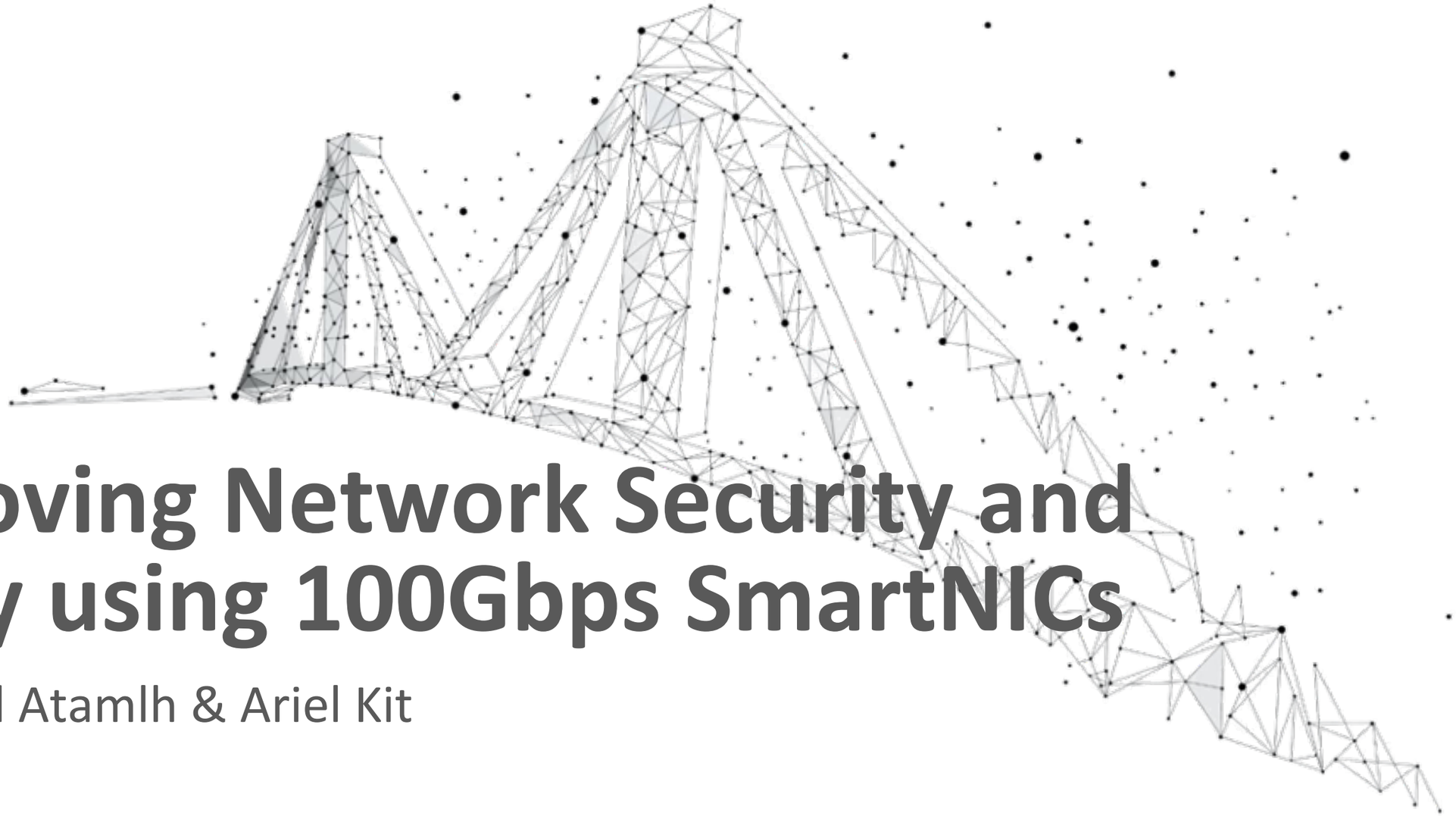


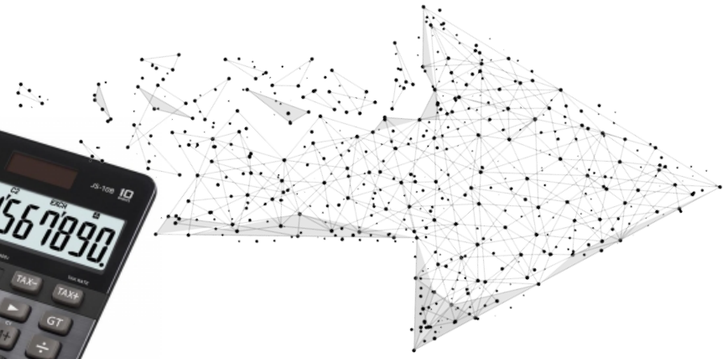
Improving Network Security and agility using 100Gbps SmartNICs

Dr. Ahmad Atamlh & Ariel Kit

January 2020

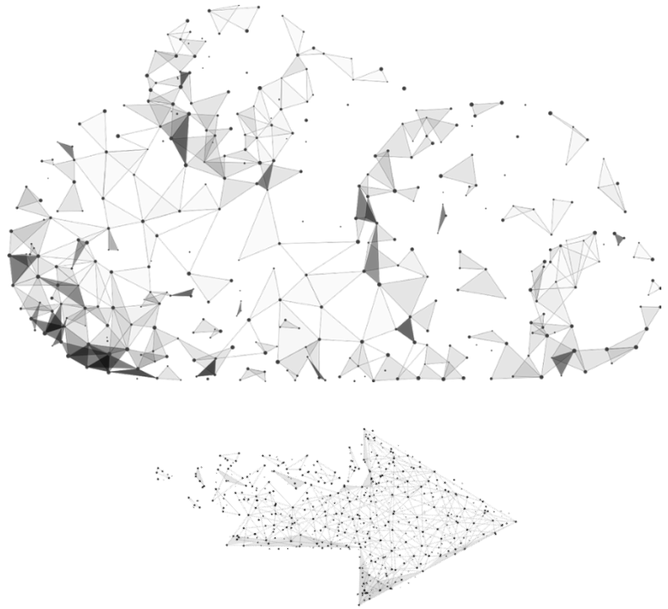
Evolution

Virtualizing Everything…



Evolution

Moving to the cloud…

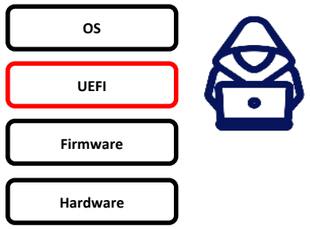


NETFLIX

Security Challenges: Platform Security

What is changing?

- Bare Metal clouds are widely adopted
- Zero Trust in the data center
- Data centers deployed at global sites
- Cloud services are moving to the edge and third-party locations
- After math of known hardware and firmware attacks



Firmware Attacks

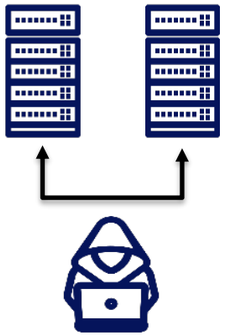
How is it being addressed today?

- Hardware root-of-trust based solutions
- Secure boot becomes a mandatory requirement
- Attestation
- New security models introduced by leading vendors (e.g. Cerberus)

Security Challenges: Cloud Architecture

What is changing?

- Mixture of public cloud, private cloud and hybrid cloud
- East-West traffic, cloud Virtualization and VM migration
- Bare Metal clouds are widely adopted
- Data centers deployed at global sites
- Cloud services are moving to the edge and third-party locations
- Zero Trust in the data center



Zero Trust

How is it being addressed today?

