:

User Experience and Productivity:

A strict Zero Trust model may lead to increased authentication steps and access controls, potentially impacting user experience and developer productivity. Striking the right balance between security and usability is crucial.



NUTANIX

Potential issues and considerations:

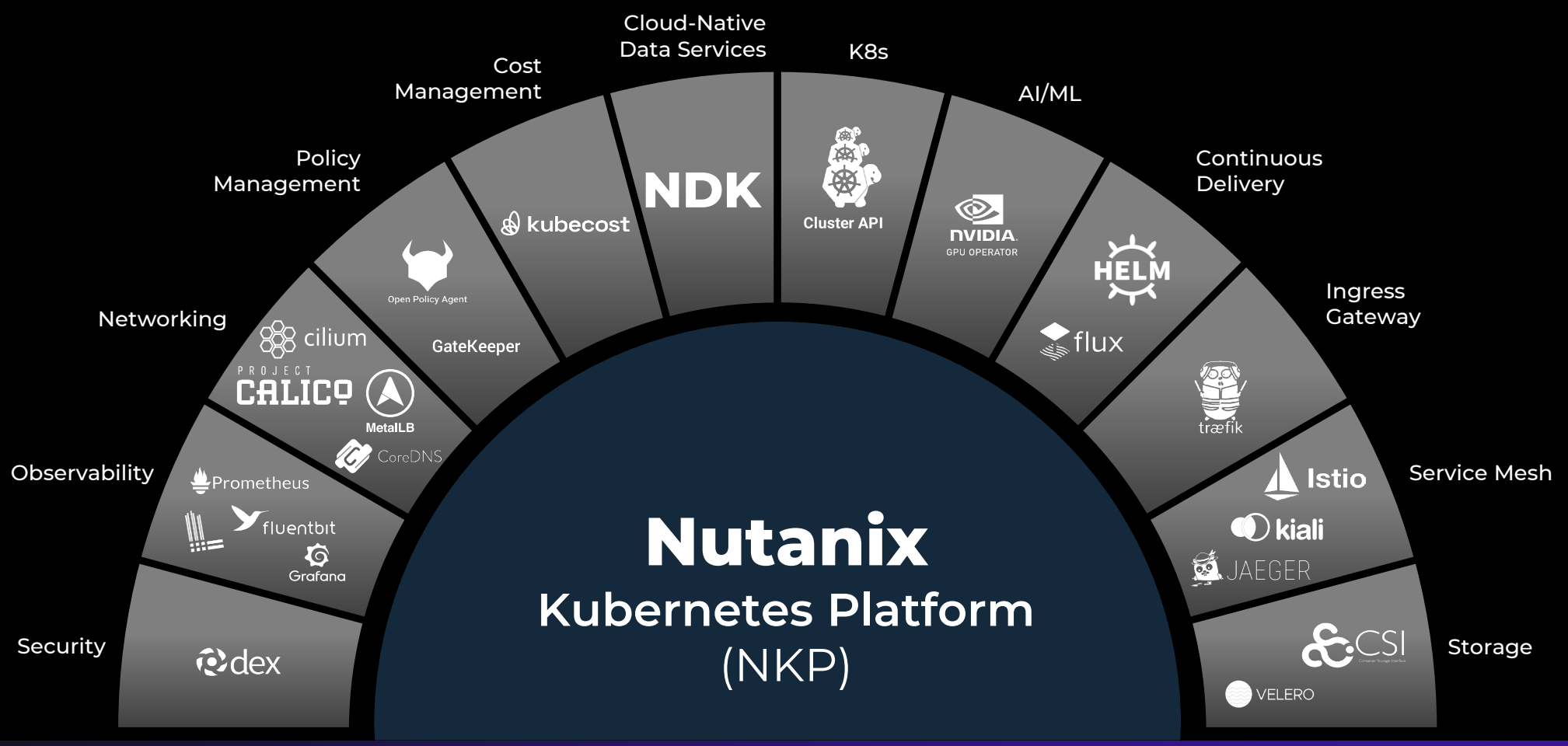
Resource Intensive:

Implementing a comprehensive Zero Trust model often requires additional security components such as identity providers, access management systems, and continuous monitoring tools. These can be resource-intensive and may require careful resource planning.

