
AWS
re:Invent

CMP301

Powering next-gen Amazon EC2: Deep dive on the Nitro System

Abby Fuller

Principal Security Engineer, EC2 Nitro

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Before we start

re:Invent is a little different this year

Since these talks don’t have Q&A, you can tweet or email me and I’ll help if I can!

@abbyfuller

abbyfull@amazon.com



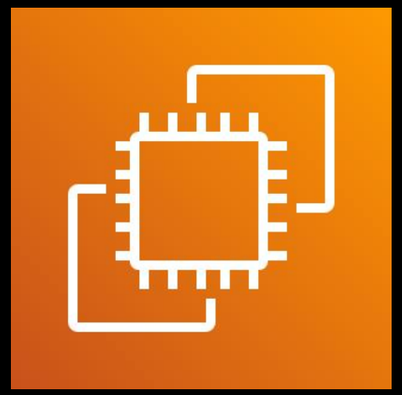
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Nitro?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Nitro?



Amazon EC2 Nitro

Launched in November 2017

In development since 2013

Purpose-built hardware and software

Custom hypervisor developed for AWS

Every new instance launch uses Nitro

Nitro in three parts

Nitro cards



- VPC networking
- Amazon Elastic Block Store (EBS)
- Instance storage
- System controller

Nitro security chip



- Integrated into motherboard
- Protects hardware resources
- Hardware root of trust

Nitro hypervisor



- Lightweight hypervisor
- Memory and CPU allocation
- Bare metal-like performance

Key aspects of Nitro

Software device models replaced by software-defined hardware devices

Amazon EC2 system changes modeled as hardware events (NVMe or elastic network adapter (ENA) hot plug, ACPI power state changes, etc.)

Extension of microservices model into hardware

- ENA, NVMe protocols are hardened APIs, behind which we can innovate
- Data hiding and service decomposition

Software elements are also microservices, all dynamically update-able

- No virtual machine (VM) downtime for even the largest updates

Let’s dig a little deeper into the components



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Nitro cards

Nitro card for VPC

- ENA controller
- VPC data plane (encapsulation, security groups, limiters, routing)

Nitro card for Amazon EBS

- NVMe controller
- Amazon EBS data plane (encryption support, NVMe to remote storage protocol)

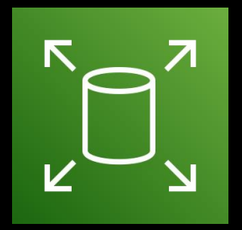
Nitro card for instance storage

- NVMe controller
- Instance storage data plane (transparent encryption, limiters, drive monitoring)

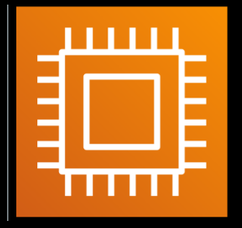
Nitro card controller

- Provides passive API endpoint
- Coordinates all other Nitro Cards, Nitro Hypervisor, and Nitro Security Chip
- Controller Hardware (root of trust, provides measurement and attestation)

Nitro security chip (more on that in a second)

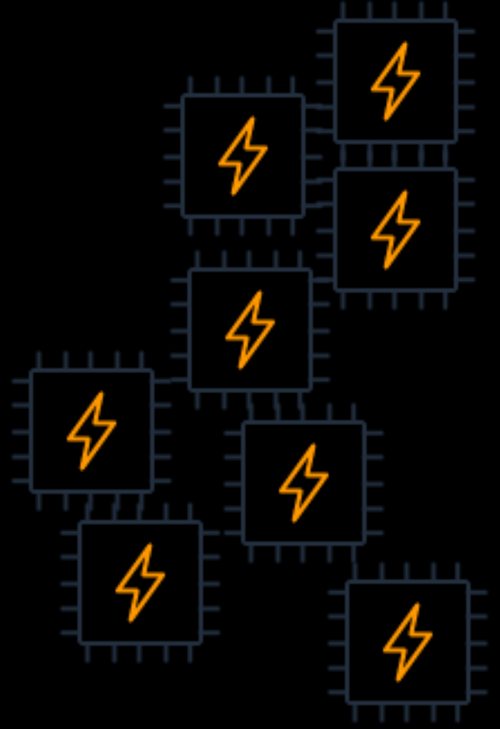








Nitro security chip



Custom microcontroller that traps all I/O to non-volatile storage

Controllable from the Nitro controller to hold system boot – various modes for measurement, validating, and updating firmware, etc.

