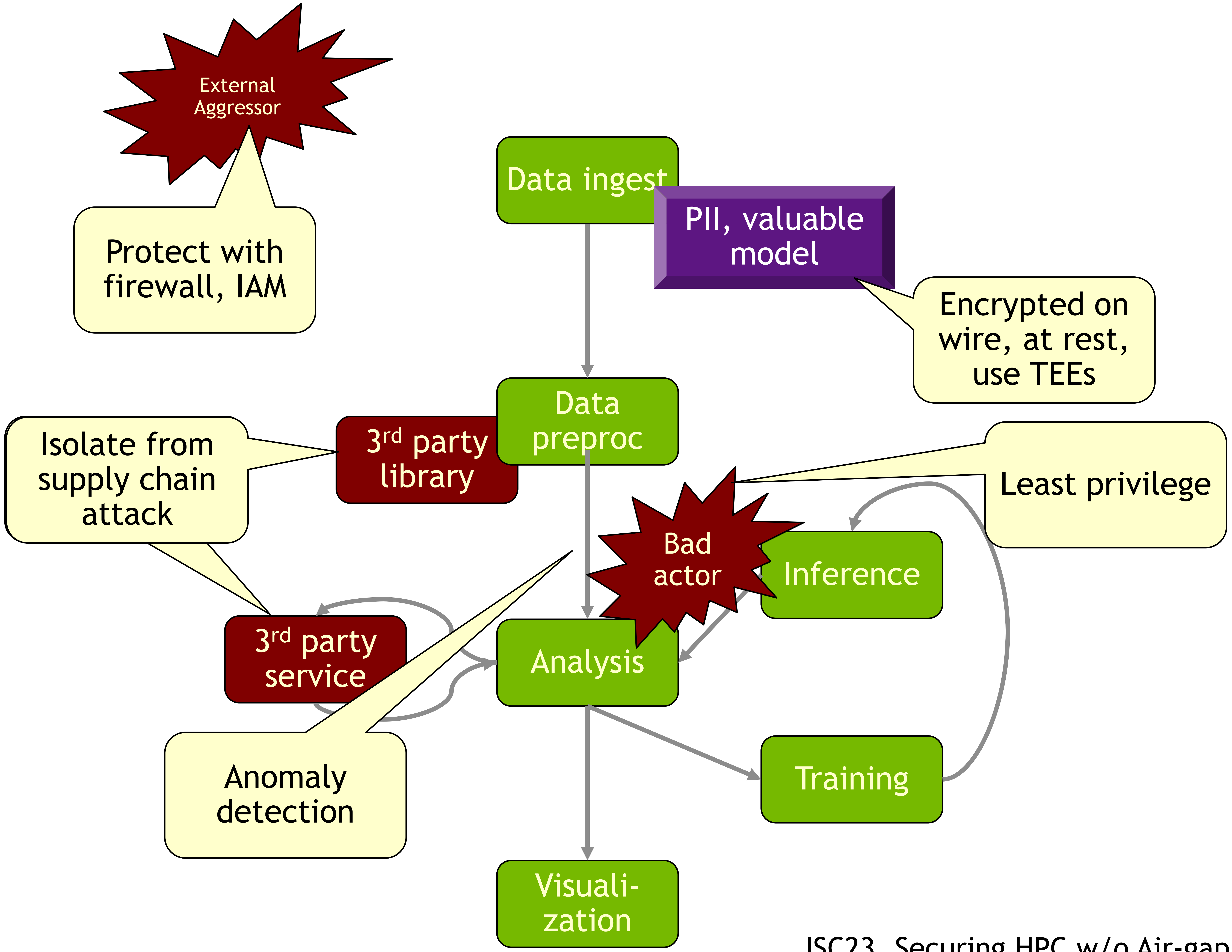
Zero trust ingredients for a modern data center

Dr. CJ Newburn, Distinguished Engineer, IO/Datacenter/Security Architect | ISC23: Securing HPC without air gapping