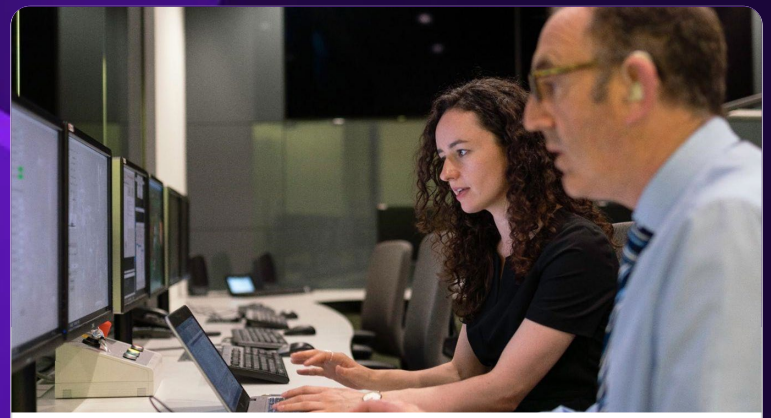
To address these challenges, organizations need to carefully design and implement Zero Trust principles in their Kubernetes environments, considering the specific characteristics and requirements of containerized architectures. Regular updates, training, and adaptation to emerging security standards can help mitigate these shortfalls.

Consolidate and master your cloud native operations

Deploy, Secure, Manage and Upgrade:
Enterprise-Ready Cloud Native Stack at Scale

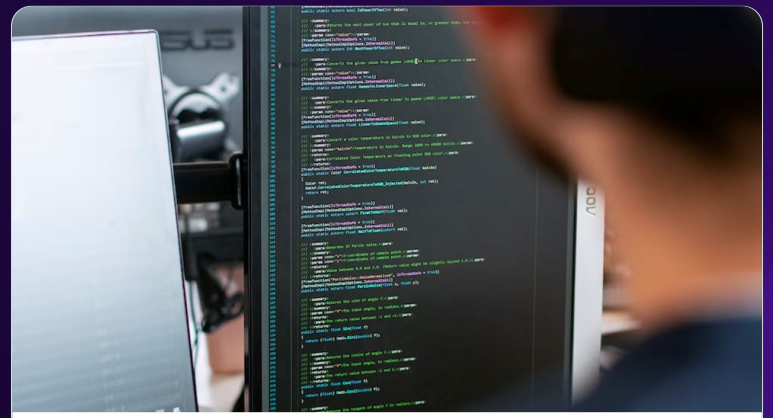


The Need for a Kubernetes Management Platform



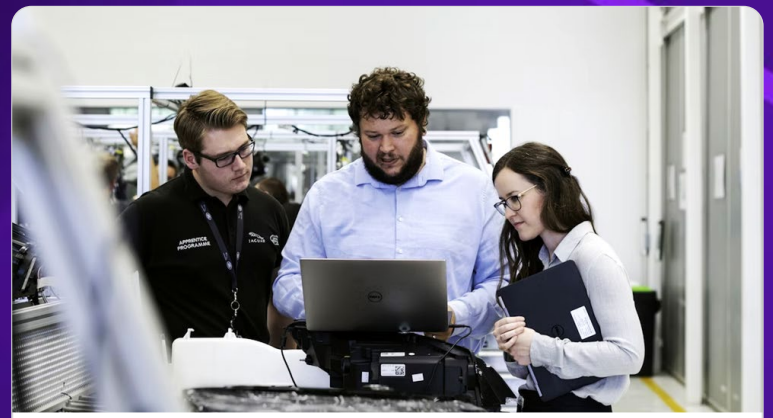
Flexibility & Resilience

Quickly deploy your applications from cloud to air-gapped and DDIL environments



Digital Modernization

Take advantage of the latest Open Source technological advances in security, observability and networking