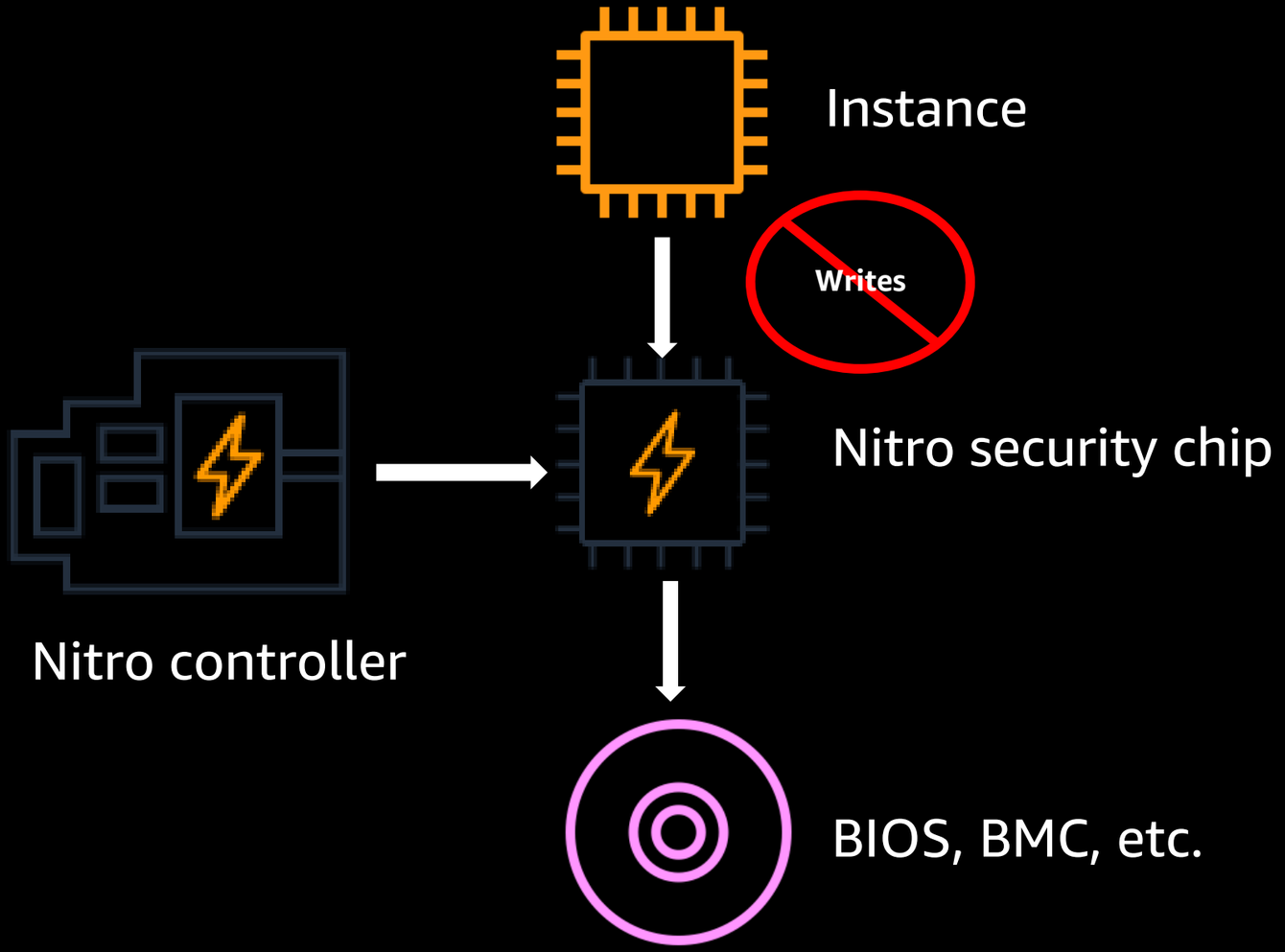
Monitors all hardware interfaces

Provides a simple, hardware-based root of trust

Nitro hardware root of trust

All write-access to non-volatile storage is blocked in hardware

