
aws
SUMMIT
OTTAWA | SEPTEMBER 8, 2022

SEC301

Enhance security with the AWS Nitro System

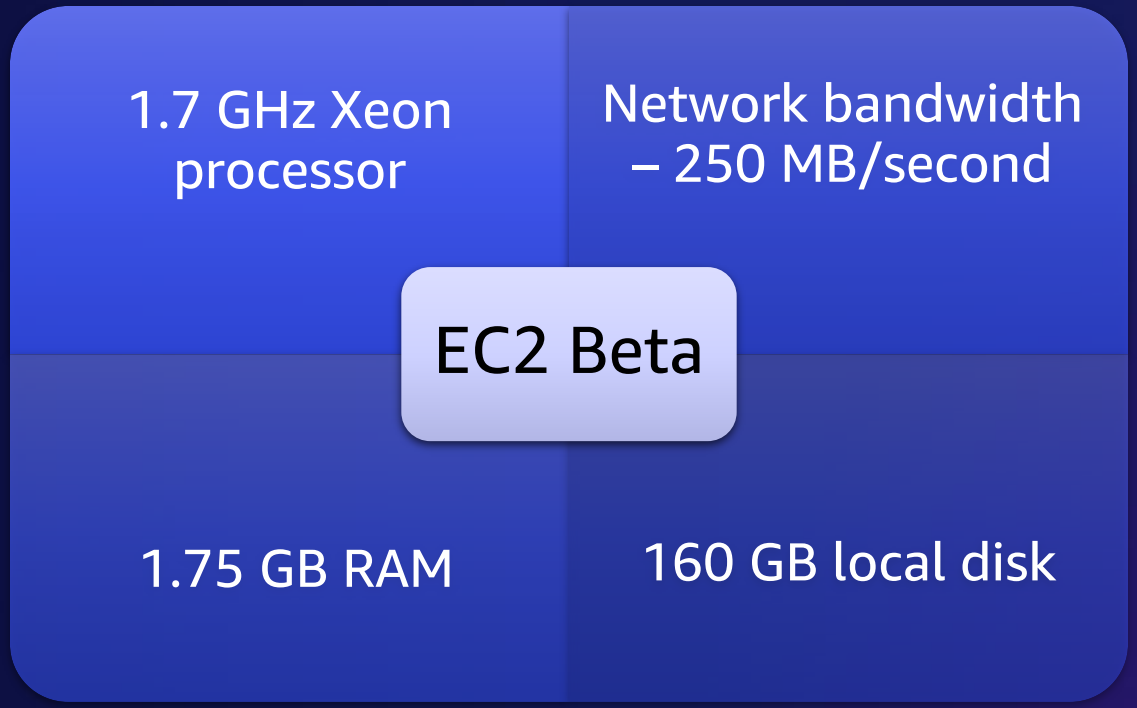
Brian Mycroft
Chief Technologist
AWS

Agenda

- History of the AWS Nitro System
- Nitro System deep dive
- Performance advantages of the Nitro System
- Nitro System as a security differentiator
- Unlocking innovation with the Nitro Systems
- Summary

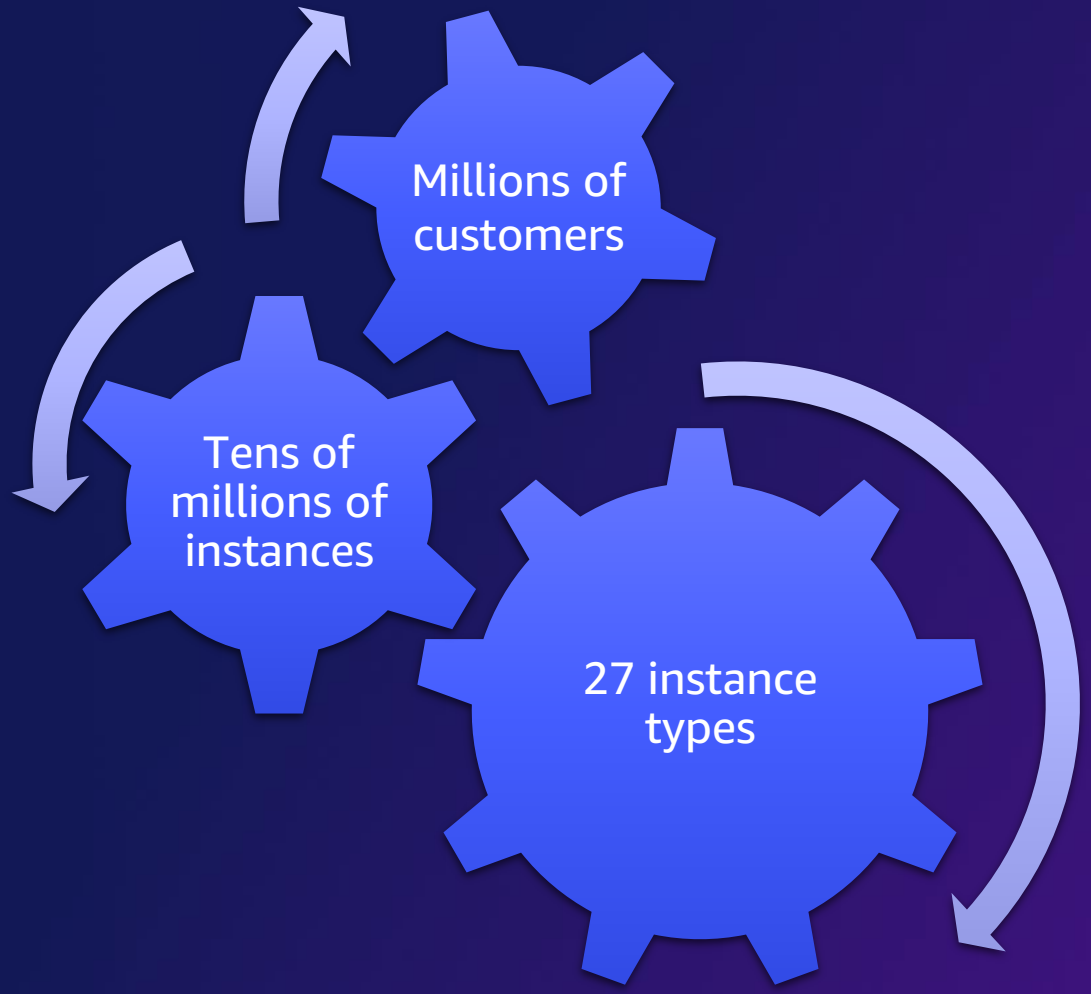
Today, over **60 million** new instances are spun up every day on Amazon EC2

m1.small – Amazon EC2's first instance in 2006

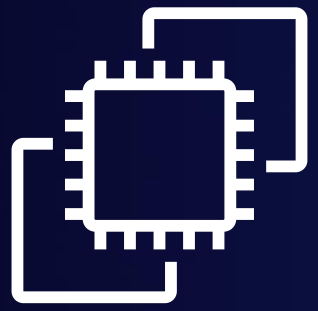


Xen hypervisor

- Para-virtualized devices
- Drivers split into frontend and backend
- Started with no hardware acceleration
- CC2, C1, M1, M2, C3, M3, R3, C4, M4, R4, T1, T2, I2, I3, X1, X1e, P2, P3, G2, G3, F1, D2, H1



AWS Nitro System



AWS Nitro System

After a decade of Amazon EC2 experience, if we applied all of our learnings, how would we change our server platforms?