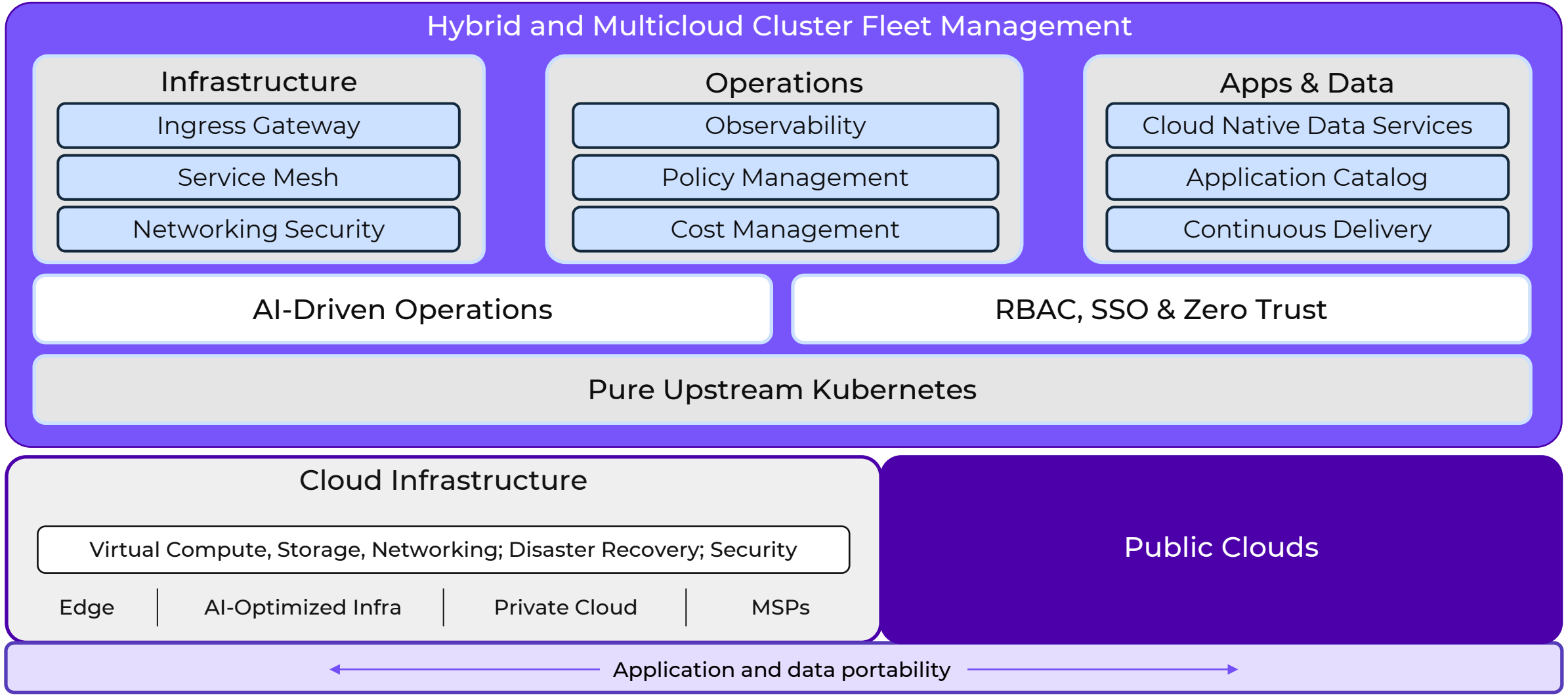


Automation & Orchestration

Accelerate, manage and optimize your deployments, operations and app configuration

NUTANIX

The Nutanix Kubernetes Platform (NKP)