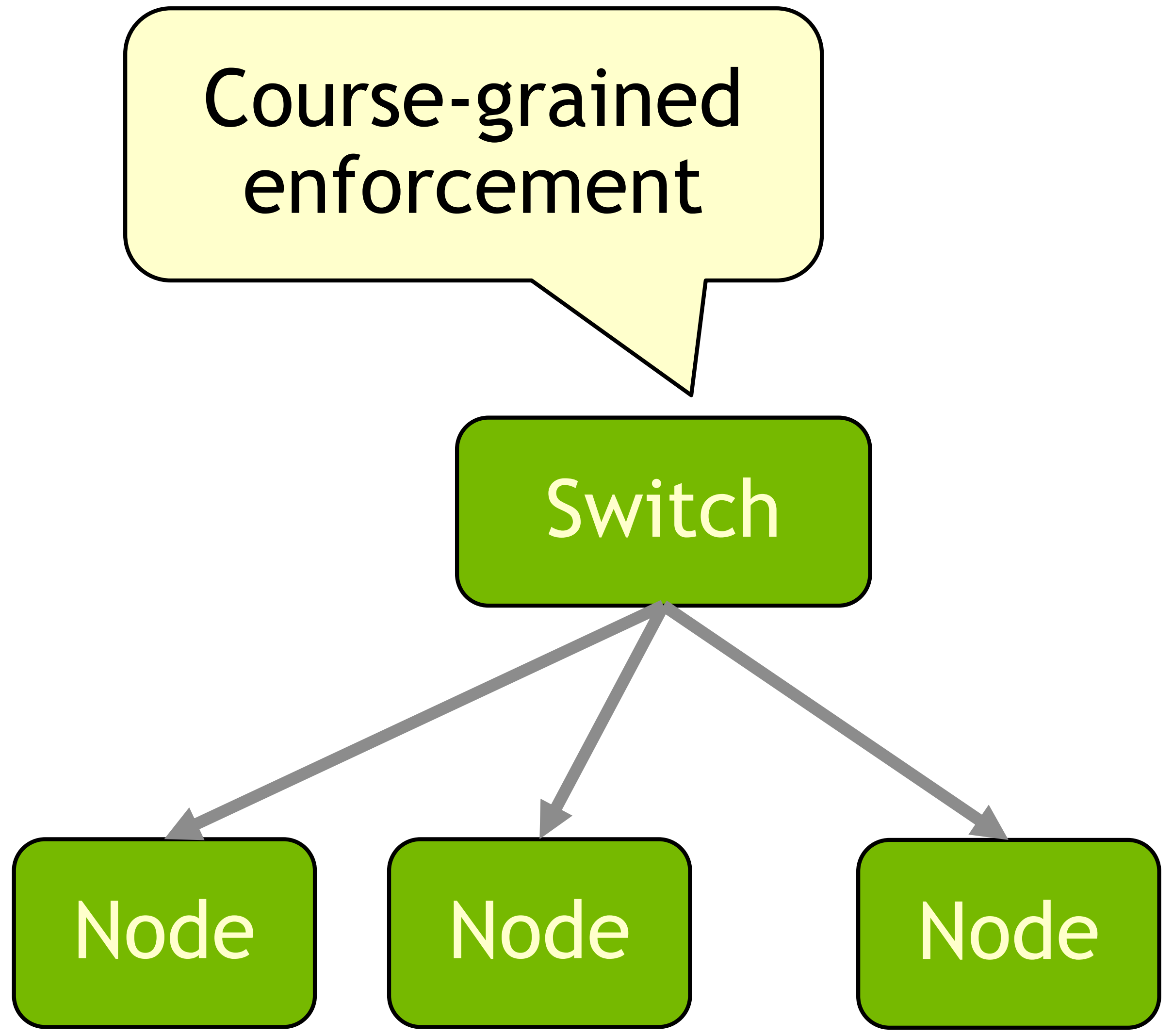
Toward security within a single workflow