Improve throughput

Simplify hypervisor

Reduce latency and jitter

Bare-metal instances

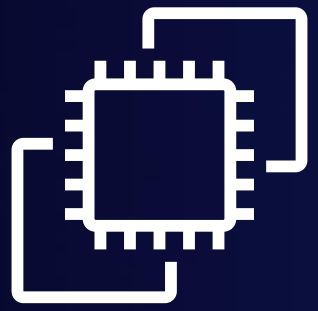
Transparent encryption

Hardware root of trust

No operator access

Narrow auditable APIs

AWS Nitro System



AWS Nitro System

Launched in November 2017

In development since 2012

Purpose-built hardware/software

Hypervisor built for AWS

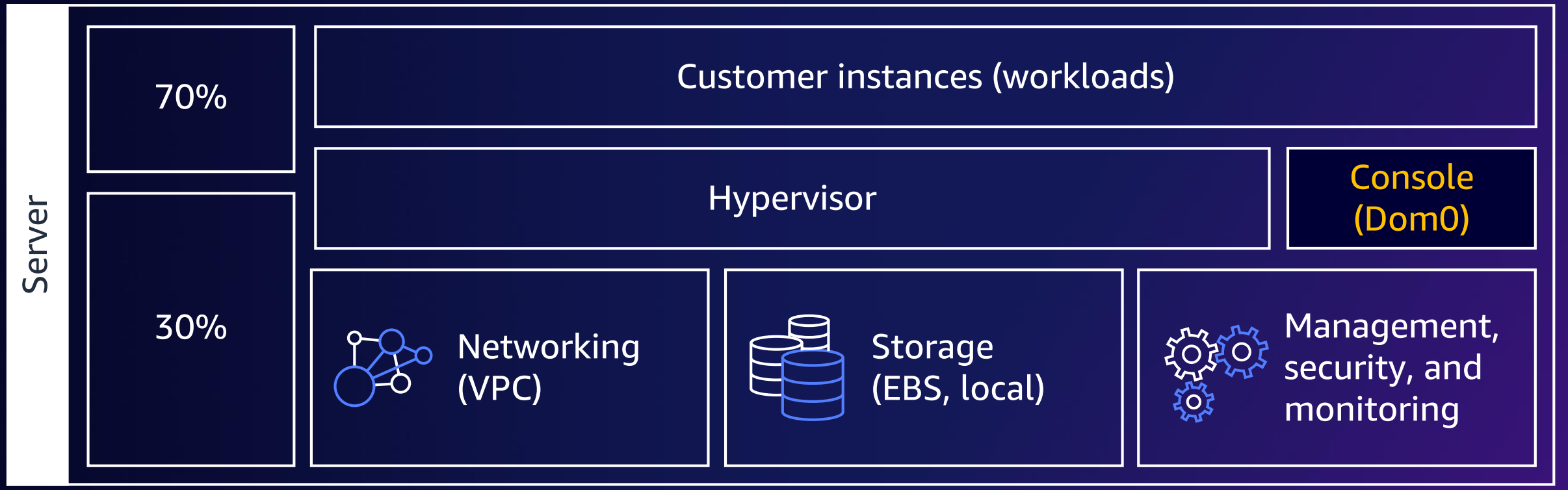
Five generations of custom chips

All new instances launch using the AWS Nitro System

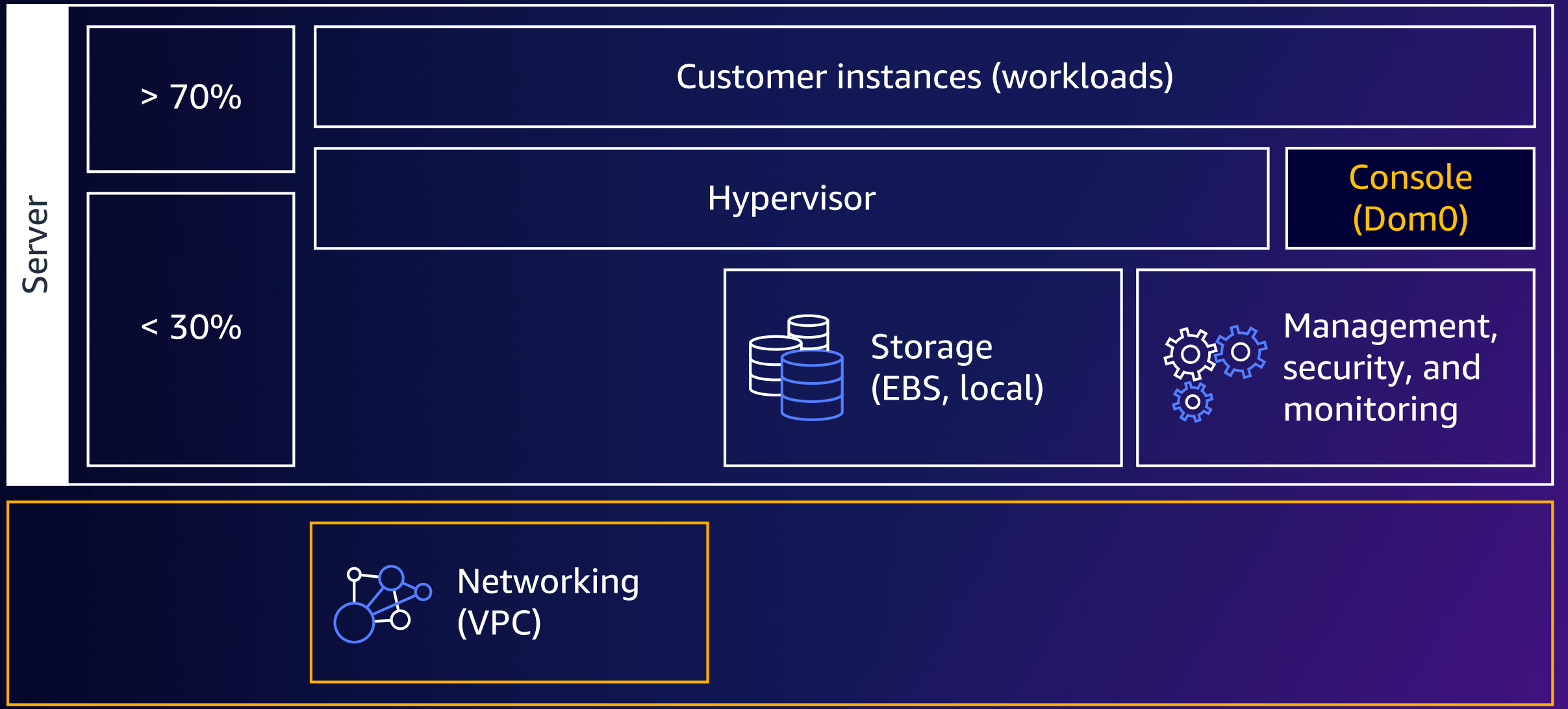
AWS Nitro System, NOT AWS Nitro Enclaves