- Perimeter based security is no longer sufficient
- Increase in using encryption at application level impacting server performance
- Workload protection and micro-segmentation solutions are getting traction
- Security agents are widely used
- Switch ACLs are exhausted to secure the Bare Metal servers

Security Challenges: Regulation & Compliancy

What is changing?

- General Data Protection Regulation (GDPR) for data privacy of EU citizens
- ANSI, CNIL and OVI for Cybersecurity in France
- Updated Australian data privacy regulations (OAIC)
- California Consumer Privacy Act (CCPA) bill for privacy rights
- Compliancy enforcement becomes stricter

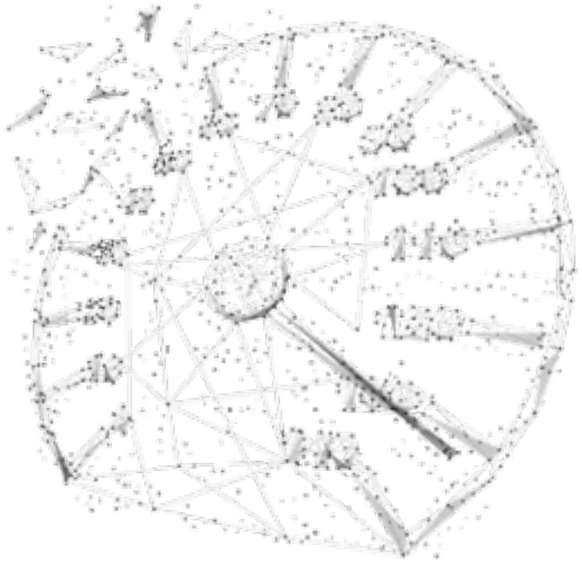
New Security Regulations

How is it being addressed today?

- Organizations adopt new security models such as Micro-segmentation
- Increase in end-to-end encryption of data-in-motion
- New data-at-rest protection schemes are being implemented
- On-going re-structuring of data center architecture and purchasing

Main Technology Trends

Network Performance and Flexibility



Intelligence Moving to the Network

Scale-Out Architectures

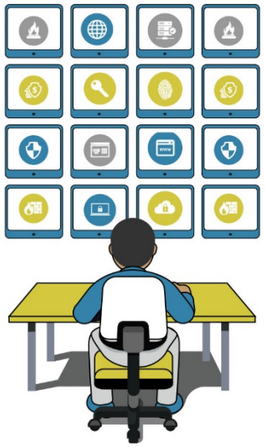
HPC | Cloud | Telco | Storage | Financial | Machine Learning

SmartNIC – an Offload Strategy

Commodity NIC

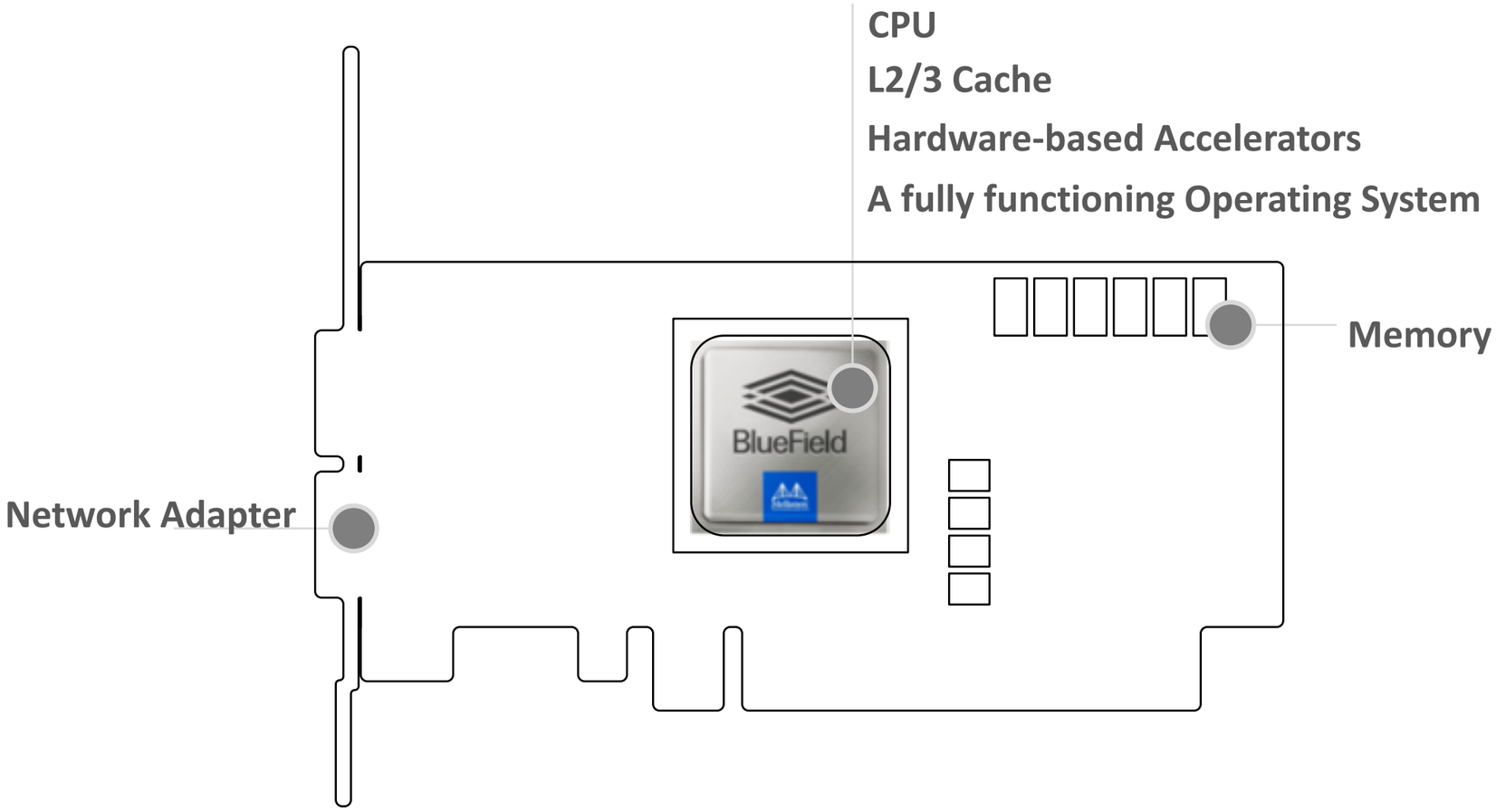
- Modern data centers suffer from task overload
  - Faster networking, cloud, overlay, SDN & NFV
- Host CPUs end up spending cores on network steering