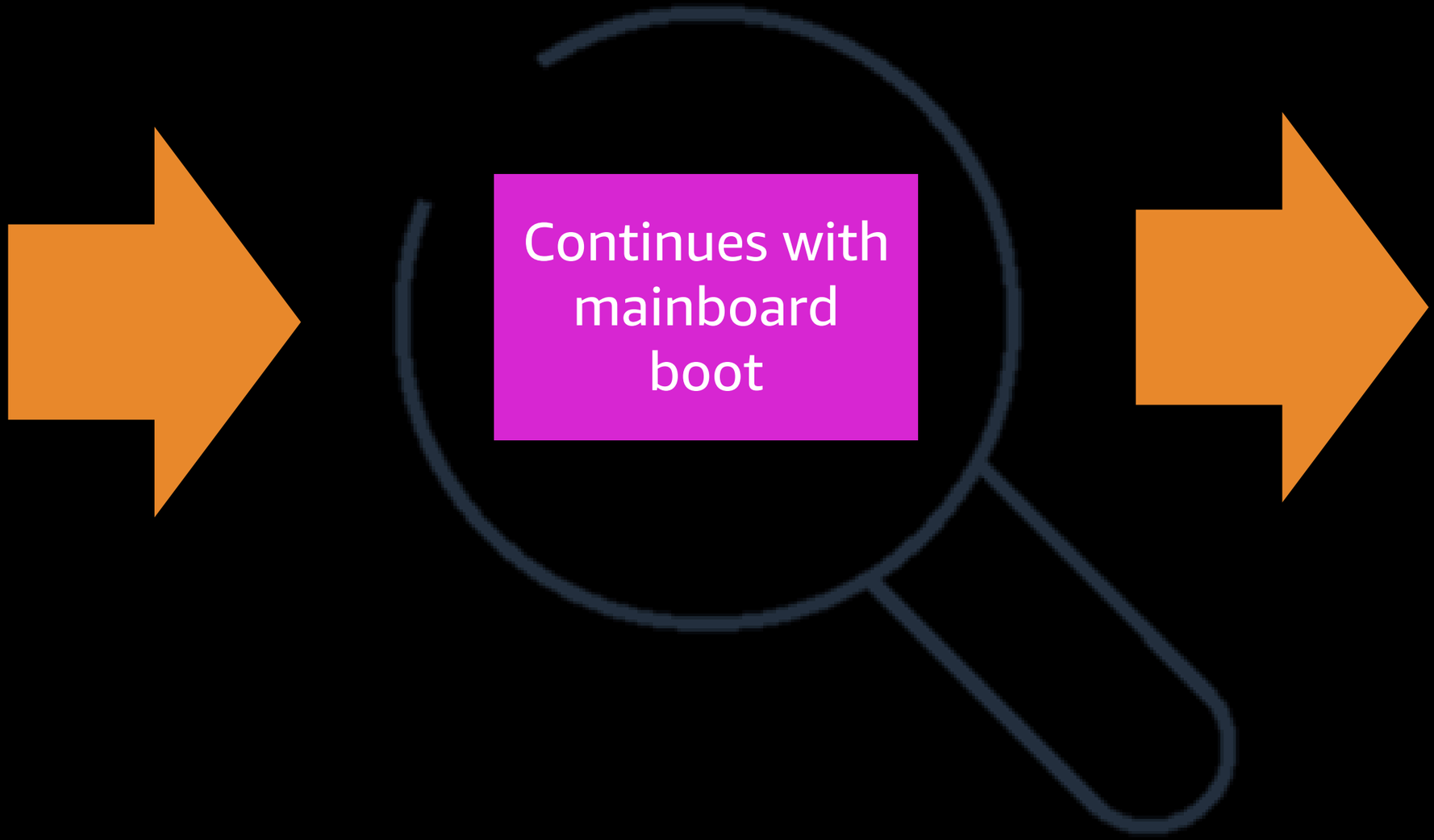
Simplification comes from offloading to cards, no legacy



Nitro hardware root of trust



Let’s zoom in on a step



Mainboard boot

Mainboard can’t update firmware (security check)