- AWS Nitro System is the AWS solution for confidential computing
- Benefits available to all modern EC2 instances – no special tooling required
- No application modifications or custom configuration
- AWS Nitro Enclaves is yet another AWS offering that allows customers to prevent access to their workloads by their own administrators

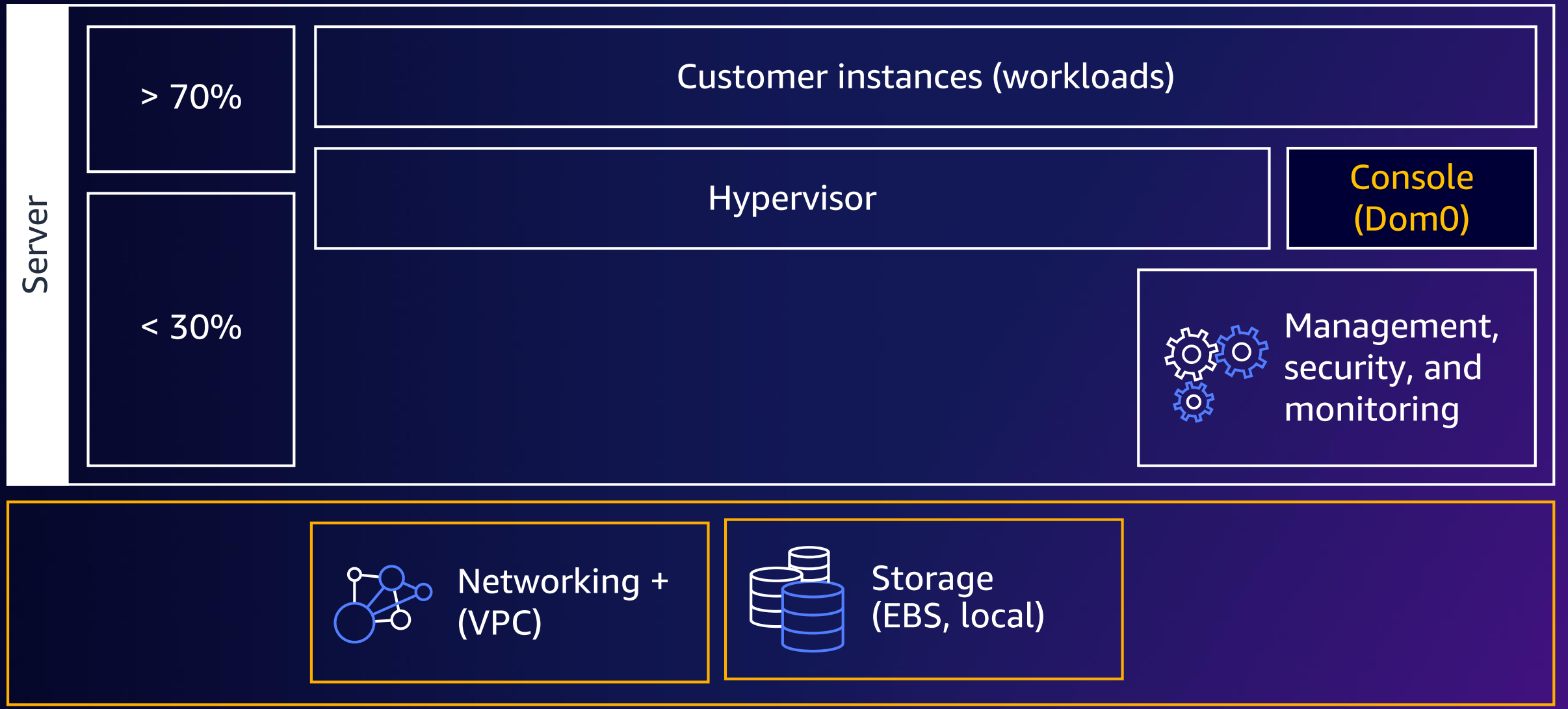
Original EC2 “instance” host architecture