SmartNIC

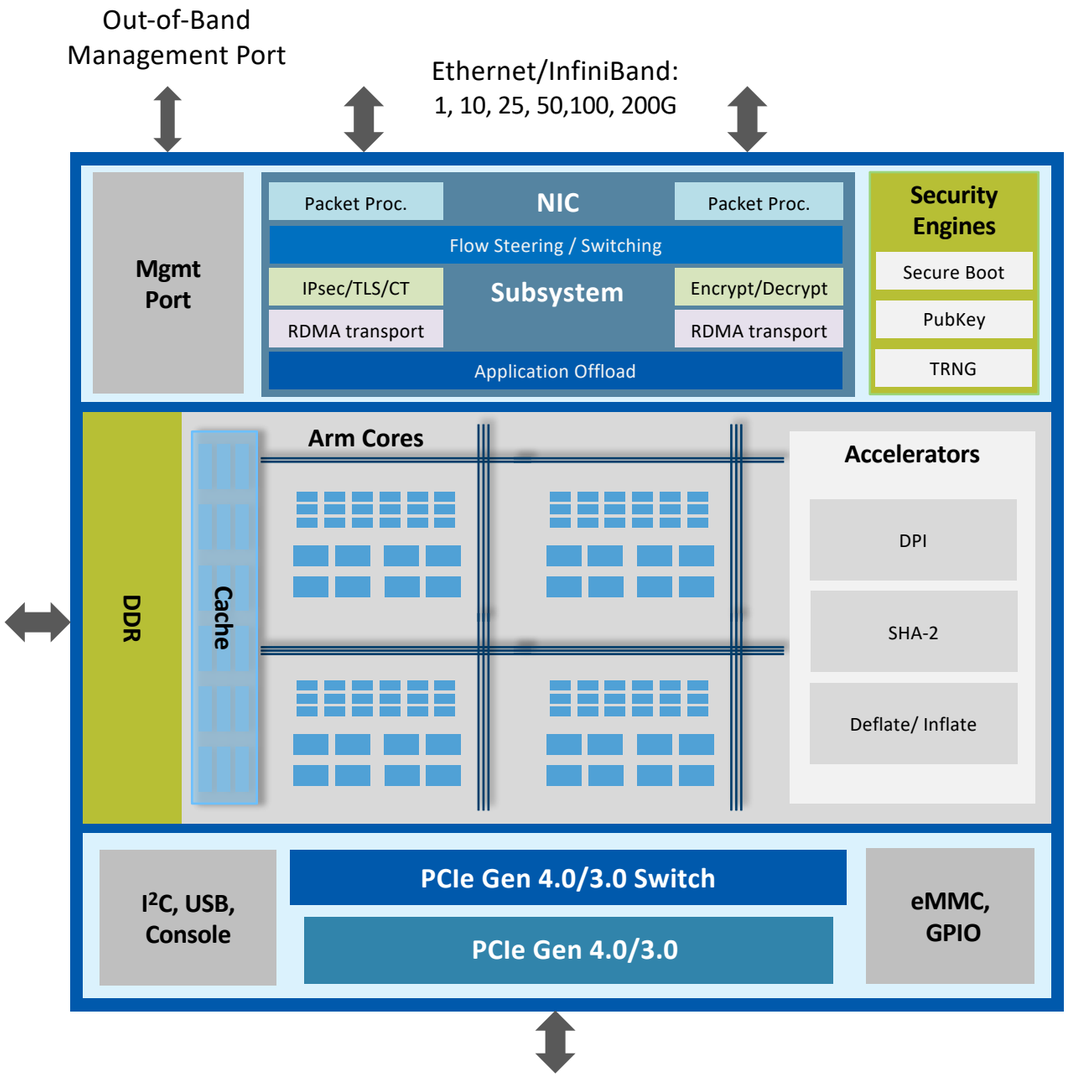


- SmartNIC frees up host CPUs by utilizing:
  - Hardware accelerations
  - Multicore array of Arm cores
  - Offload the Networking, Storage and Security controls

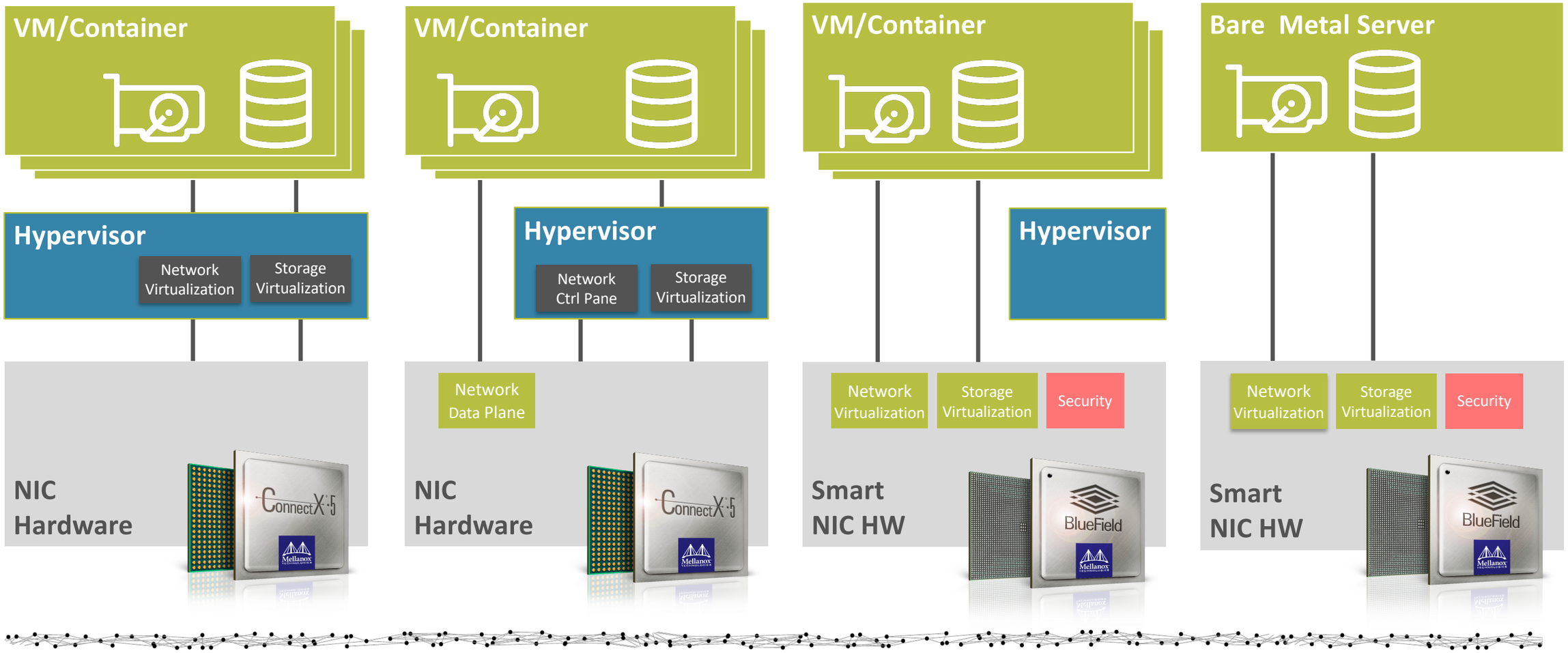
SmartNIC is a Computer



SmartNIC Reference Block Diagram



Software Defined Network, Storage, Security Transition



Building a Secure Data Center

Security Applications and Agents

- Web application firewall, key orchestration, memory forensic, anomaly detection, security analytics, …

Accelerated L2-7 Firewall and Isolation

- L3-4, stateful connection tracking and DPI based firewalls

Accelerated Cryptography

- Inline acceleration for Networking (TLS, IPSEC) and Storage (XTS)

Secure Software and Firmware

- Functional isolation, secure software update,…

Secure Hardware

- Secure boot, secure enclave, hardware isolation, Arm Trust Zone, ..