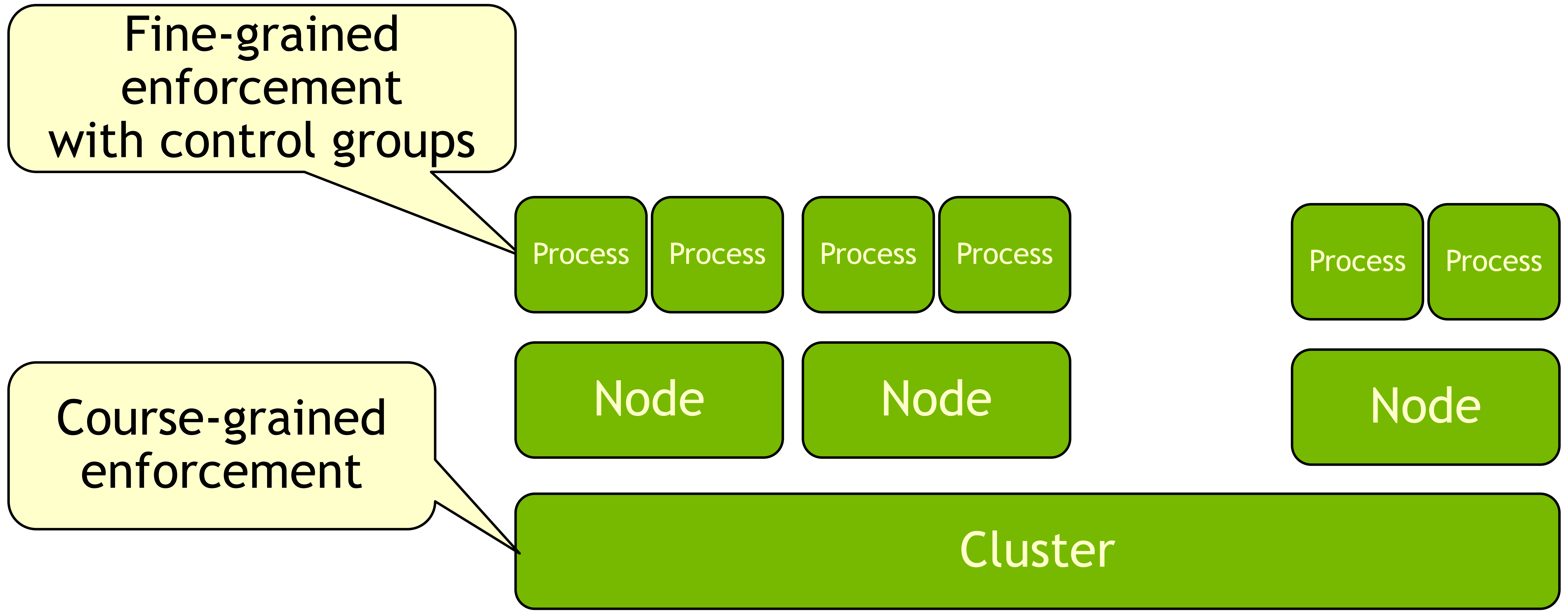
Isolate compartments regardless of context