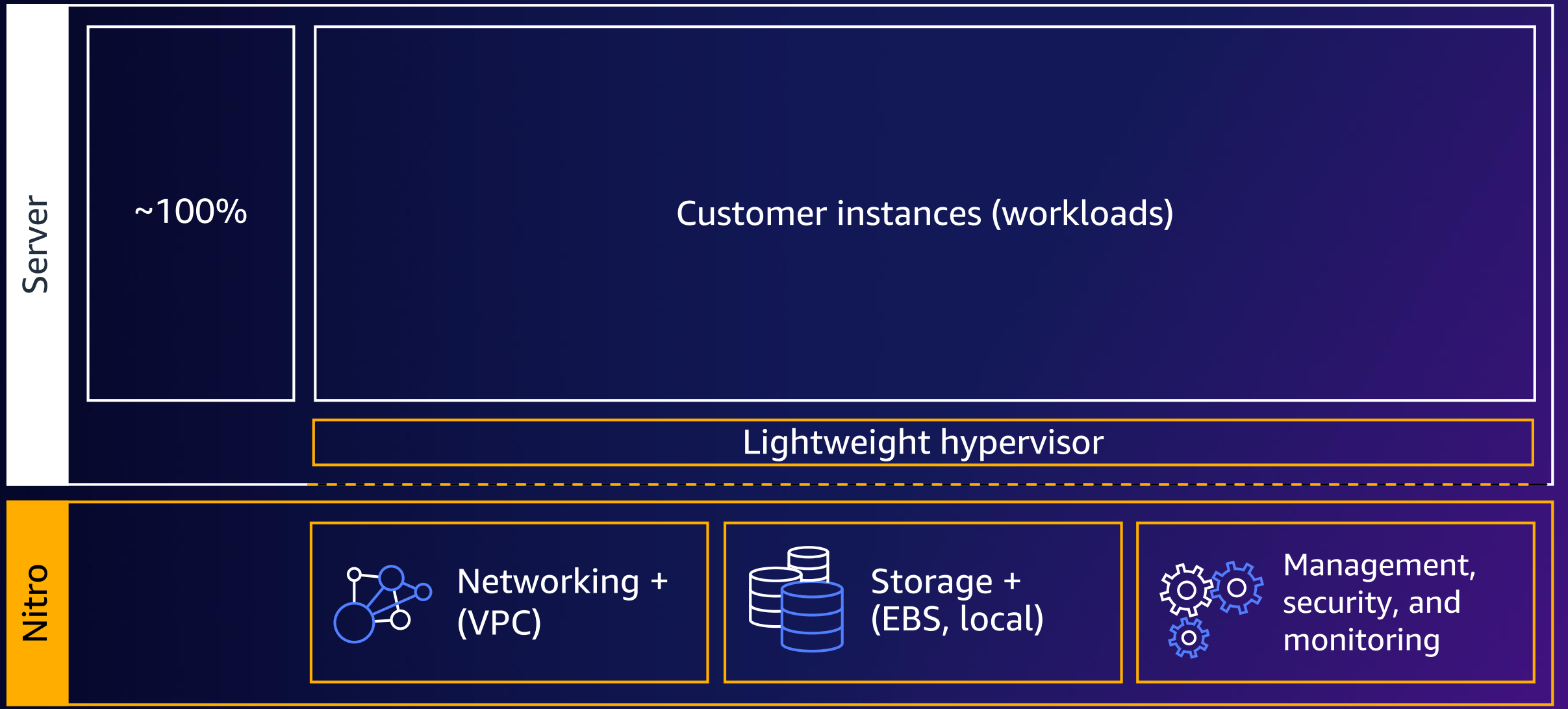
2013 EC2 “instance” host architecture



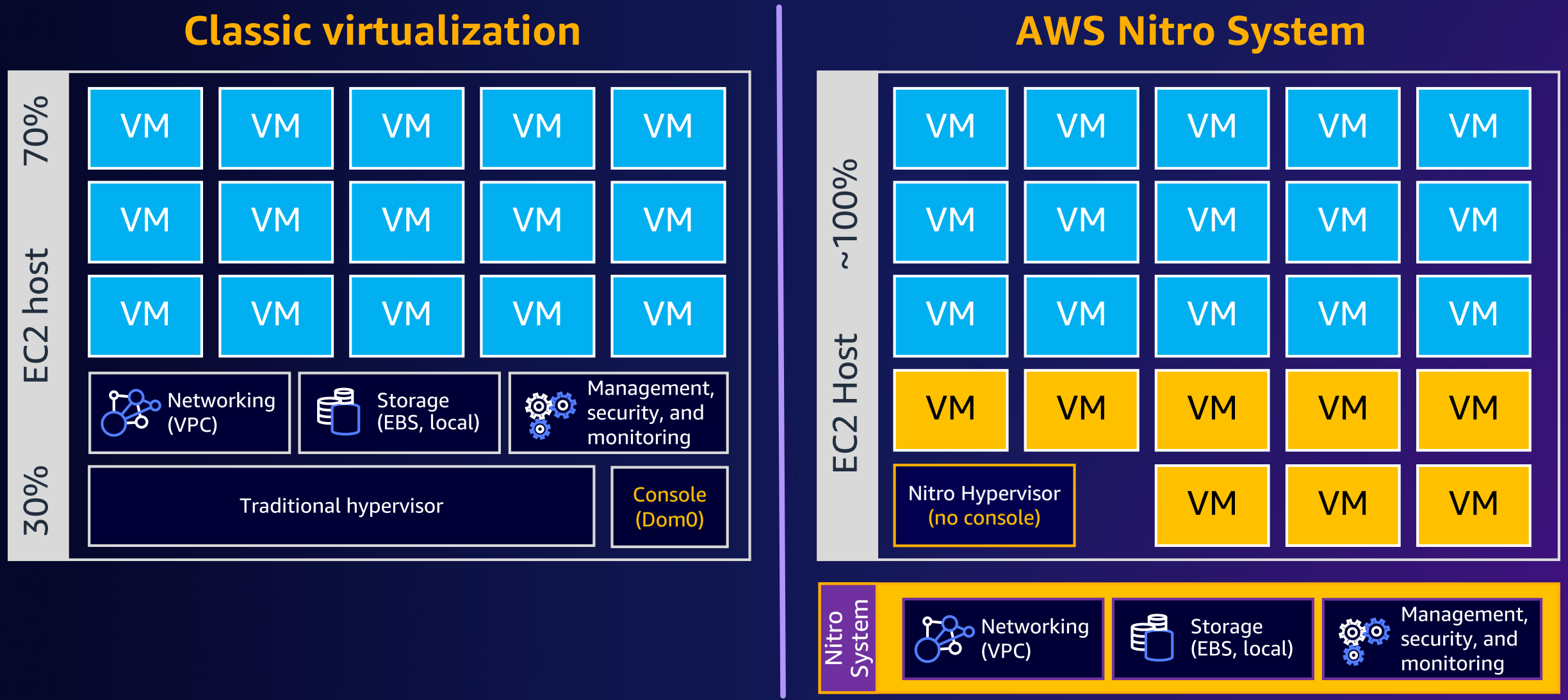
2014 EC2 “instance” host architecture



Today: The AWS Nitro System architecture



Reinventing virtualization for the cloud



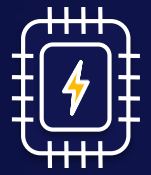
Let’s dig a little deeper into the components

AWS Nitro System

Nitro Cards

VPC networking
Amazon EBS
Instance storage
Nitro SSDs
System controller

Nitro Security Chip



Integrated into motherboard
Traps I/O to nonvolatile storage
Hardware root of trust
Protects hardware resources