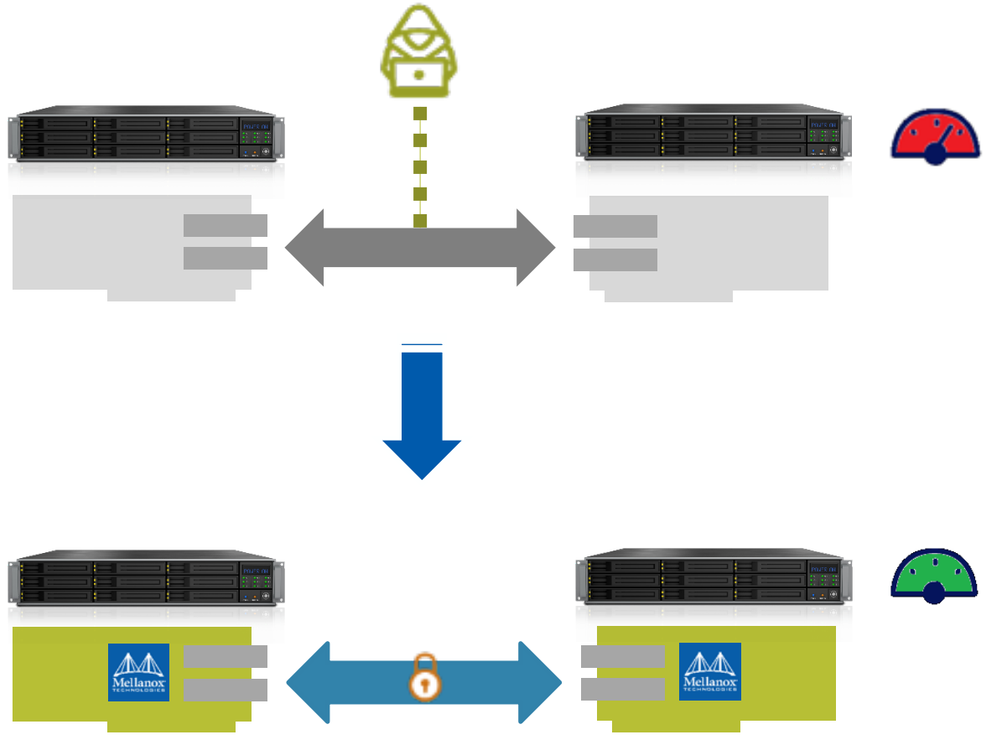
"Zero Trust" paradigm

Security shift from the perimeter to the heart of the cloud multi tenant data center

Innovative Security Approach

Inline encryption acceleration

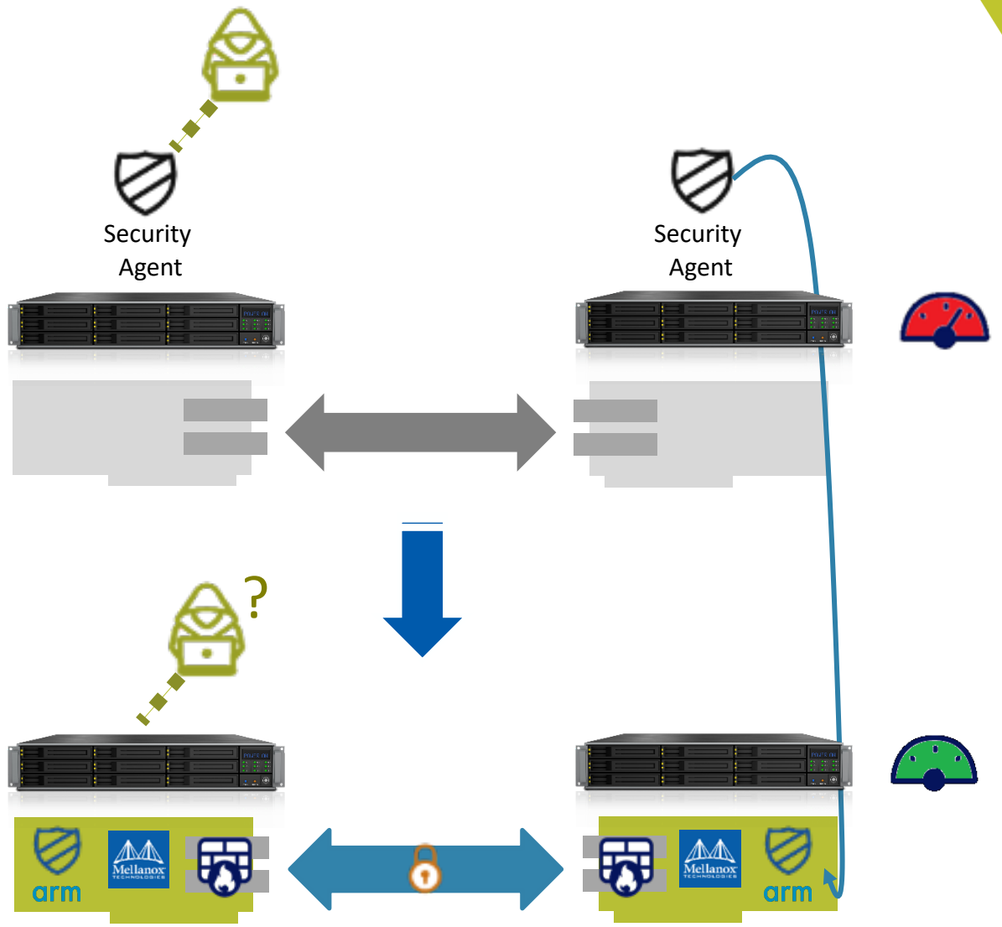
- Protection of Data-in-Motion and Data-at-Rest
- Encryption\decryption is done as another data-path action
- **“Zero Utilization”-** Host CPU is fully offloaded from encryption functions
- SmartNIC enable fully Isolated control plane and key management (Transparent Mode)



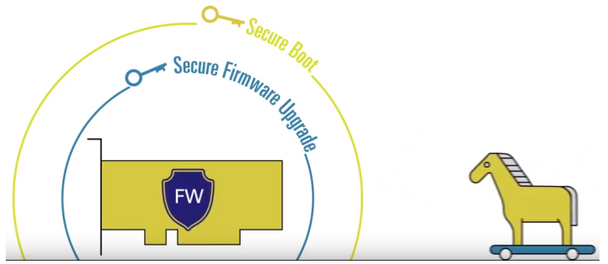
Innovative Security Approach

Securing the cloud end-point

- SmartNIC Arm cores are running Linux OS and deploy security agents
- Bare-metal, VM and Container complete visibility and line-rate mitigation
- **“Zero Trust”** – Security agents are running on SmartNIC in an isolated environment
- **“Zero Touch”** – SmartNIC implements security infrastructure independent of the host