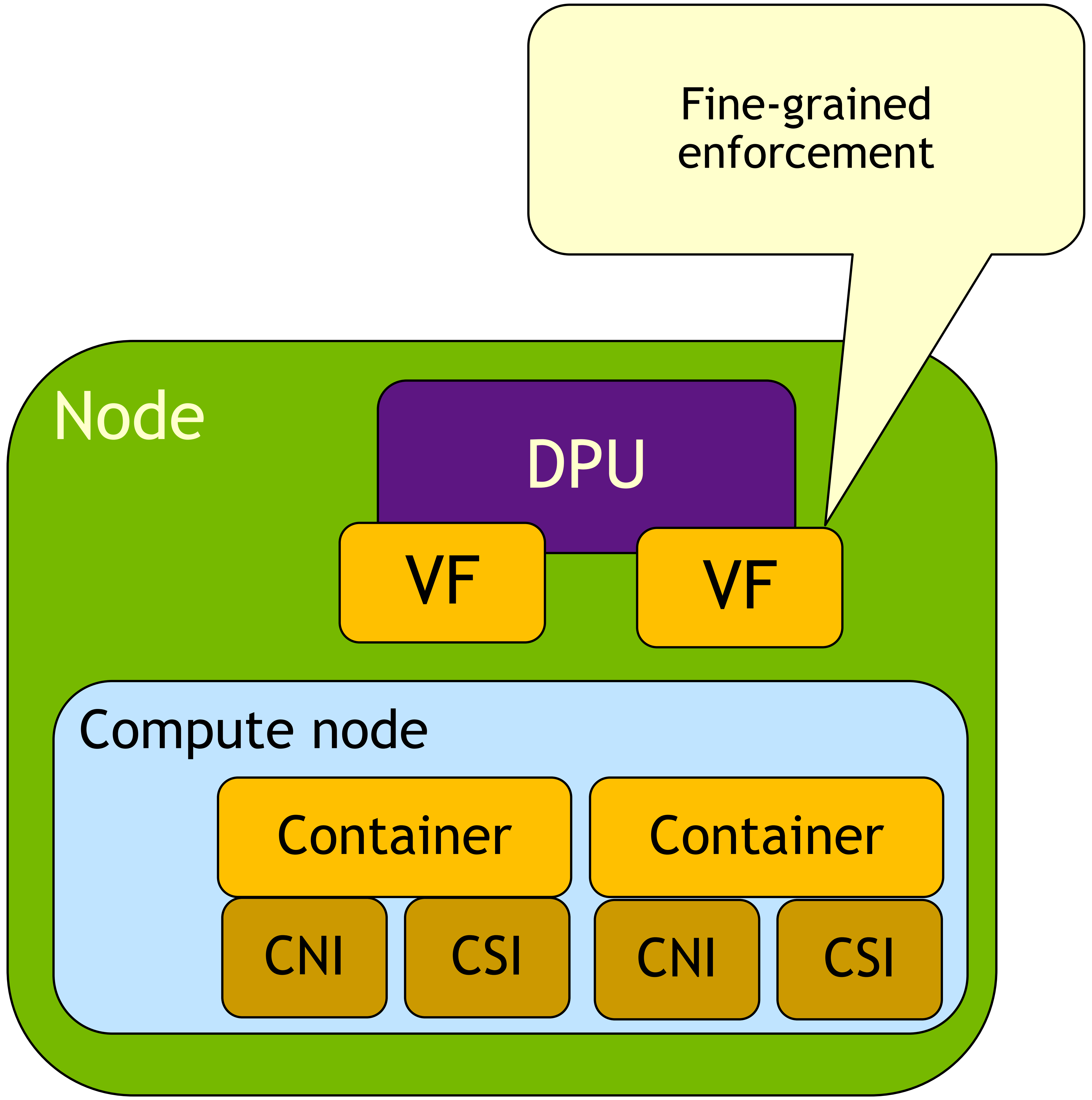


Making enforcement more fine-grained

Down to the container/VF level




Fine-grained enforcement with control groups
Process
Process
Process
Process
Process
Process
Node
Node
Node
Course-grained enforcement
Cluster