Hold mainboard in reset during powerup while firmware gets validated by the controller; if it’s validated, continue

Then, either inject known-good hypervisor, or boot customer AMI from EBS volume



How did we get here?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A quick background on virtualization

Started with Xen in 2006

- Xen enabled running multiple OS's on the same hardware
- With Xen, we had two types of virtualization –
  - PV (paravirtualization) and HVM (hardware-assisted virtualization)

With PV, runs on guests with a modified OS

- This works even on hosts with no explicit virtualization support

With HVM, guests are fully virtualized – no modified OS

- Guests get fast access to the host hardware

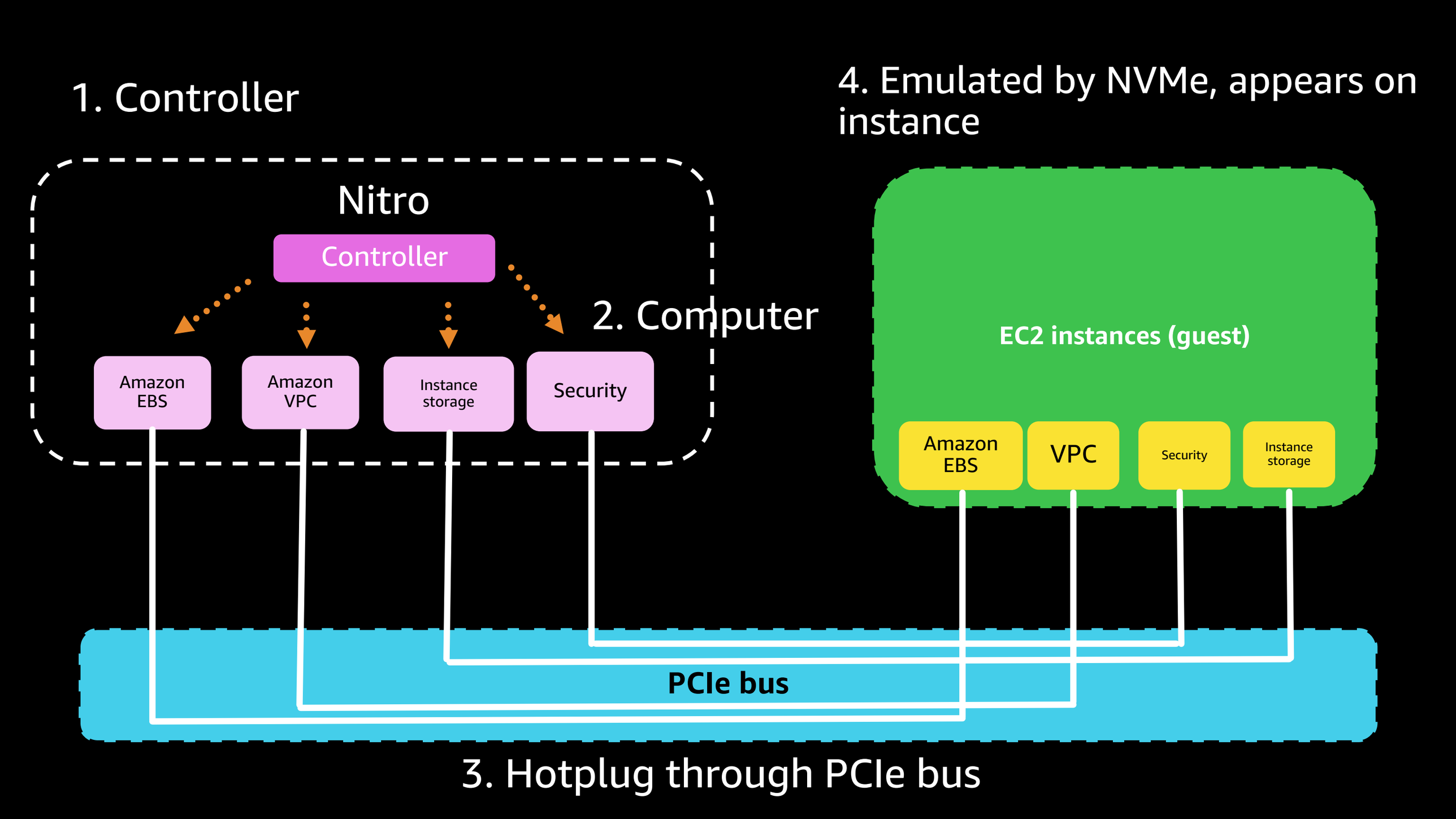
KVM and Nitro

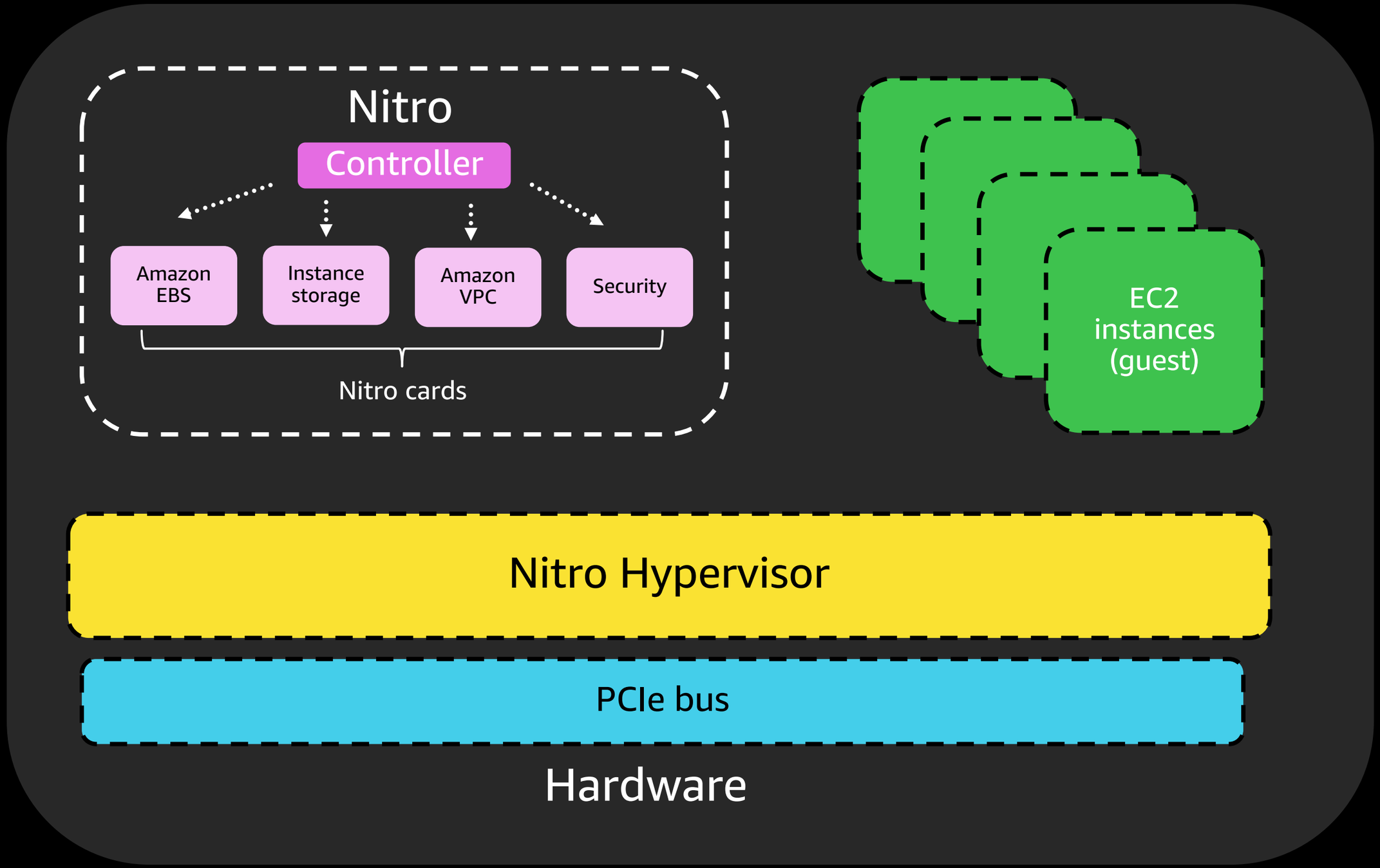
With Nitro, switched to KVM-based; Nitro provides cards and controllers for VPC, EBS, instance storage, and security; Controller also handles resource (CPU and memory) allocation