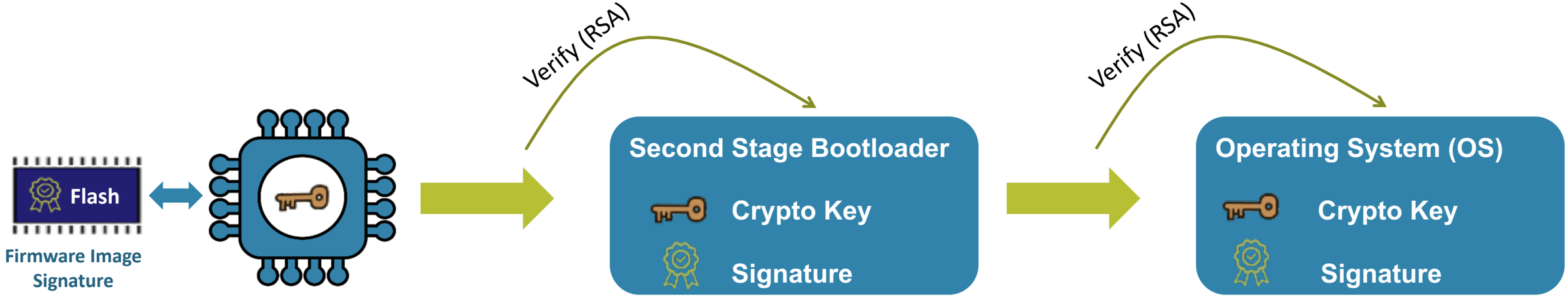


Hardware Root-of-Trust: Secure Boot



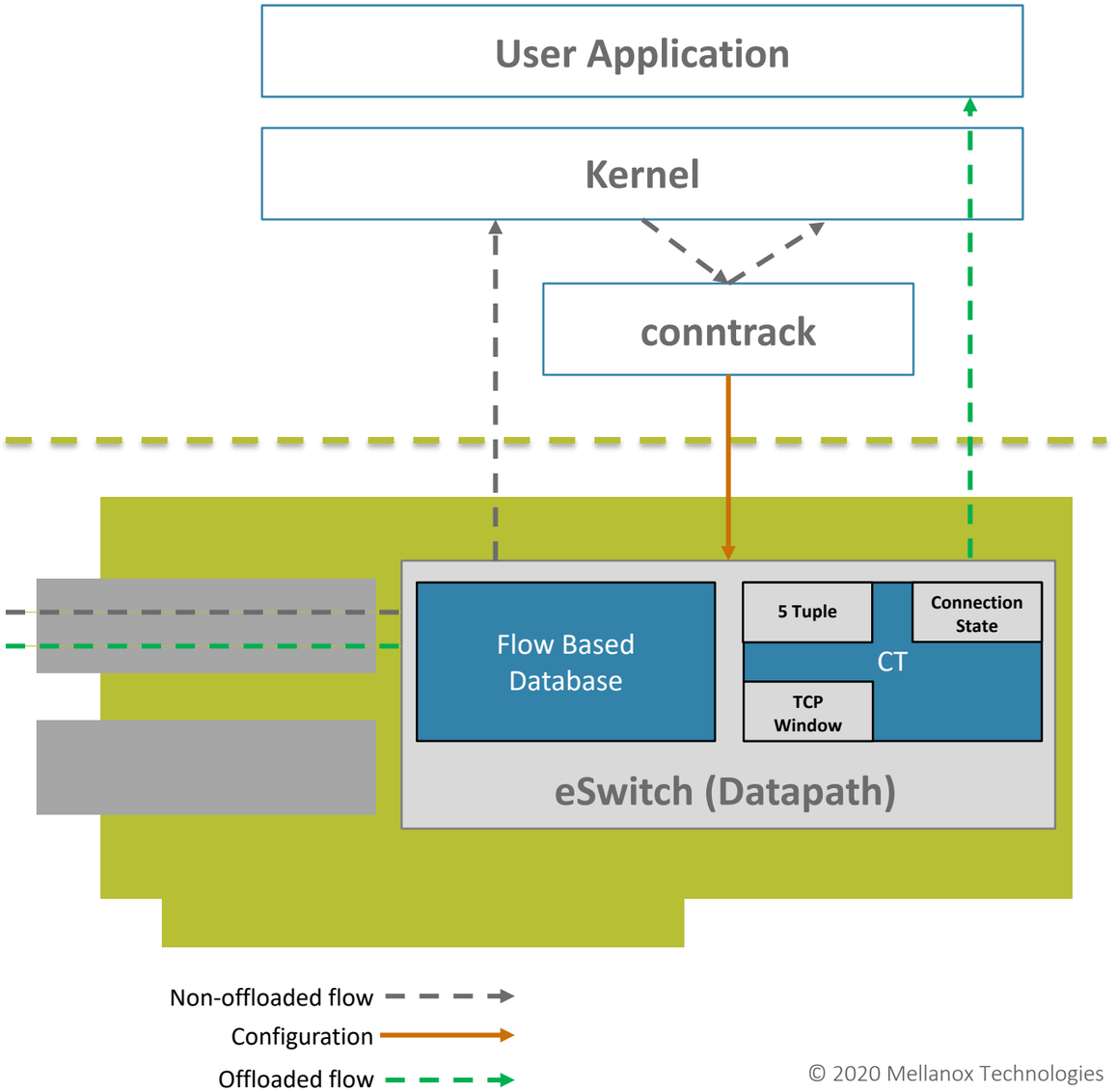
- Protect the product from supply chain and firmware attacks
- Assure the authenticity and integrity of the off-chip storage
- Root-of-Trust is an on-chip ROM code and OTP (One Time Programmable)

- Secure Boot in SmartNIC
  - RSA based with SHA2-512 (of 4K public keys) burned in EFUSE
  - Follows NIST spec ***SP 800-147*** "*BIOS Protection Guidelines*"
  - Hardware roll-back protection information is included in the device-specific digest calculation
  - Secure Firmware Update must be enabled