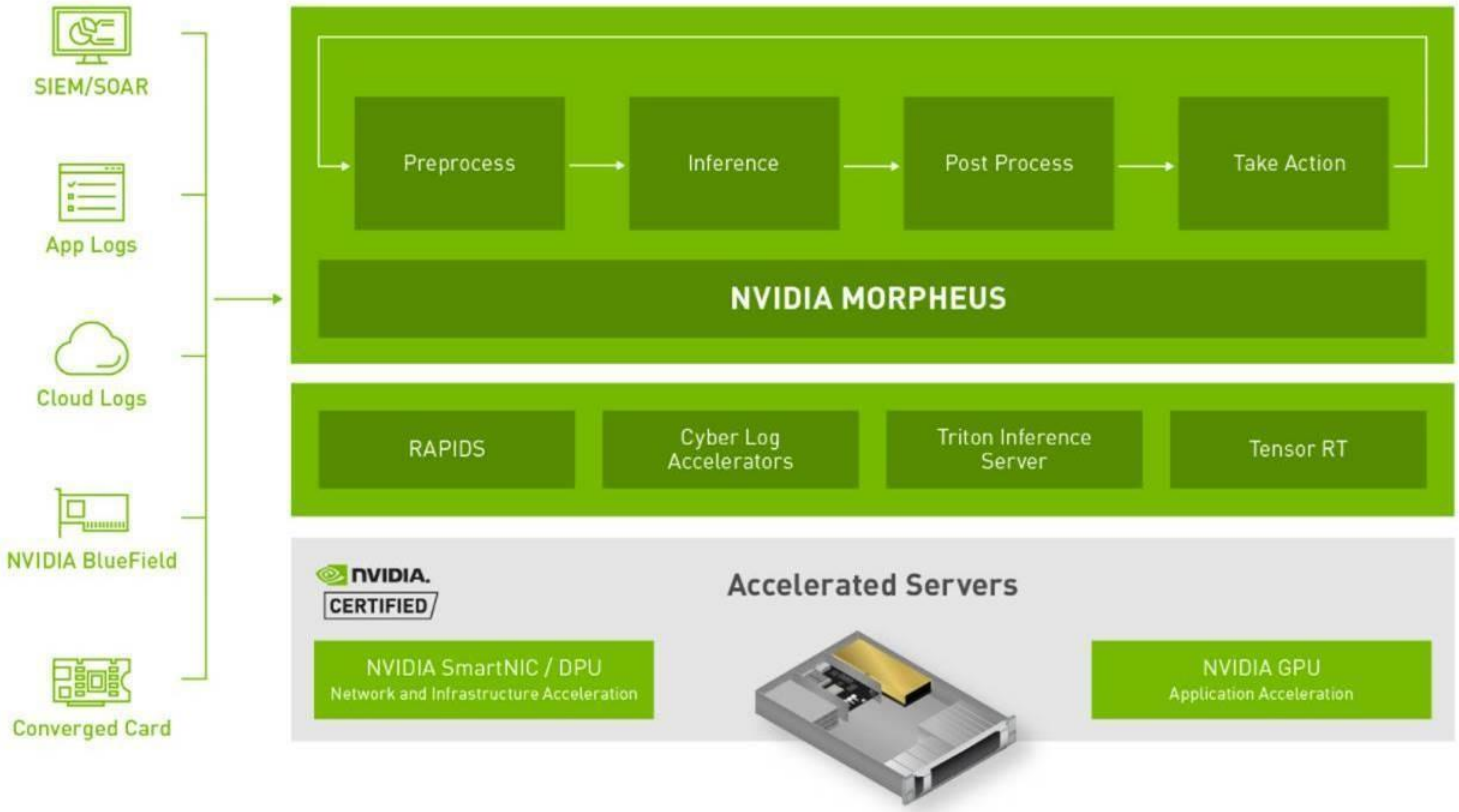
Confidential computing

A set of TEEs span CPU, GPU, DPU for unified protection and isolation; work in conjunction with containers/orchestration

CC Off
CPU
Legacy VM
NVIDIA Driver
Host OS
Hypervisor
Unencrypted Transfers
Full Access
NVIDIA H100 GPU
CC On
CPU
Confidential VM
NVIDIA Driver
Host OS
Hypervisor
Encrypted Transfers
No Read or Write Access
NVIDIA H100 GPU
CC Possible future
CPU
GPU
DPU
Confidential VM
NVIDIA Driver
Future GPU
Future DPU
Green TEE
Red TEE
Blue TEE