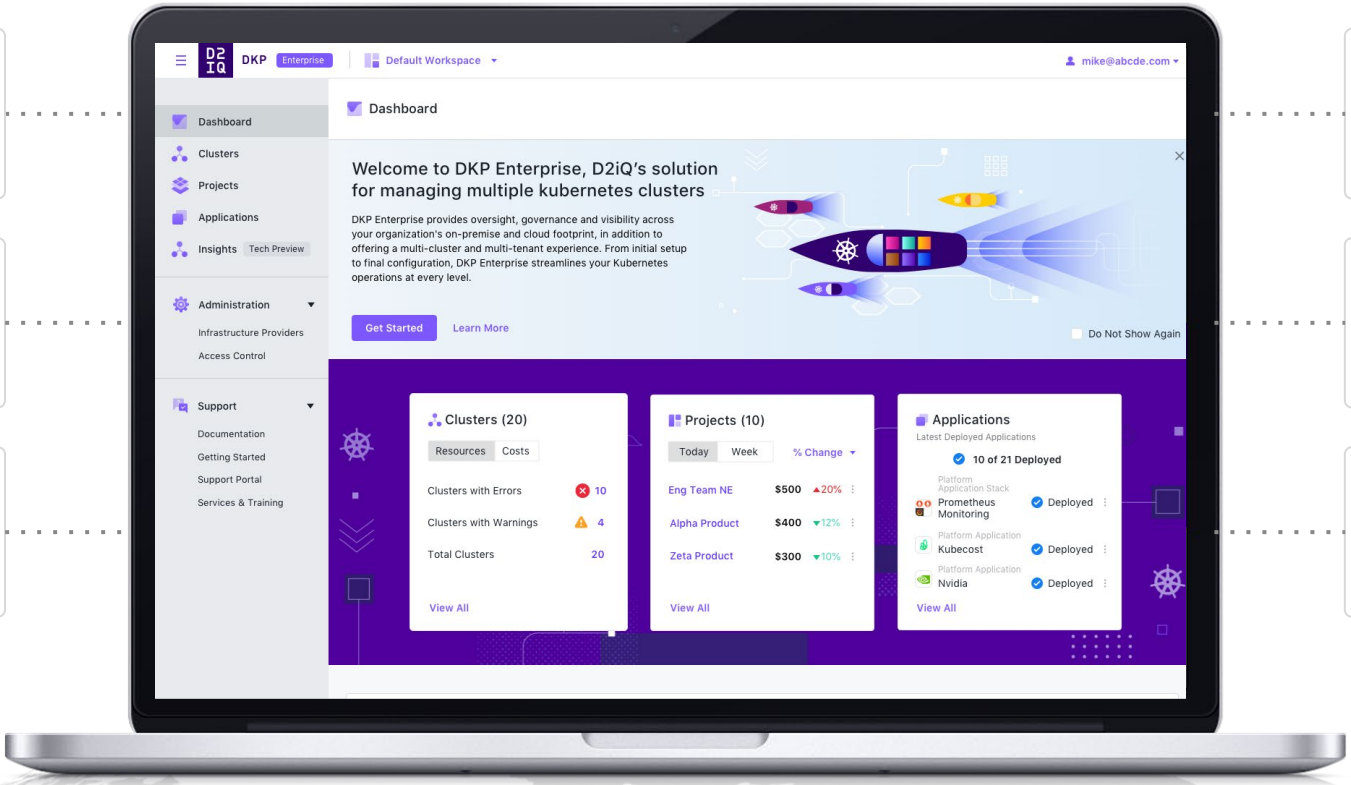
Federated Kubernetes Management

Consistent Day 2 Operations

Governance
Any CNCF Distribution
Any Cloud

User Access Control
Centralized Access Management

Workload Optimization
Scale Mission Critical Workloads



Observability
Centralized Monitoring and Alerts

Financial Visibility
Track Multi-Cloud Cost

Application Management
Continuous Deployment

USE CASES

NUTANIX

Air-Gapped Kubernetes Challenges

- No internet connection / temp proxy
- National Security
- Cyber security
- Regulatory compliance
- Highly sensitive data
- Remote locations
- Lack of bandwidth/ isolated clusters

NUTANIX

Making Air-Gapped Easy

- We built our Kubernetes distribution from the ground up for easier air-gapped installation
- We purpose-built automation to speed and simplify air-gapped installation
- We thoroughly tested and documented our installation processes to make them fast and easy
- We are successfully running Kubernetes in air-gapped environments—we know how to do this and how to teach you to do it

NUTANIX

Hybrid/Multi-Cloud Challenges

- Unnecessary operational code modifications cost time and money and add risk
- Each environment has its own distinct Kubernetes controls limiting visibility and control.
- Reduced application portability due to differing operating frameworks across environments

NUTANIX

Simplifying Hybrid/Multi-Cloud Environments

- Run anywhere: in the cloud or clouds, on-prem, air-gapped
- NKP Kubernetes, Nutanix Prism, Amazon EKS, Microsoft AKS, or any CNCF compliant K8s
- Installation processes to make them fast and easy in all of these environments
- Single, strategic point of control for all of your different environments, providing a centralized, unified view and the ability to manage across platforms

NUTANIX

Thank You

NUTANIX