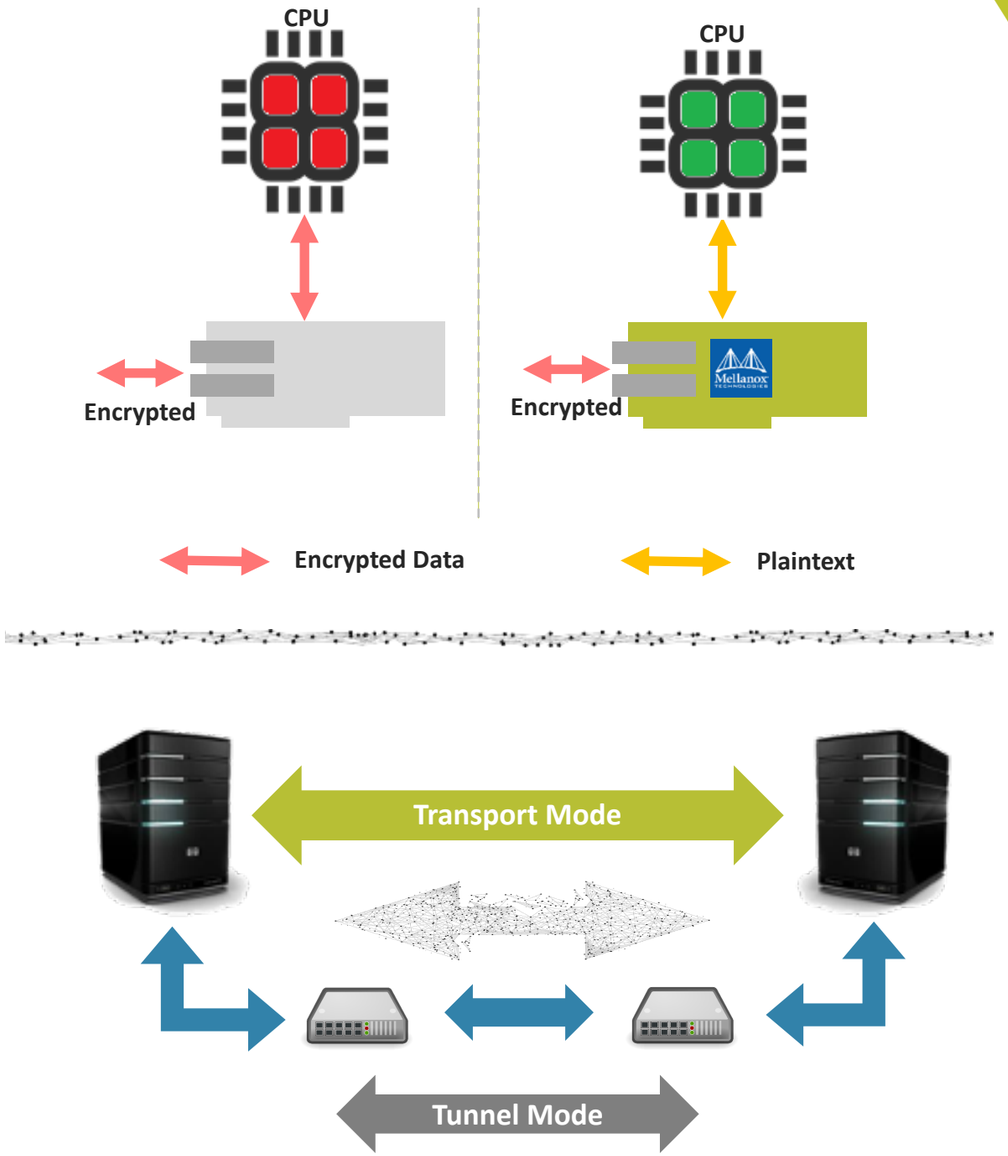
Connection Tracking Acceleration

- Hardware offload of Connection Tracking
  - Allows to inspect and restrict connections to services based on their connection state
  - Check TCP connection state in hardware in real-time
  - Hardware counter per flow for activity/aging
- Offload flow
  - Packets of new connection are forwarded to the SmartNIC CPU
  - Software can then
    - Complete the TCP Hand-Shake
    - Drop the packet
  - Driver adds the connection (5-tuple) to the hardware using Kernel
  - Following packets of the TCP streams are forwarded directly to the VF
- Protect the host from attacks in wire speed



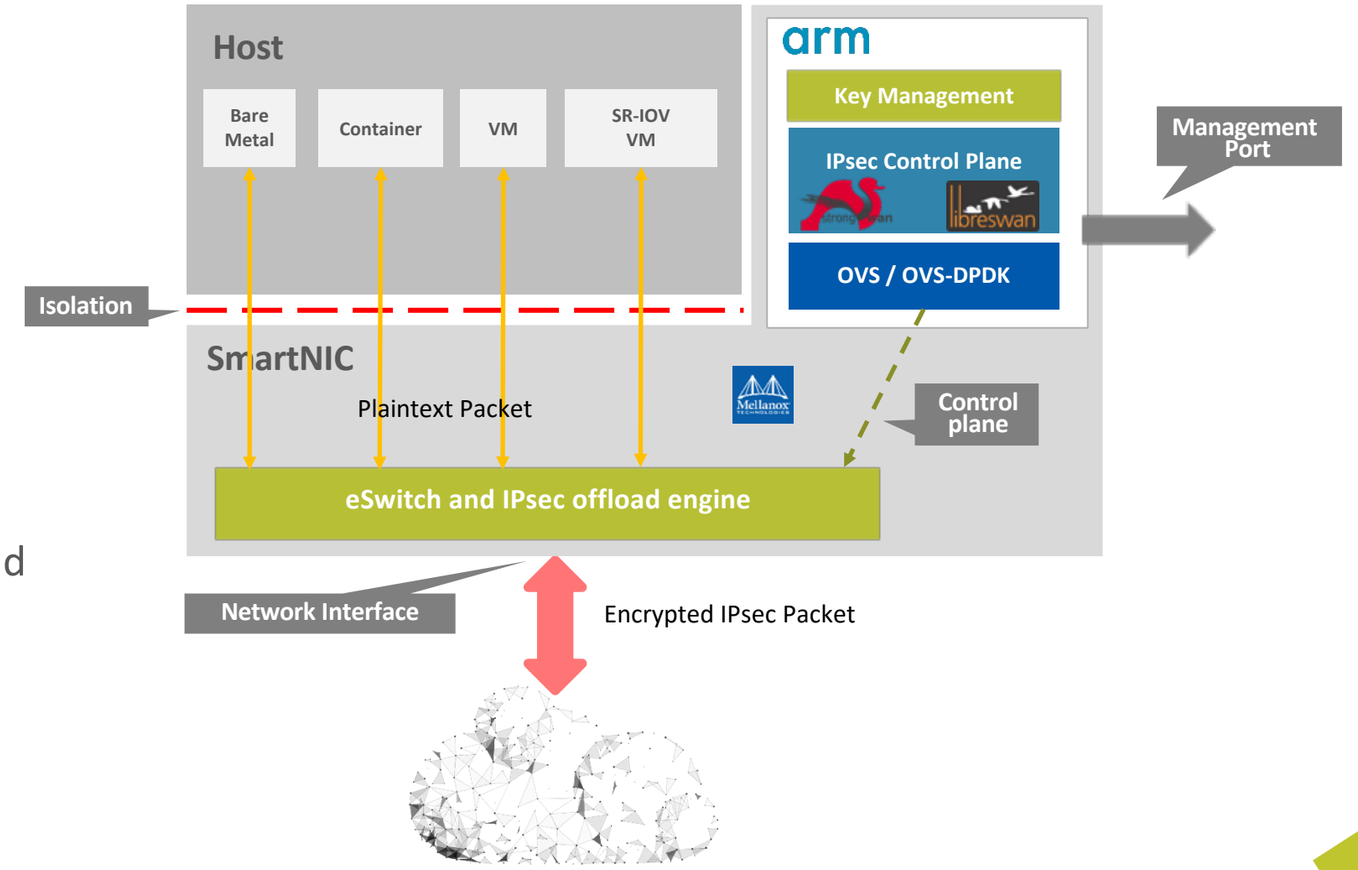
IPsec Inline Encryption of Data-in-Motion

- Encryption/decryption at 100Gb/s bidirectional
  - Lower CPU utilization with significant higher performance
  - Protocol encapsulation and data plane offloads (aware/un-aware modes)
- Inline offload
  - Inline with other offloads (tunneling, TLS, OVS, SR-IOV etc.)
  - Removes software overhead of invoking accelerator (lookaside roundtrip)
  - IPsec key management in software
- Support Transport mode and Tunnel mode
- Use-cases
  - East-west data center encryption
  - Transparent IPsec (SmartNIC and Hypervisor)
  - Encrypted bare metal cloud (SmartNIC)