Dom0 (software device models) in Xen are replaced by software-defined hardware devices on the system bus:

Nitro controller → Nitro computer (VPC, EBS) → hot plug to PCIe → emulated by NVMe

Only Nitro controller has access to AWS network; Mainboard does not; Hypervisor only executes on behalf of instance


1. Controller
4. Emulated by NVMe, appears on instance
Nitro
Controller
2. Computer
Amazon EBS
Amazon VPC
Instance storage
Security
EC2 instances (guest)
Amazon EBS
VPC
Security
Instance storage
PCIe bus
3. Hotplug through PCIe bus


Nitro
Controller
Amazon EBS
Instance storage
Amazon VPC
Security
Nitro cards
EC2 instances (guest)
Nitro Hypervisor
PCIe bus
Hardware

Security benefits of Nitro



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Trust and simplify



Secure boot, encrypted communication channels

Hardware root of trust

- Cryptographically measure and validate the system continuously
- Higher level of trust than in traditional systems

Simplified overall stack (through offloading to cards) to minimize the Trusted Computing Base (TCB)

Limited operator access

With a typical hypervisor, administrators have unrestricted access; with Nitro, admins only have access through the limited operator API

Operators have no access to customer data, and cannot change the system in unapproved ways

No ”root” user access, no SSH

All access via AuthZ/AuthN with logging enabled



Purpose-built hardware to limit attack surface

Traditional virtualization uses general-purpose servers, which include unnecessary components; this increases the attack surface

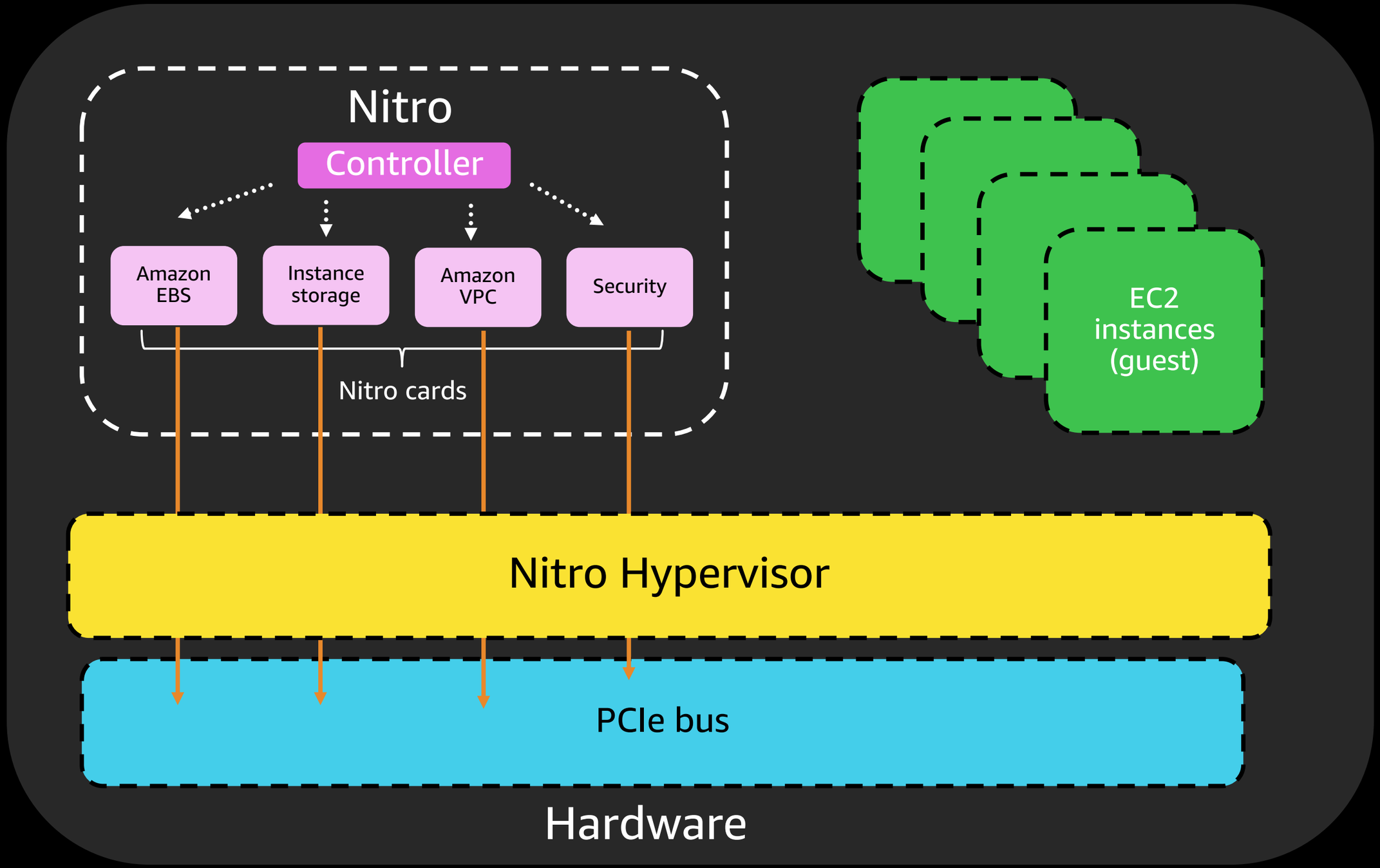
Nitro uses purpose-built hardware, with only what is necessary for the hypervisor; this reduces the attack surface