AI on the wire: NVIDIA Morpheus

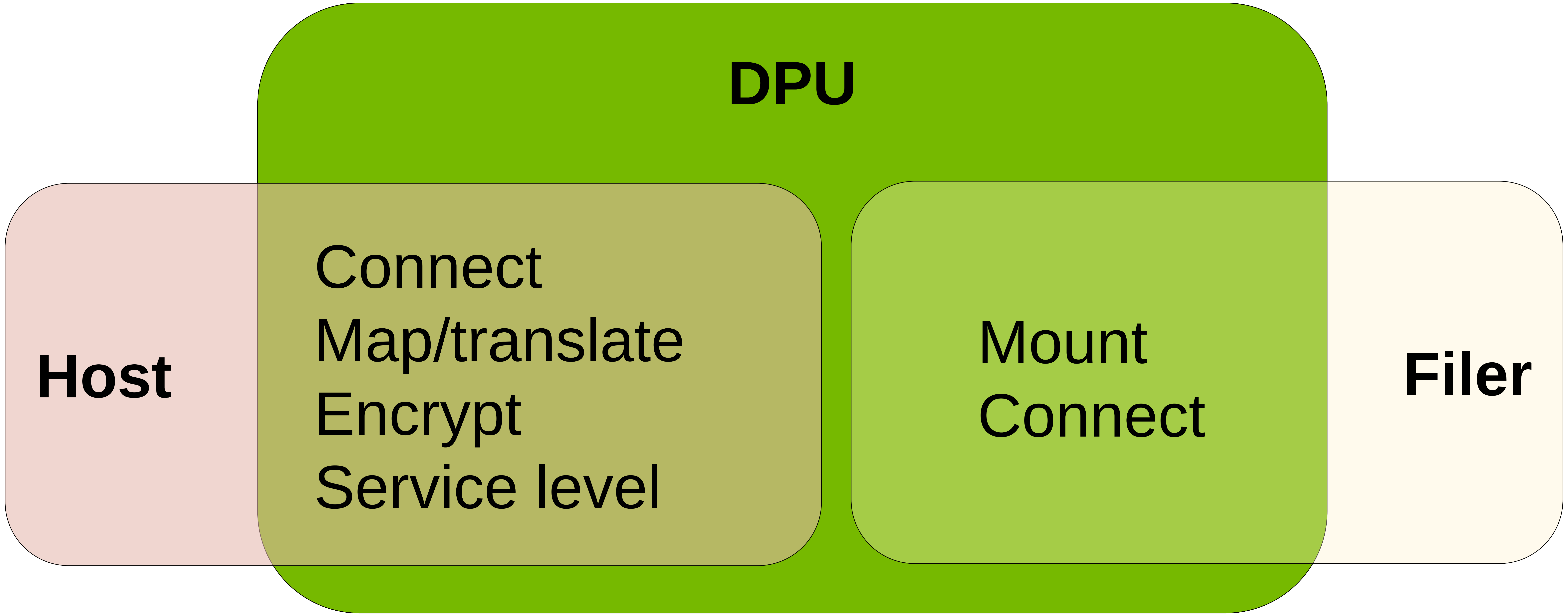
Open AI framework for accelerated cybersecurity workflows



- Automation: take the human out of the loop
- Increased data density: 10M events/day → 8-10 actionable
- Responsiveness: weeks → minutes
- Adaptiveness: respond to evolving threats
- “Noticing different” doesn’t require the updates that “notice signature” does
- Avoid CSP lockin
- + SDK for DiY