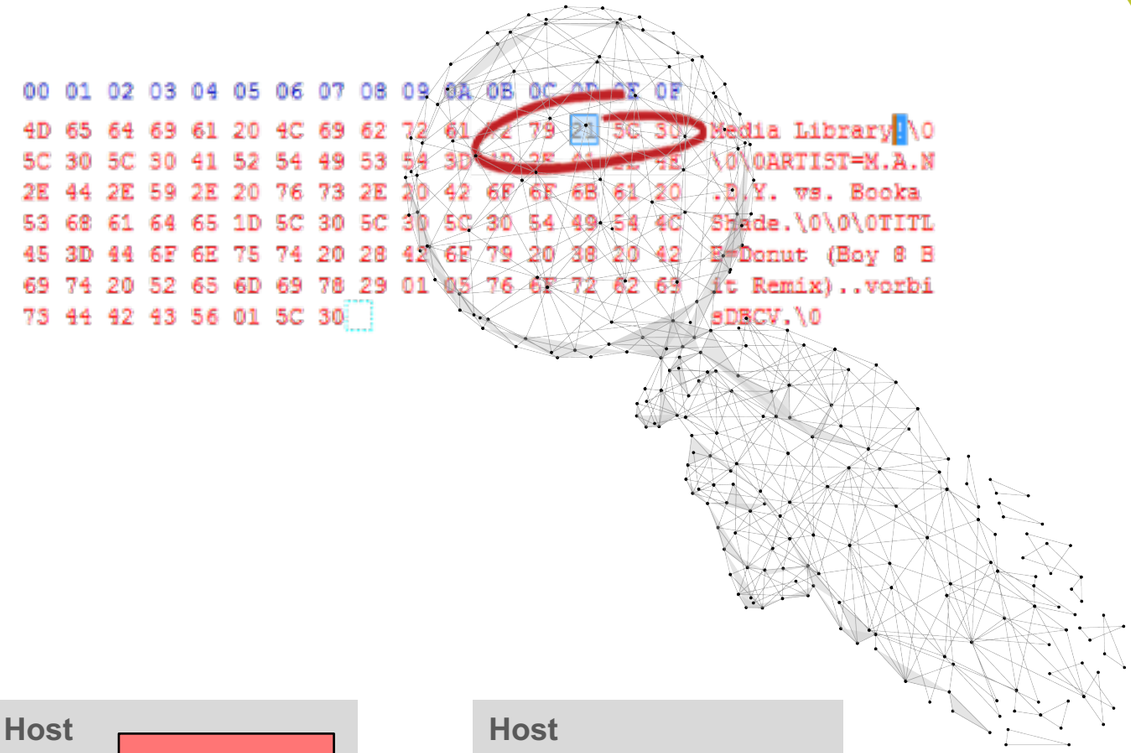
Transparent IPsec with SmartNIC

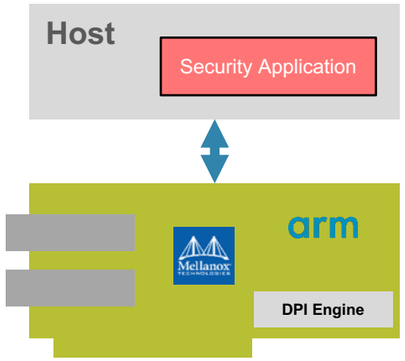
- Host is un-aware that traffic is encrypted
- Intensive cryptography functions are handled by the SmartNIC up to 100Gbs rate
- Key management done on the Arm cores in an isolated trust domain
- Scalable and agnostic
- Address the increasing demand of privacy in existing clusters
- Network steering
  - Kernel implementation (XFRM) with OVS offload
  - DPDK implementation running in Arm with DPDK offload (rte_security)



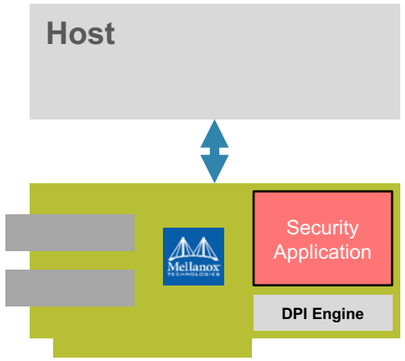
DPI for Security

- Analyze IP flows and files for malicious unwanted content and DPI classification
- DPI processing is widely used by
  - Next generation Firewalls (NGFW)
  - Network based Application Recognition
  - Intrusion Detection and Prevention solutions
  - Cyber security DPI based applications
  - Security Information and Event Management (SIEM) systems
- SmartNIC with DPI engine enables
  - Application recognition at real time
  - Flow rules based filtering for NGFW
  - Host Introspection and memory forensics
- Modes of Operation
  - Accelerator card for security applications
  - SmartNIC for endpoint security
  - Security appliance (bump-in-wire)