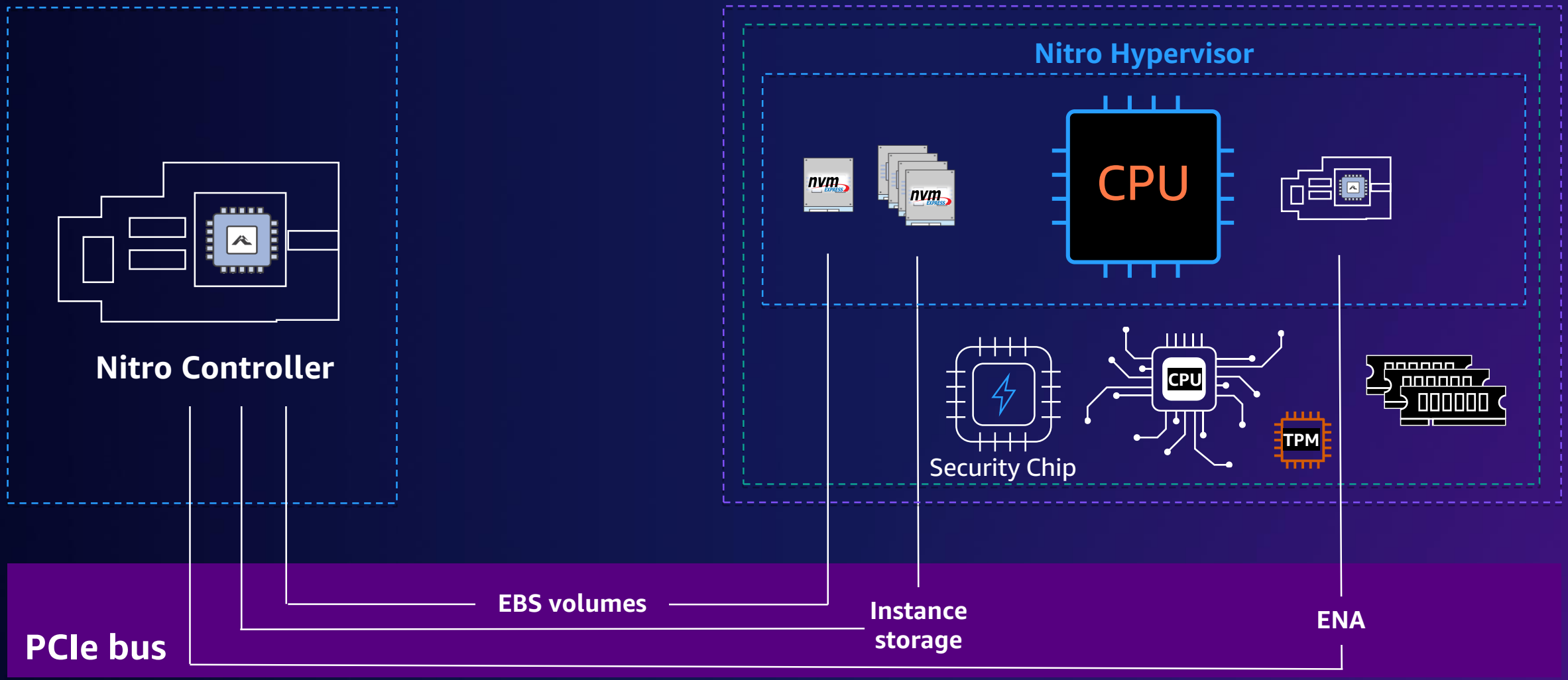
Nitro Hypervisor

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

NitroTPM

Trusted Platform Module 2.0
Instance health attestation
Cryptographic offload

Nitro architecture full view



Nitro Cards

Nitro Card for VPC

- ENA PCIe controller – drivers for all major operating systems (EFA w/kernel-bypass)
- VPC data plane (encapsulation, security groups, limiters, routing, flow logs, DHCP, DNS)
- Transparent end-to-end line-rate 256-bit encryption, up to 800 Gb/s bandwidth
- Independent of fabric

Nitro Card for EBS

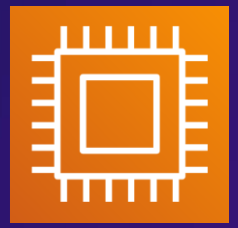
- NVMe PCIe controller – standard drivers broadly available
- EBS data plane (encryption support, NVM to remote storage protocol), up to 60 Gb/s

Nitro Card for instance storage

- NVMe PCIe controller – standard drivers broadly available
- Instance storage data plane (transparent line-rate encryption, limiters, drive monitoring)

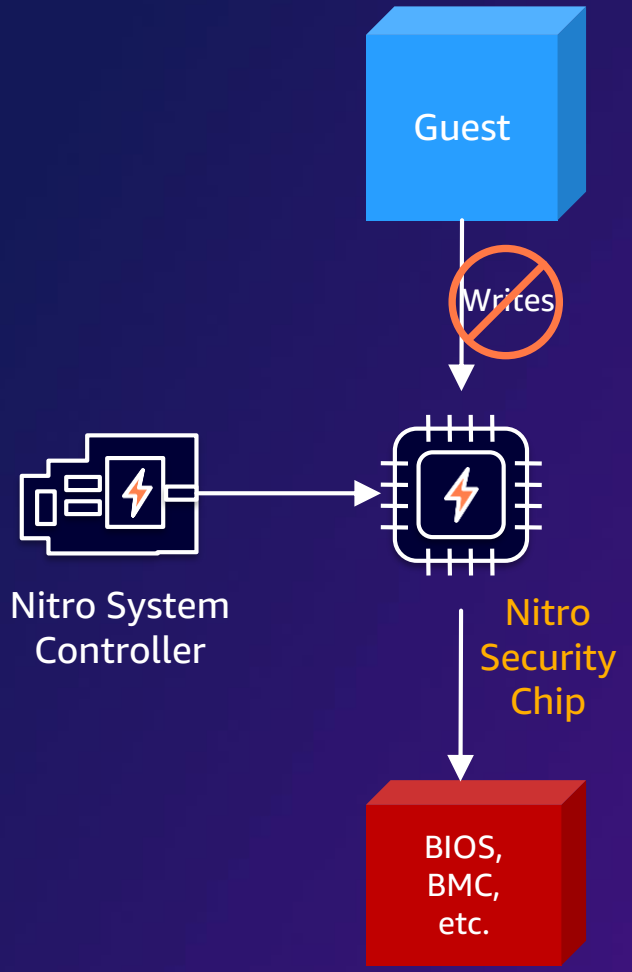
Nitro Card controller

- 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

- Custom microcontroller integrated into motherboard
- Traps all I/O to nonvolatile storage
- All **write-access to nonvolatile storage is blocked** in hardware
- Hardware-based root of trust
- Used by Nitro Controller to monitor hardware, validate and update system firmware and software
- Nitro software is signed and validated
- Enabled metal instances and VMware Cloud on AWS



