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

External Aggressor

Protect with firewall, IAM

Isolate from supply chain attack

3rd party library

Data ingest

PII, valuable model

Encrypted on wire, at rest, use TEEs

Least privilege

Inference

Training

Analysis

Visualizaition

Anomaly detection

3rd party service

Data preproc
Making enforcement more fine-grained
Down to the container/VF level

Course-grained enforcement

Switch

Node
Node
Node

Fine-grained enforcement with control groups

Process
Process
Process
Process

Node
Node
Node

Cluster

Course-grained enforcement

Fine-grained enforcement

Node

DPU

VF
VF

Compute node

Container
CNI
CSI

Container
CNI
CSI

ISC23, Securing HPC w/o Air-gapping, Newburn 3
Confidential computing

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

ISC23, Securing HPC w/o Air-gapping, Newburn
Shift storage functionality to the DPU

Credentials supplied to the DPU vs. the untrusted compute node

Diagram:
- Host:
  - Connect
  - Map/translate
  - Encrypt
  - Service level

- DPU
- Mount
- Connect

- Filer
DPU as a gate to authorization

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

Node 1
User A
User B

Node 2
User C

Filer

Scheduler
User-node mapping
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

ISC23, Securing HPC w/o Air-gapping, Newburn