Security Accelerator Card



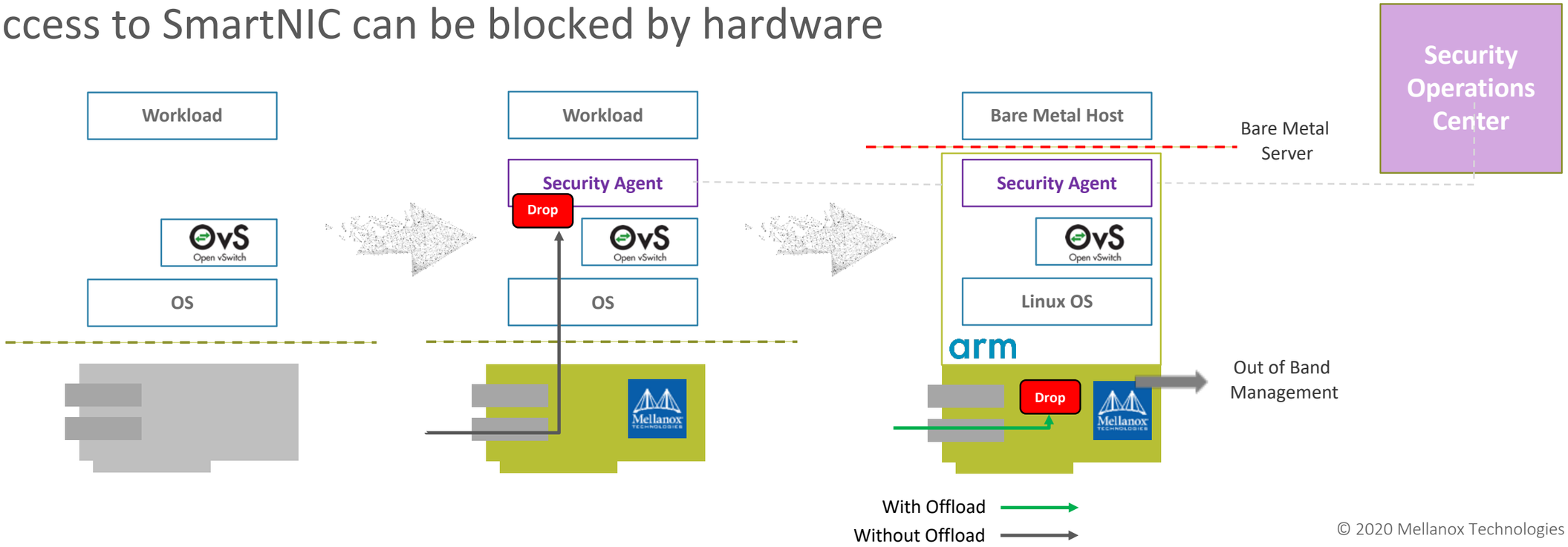
SmartNIC for Security

Isolated Security Trust Domain with SmartNIC

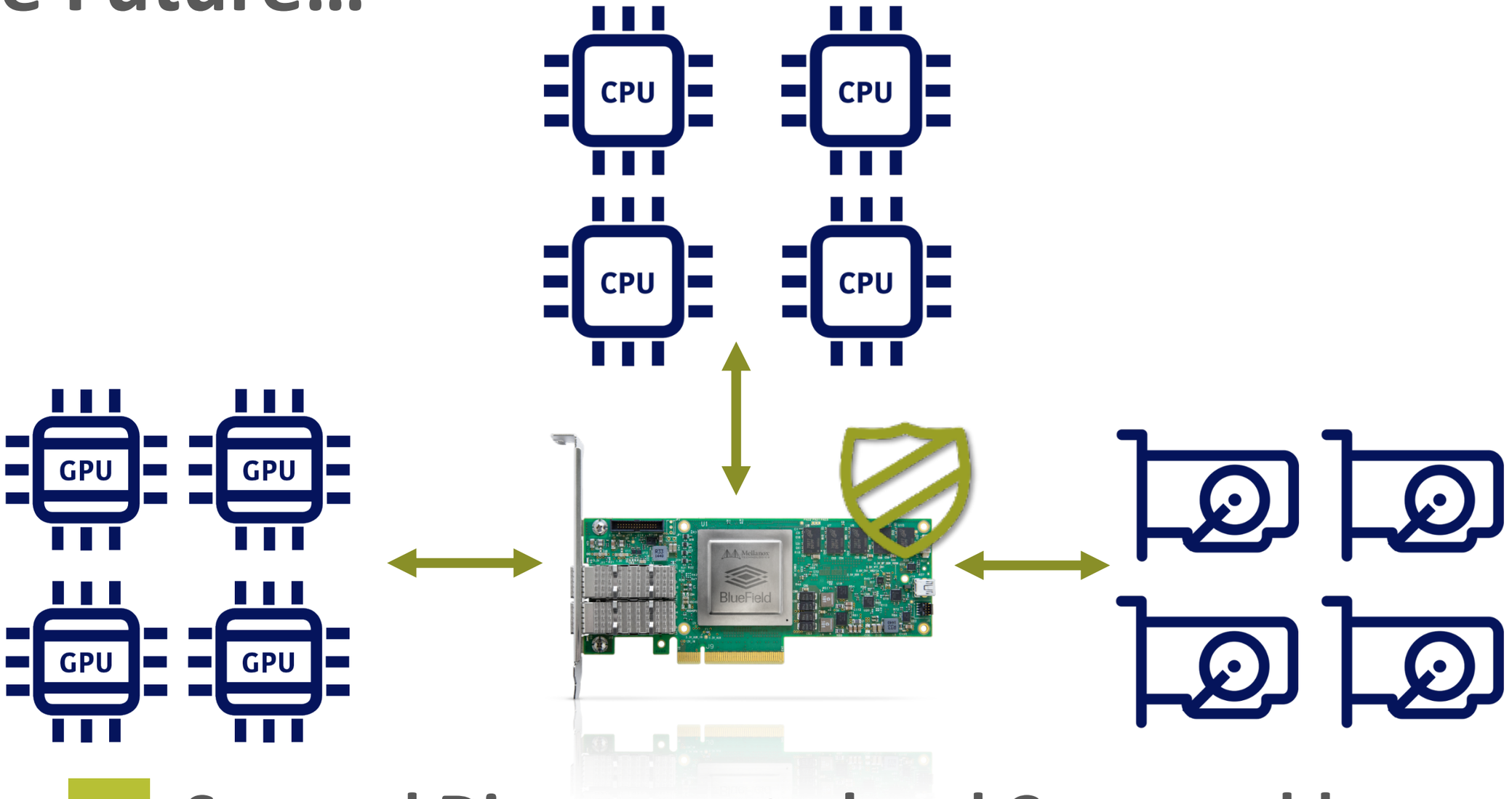
- SmartNIC is a computer in-front of a computer
- Isolation and Offload
  - Security infrastructure functions fully implemented in SmartNIC
  - CPU intensive security tasks are offloaded to the SmartNIC Arm cores and hardware accelerators
- Security functionality in a separated trust domain
  - SmartNIC enforces policies even on a compromised host
  - Host access to SmartNIC can be blocked by hardware
  - Enables agentless end point protection schemes
- Arm TrustZone enable a Trusted Execution Environment (TEE) for key management and more..

The Path to Agentless Security

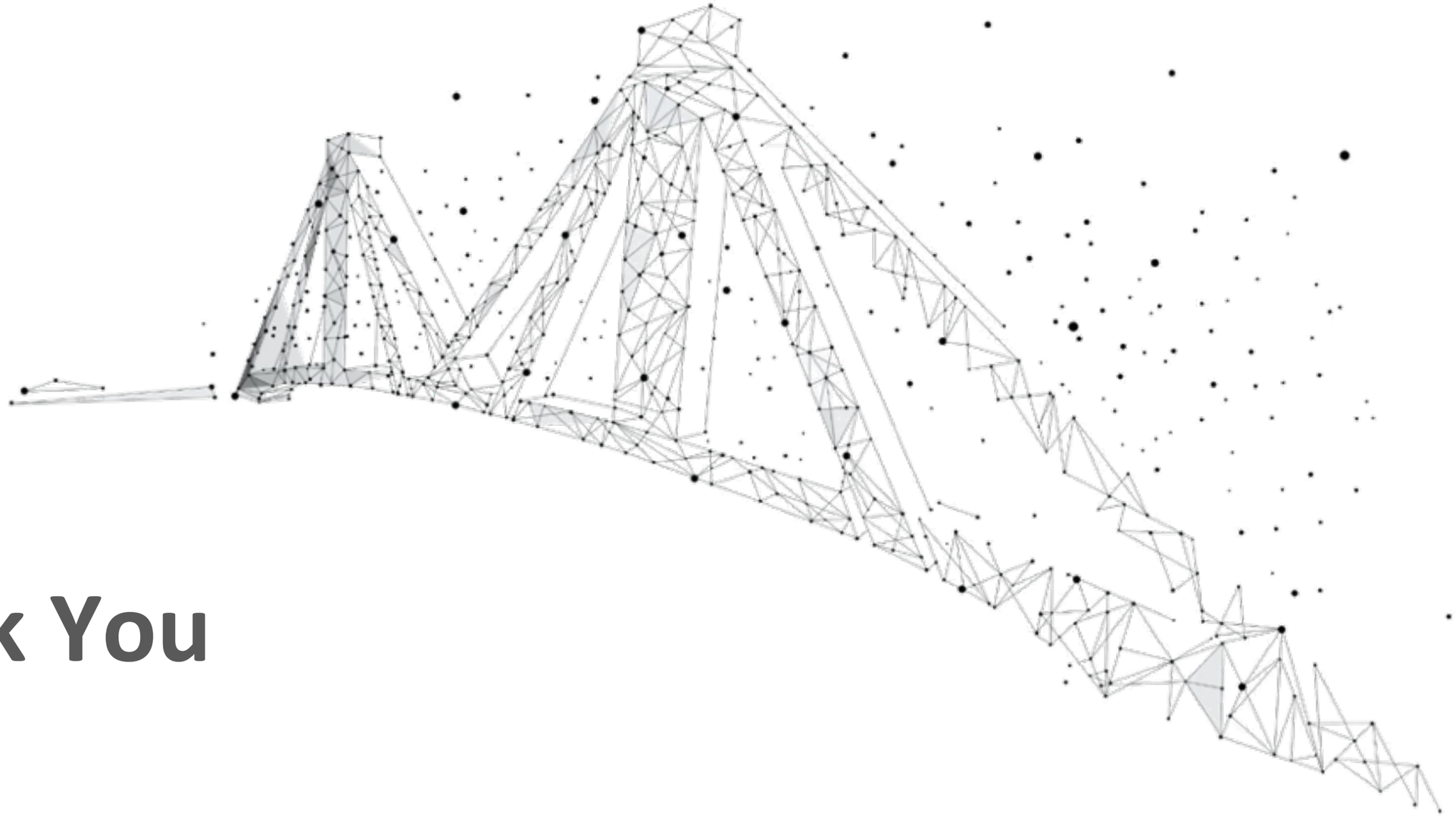
- ✓ Security agent is running on the SmartNIC cores in a separated trust domain
- ✓ Security agent introduces complete network level visibility
- ✓ Enforcement policy is accelerated in SmartNIC hardware
- ✓ SmartNIC enforces policies even on a compromised host
- ✓ Host access to SmartNIC can be blocked by hardware



The Future…



Secured Disaggregated and Composable



Thank You