AWS Nitro Hypervisor

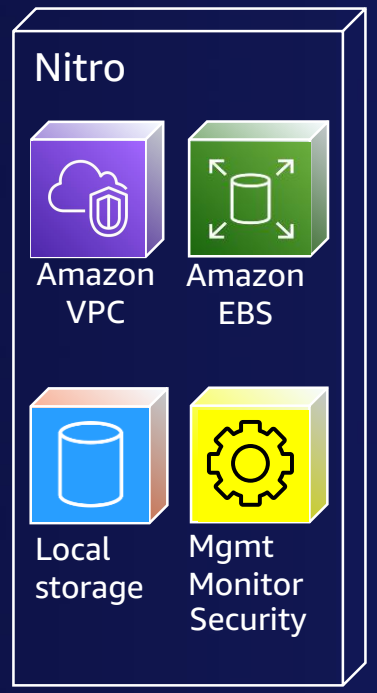
Nitro Hypervisor

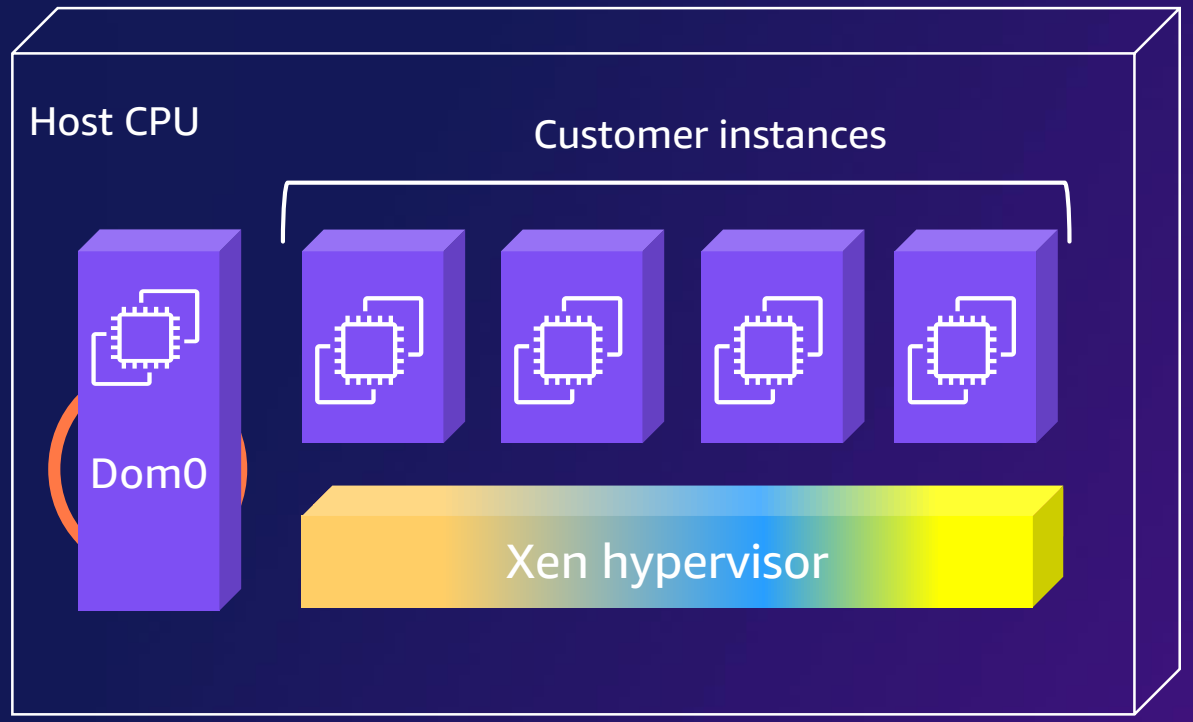
Lightweight hypervisor

Memory and CPU allocation

Bare-metal-like performance

Eliminates the console and human access





AWS Nitro TPM and UEFI Secure Boot

NEW!

ADDITIONAL PROTECTION OF SENSITIVE INFORMATION IN AMAZON EC2 INSTANCES

Allows attestation of the health of Amazon EC2 instances and provides a source of trust that is rooted in silicon

Easy to migrate on-premises applications that depend on a TPM

Conforms to the TPM 2.0 specification

UEFI Secure Boot ensures the bootloader is properly signed by a known authority

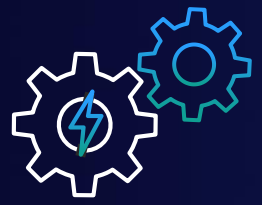
Detects guest image tampering, only allows boot if the image is unmodified

Enables new use cases in EC2

Microsoft Bitlocker | Attestation | DM-Verity | Linux Unified Key Setup (LUKS)

aws

The AWS Nitro System enables . . .



Performance

Better performance across CPU, networking, and storage

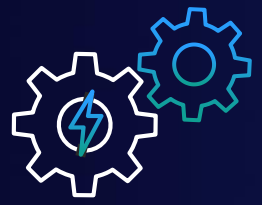
Security

Enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware

Innovation

Building blocks can be assembled in many different ways, giving us the flexibility to design and rapidly deliver Amazon EC2 instances

The AWS Nitro System enables . . .



Performance

Better performance across CPU, networking, and storage

Security

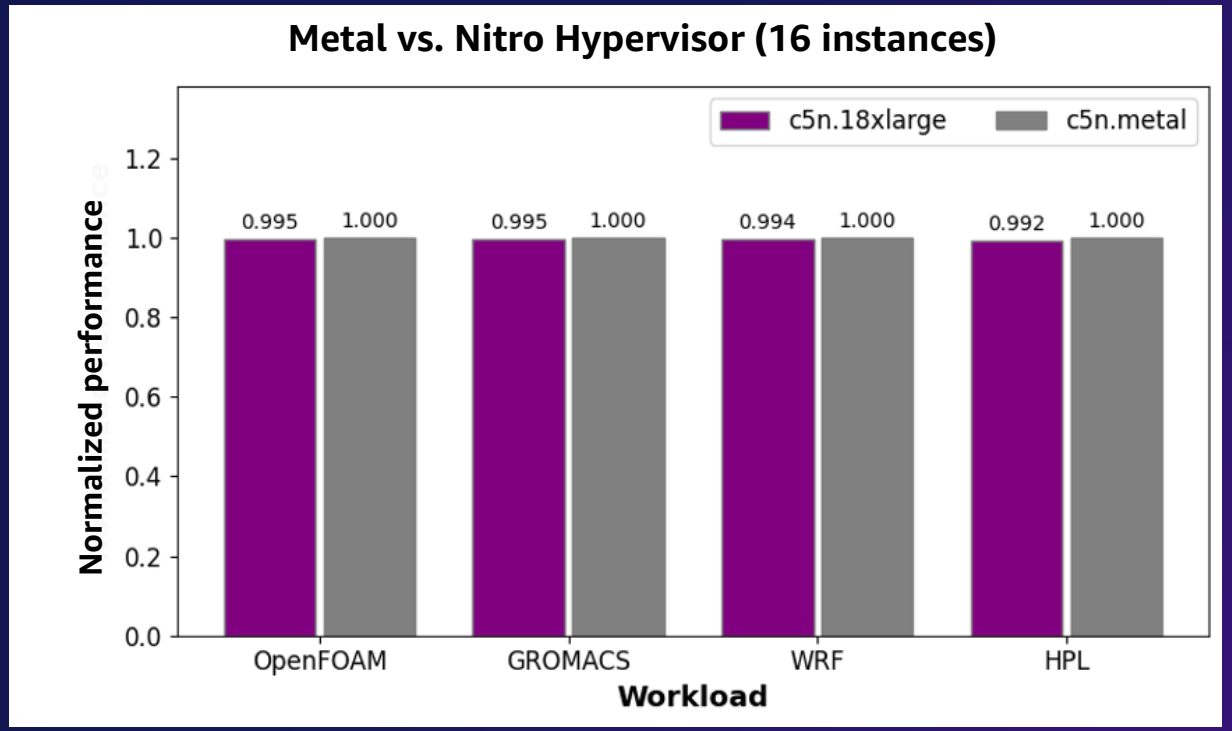
Enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware

Innovation

Building blocks can be assembled in many different ways, giving us the flexibility to design and rapidly deliver Amazon EC2 instances

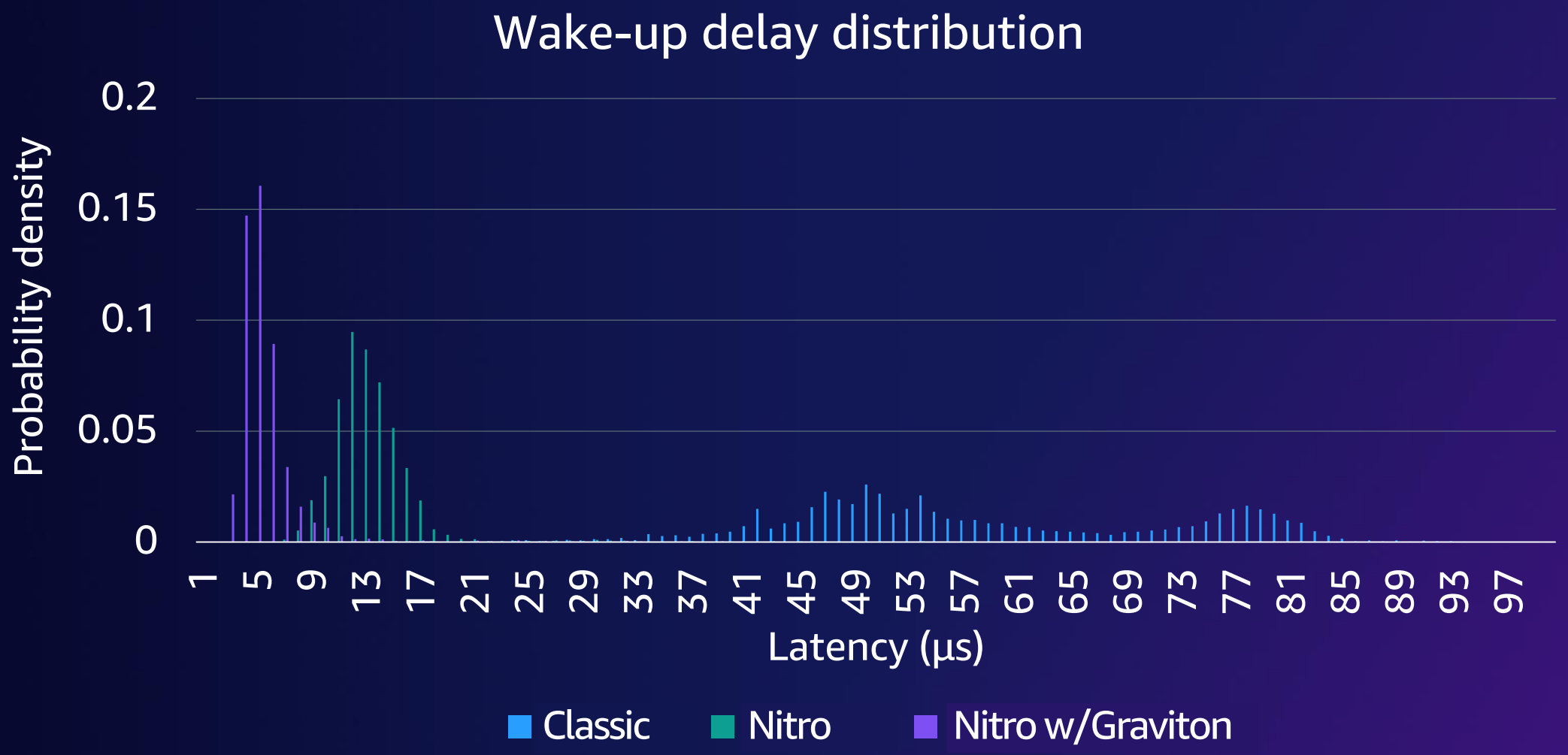
Metal vs. Nitro Hypervisor instances on AWS

- AWS offers ".metal" instances, which remove the hypervisor entirely
- The Nitro Hypervisor has minimal overhead in the evaluated HPC applications/benchmarks



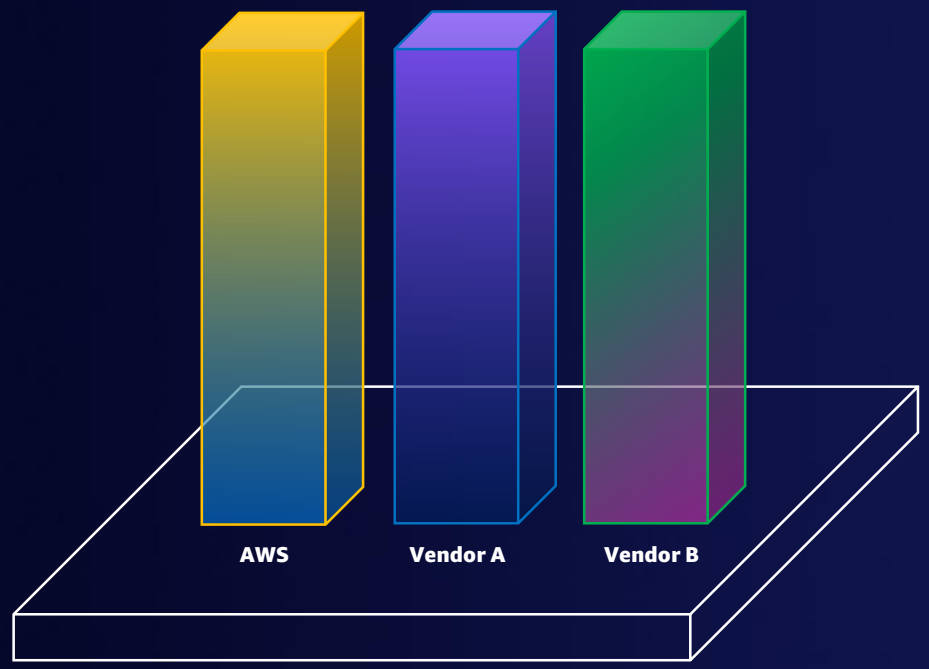
https://aws.amazon.com/blogs/hpc/bare-metal-performance-with-the-aws-nitro-system/