Smaller attack surface means less area for potential security vulnerabilities

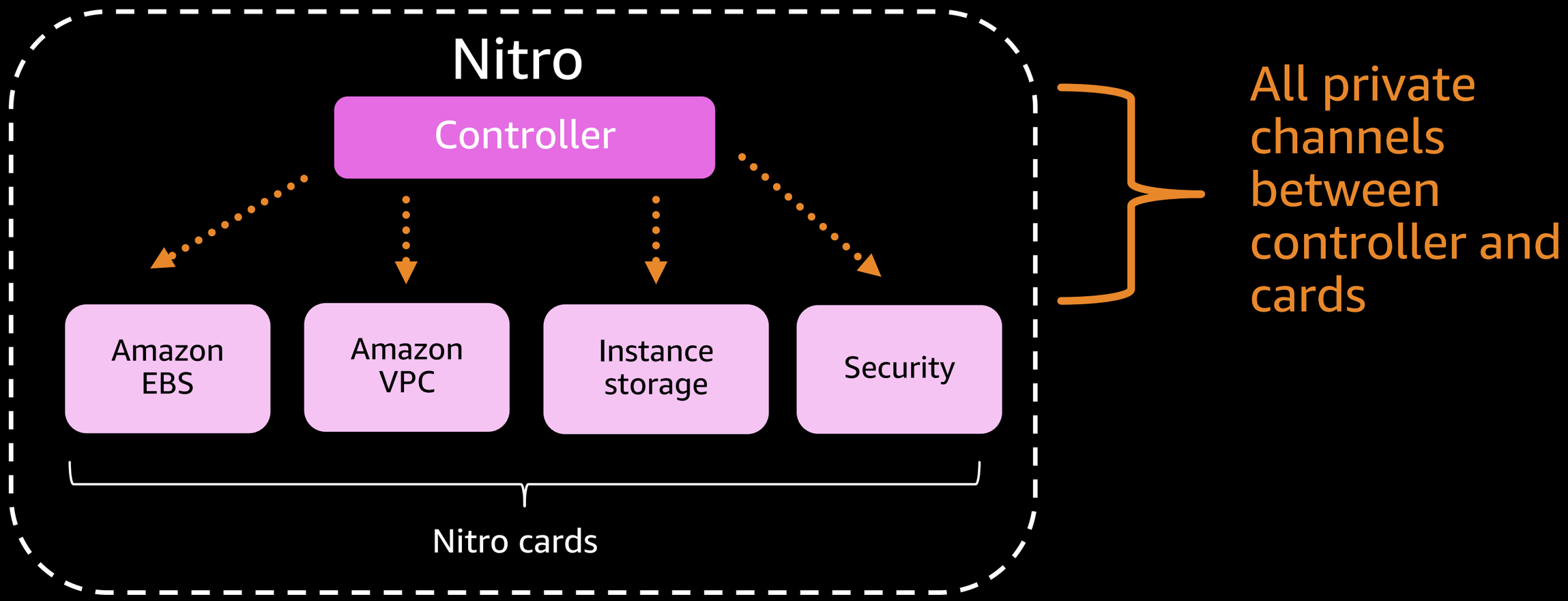
Plus, with functions being off-loaded to dedicated hardware and software (like the chips), the hypervisor stays minimal



Remember this?