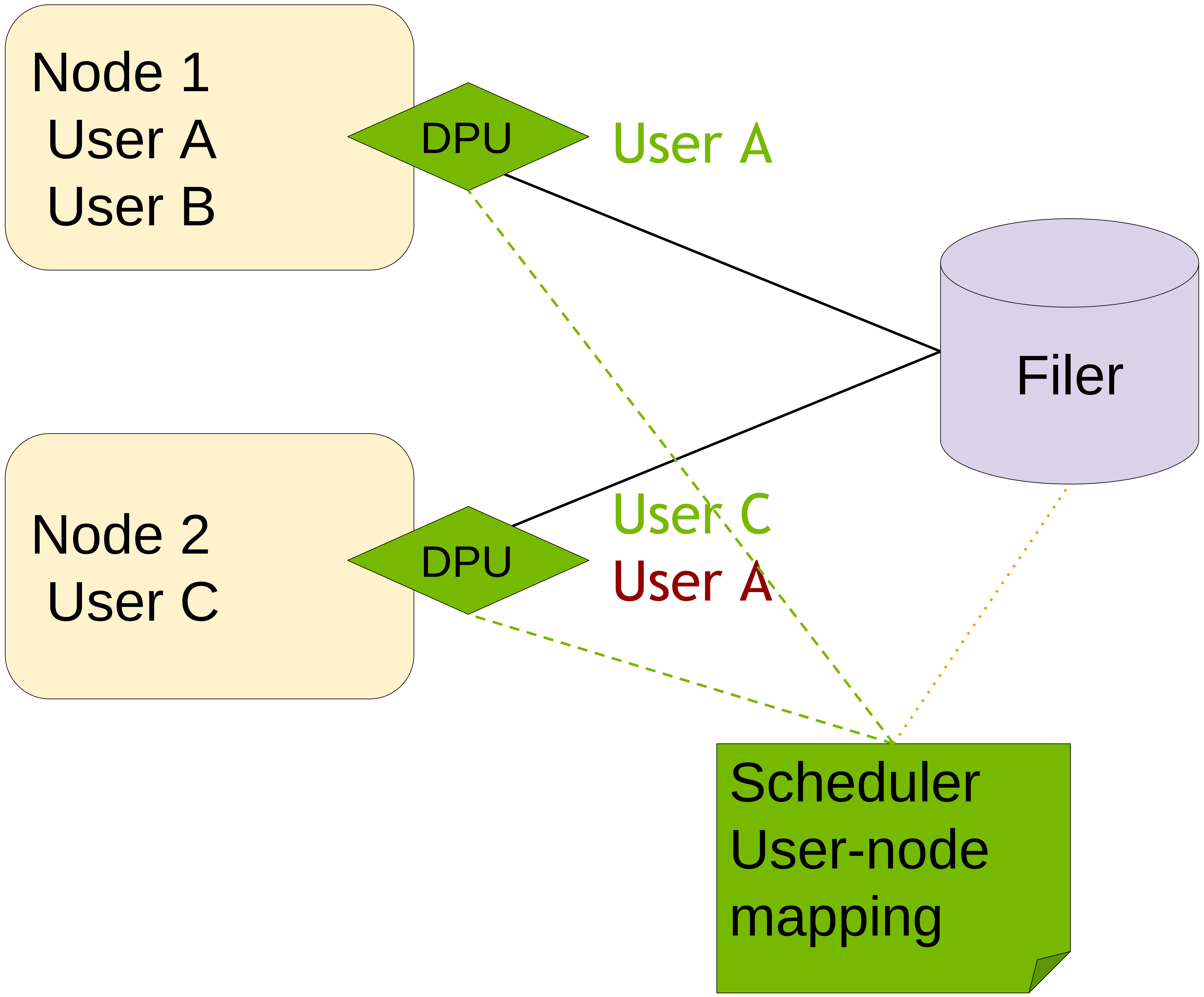
Shift storage functionality to the DPU

Credentials supplied to the DPU vs. the untrusted compute node



DPU as a gate to authorization

Credentials sent to and used by more-trusted DPU vs. compute node



Cloud-based control plane

Preferred path to most-effective management

Cluster-scale SW management required for

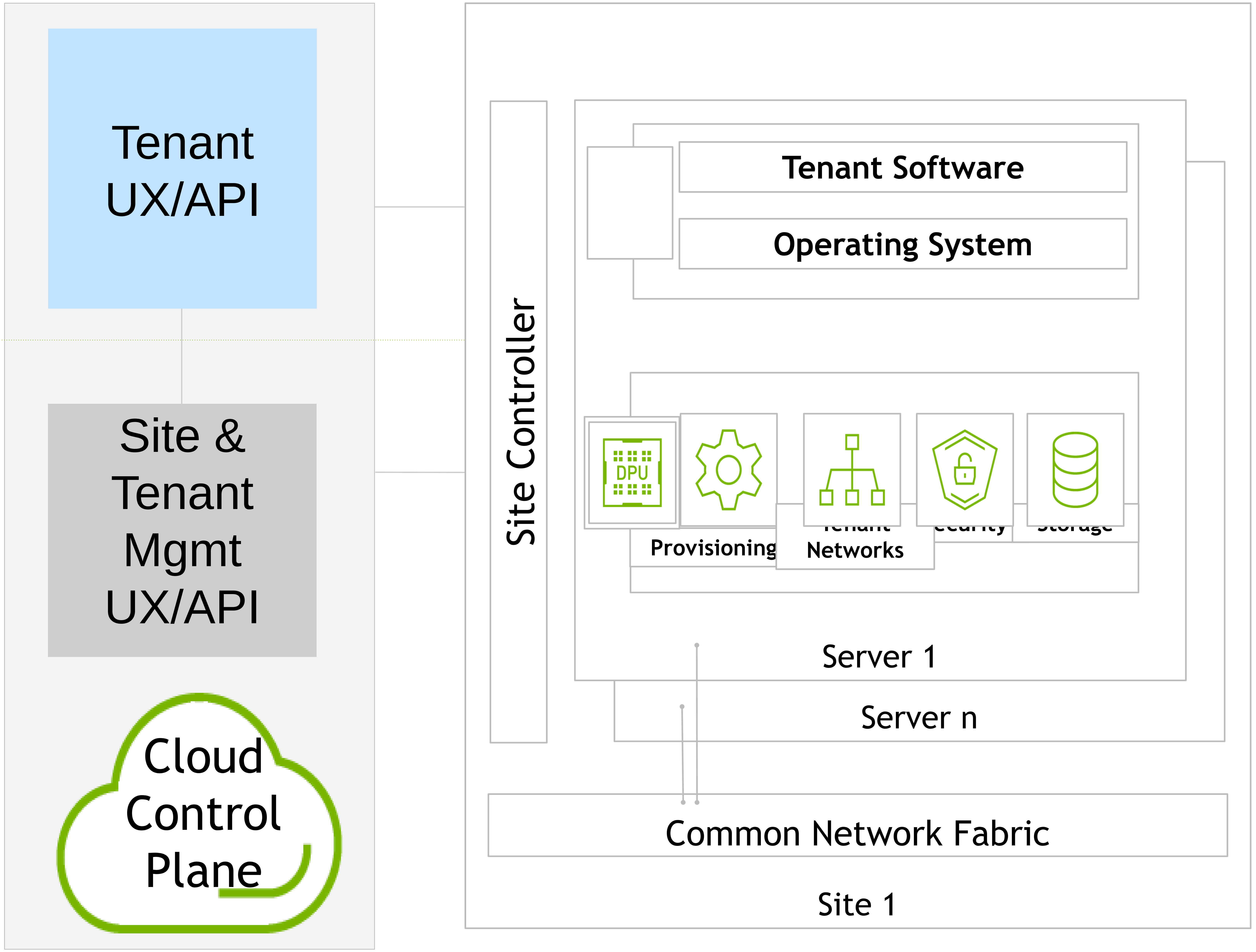
- Effective security
- Automated resource management

Cloud-based service vs. packaged SW

- Single locus of infra management
- Maximize security, consistency, manageability

Examples of cloud-managed services vs. pkg SW

- IAM, Virus SW, Kentik NW observability, Splunk DA



Tenant UX/API
Site & Tenant Mgmt UX/API
Cloud Control Plane
Site Controller
Tenant Software
Operating System
DPU
Provisioning
Tenant
Networks
ecurity
Storage
Server 1
Server n
Common Network Fabric
Site 1