Nitro
Controller
Amazon EBS
Instance storage
Amazon VPC
Security
Nitro cards
EC2 instances (guest)
Nitro Hypervisor
PCIe bus
Hardware

Private channels between controller and cards



Encryption

Hardware acceleration allows for line-rate AES-256 encryption of Amazon EBS, Instance Storage, and network without a performance hit

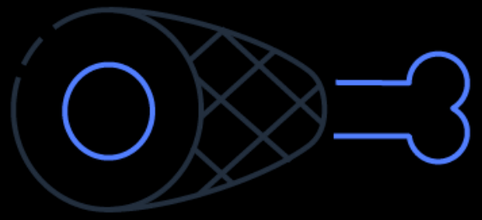
Instance storage: all data is encrypted

Amazon EBS – encryption is enforceable at the account level

Network – starting with N instance types, all direct inter-N customer traffic

- Same VPC and cross-VPC peering, cross region
- All at up to 100 Gb/s

This “encrypt-ham” is symbolic



Key management

Amazon EBS – volumes have independent lifetimes/snapshots, so key management is through AWS Key Management Service (AWS KMS)

Instance storage – local generated, used and deleted (instance lifecycle)

Amazon VPC – seed materials generated and managed by AWS KMS

In all contexts – plaintext data keys are cached/used only on Nitro computers, and are protected from “customer workload co-processor”



Passive communication



Hypervisor waits for instructions from Nitro controller

- All instructions send through private channel
- Hypervisor never initiates communication with controller
- Hypervisor never connects to the network

Nitro controller takes instructions from external control plane

- Listens on substrate network for encrypted, authenticated API calls
- Never initiates outbound connections

Outbound connections from either of these layers would be considered compromise



Nitro Enclaves

Isolated compute environments

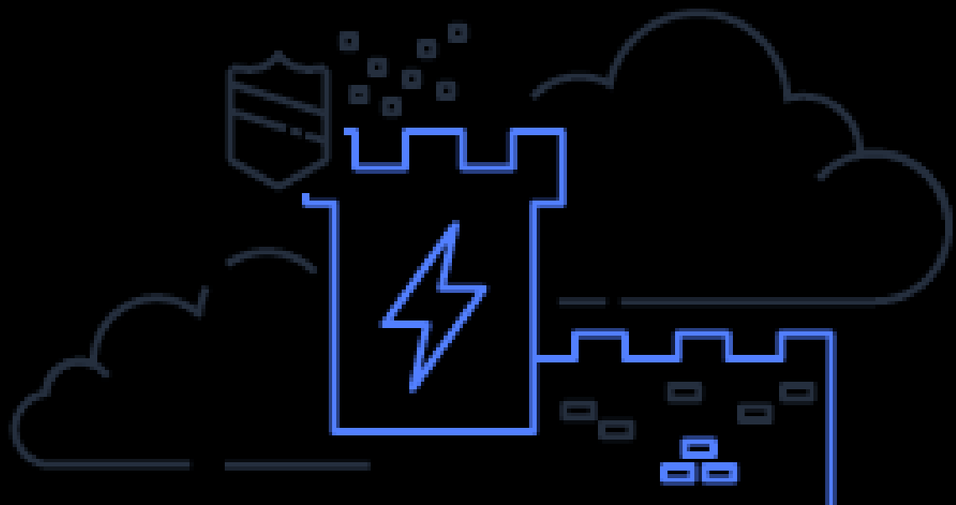
No persistent storage, no interactive access, no external networking

All communication through secure local channel (VSOCK)

Root/admin/super users on the instance don’t have special privileges to access the enclave

Good for confidential workloads (PII, etc.)

AWS KMS integration, cryptographic attestation



Thank you!

Abby Fuller

Principal Security Engineer, EC2 Nitro

@abbyfuller

abbyfull@amazon.com

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.