AWS Nitro System – Reduced jitter

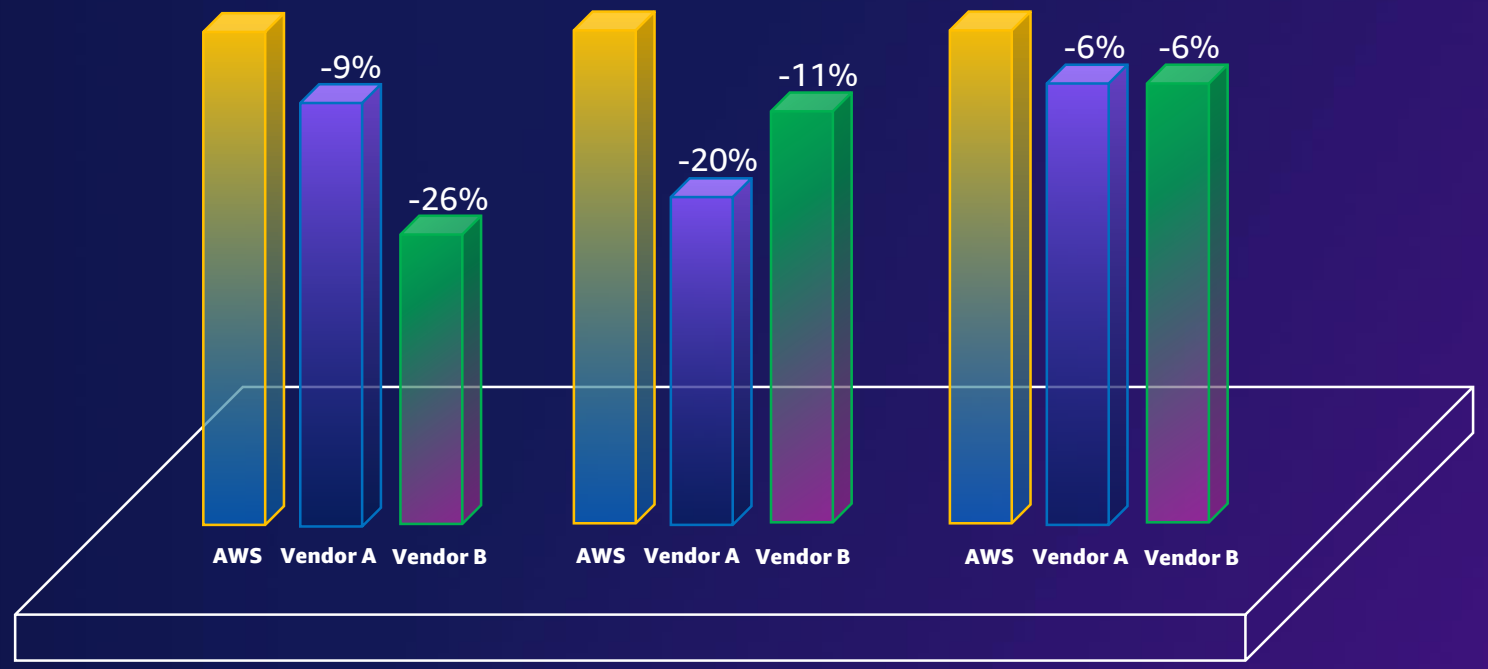


Nitro performance for real-world workloads

NITRO SYSTEM PROVIDES BETTER PERFORMANCE



SPECINT2017



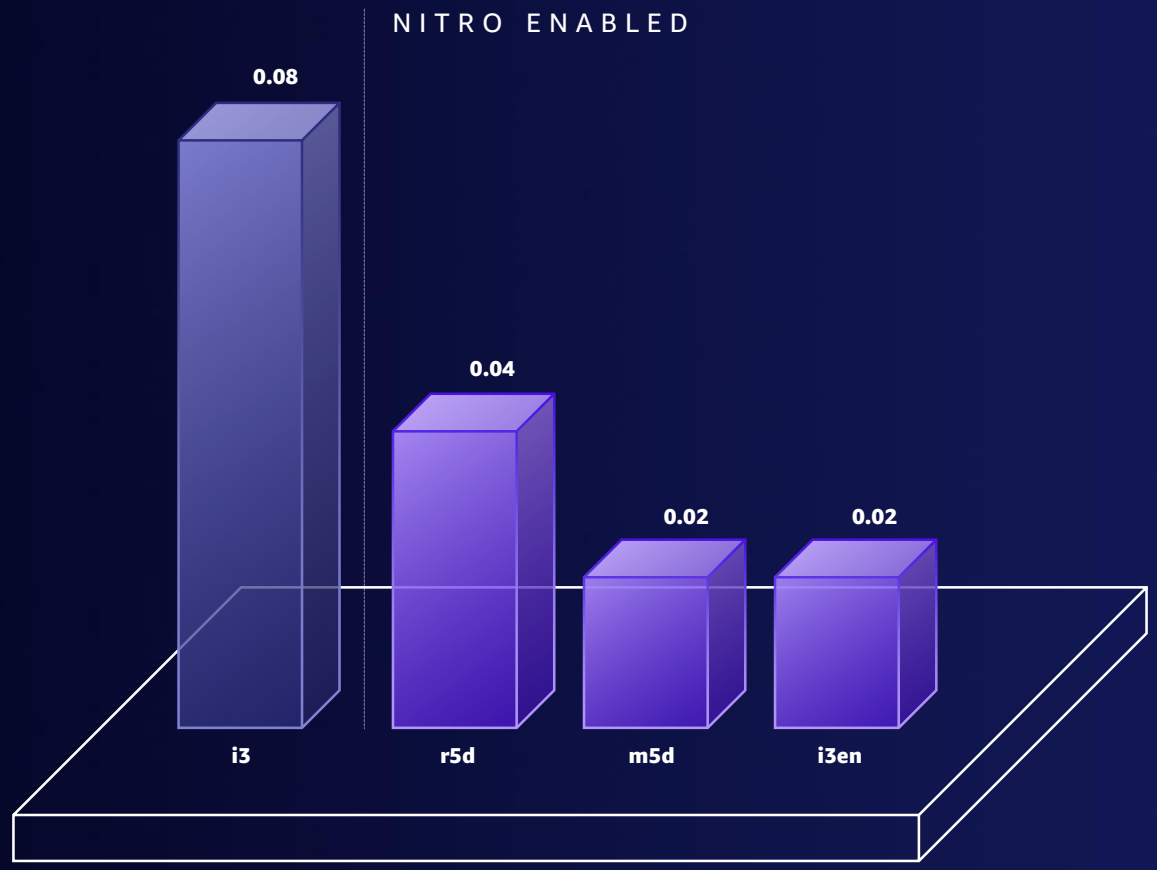
MEMCACHED

NGINX WEBSERVING

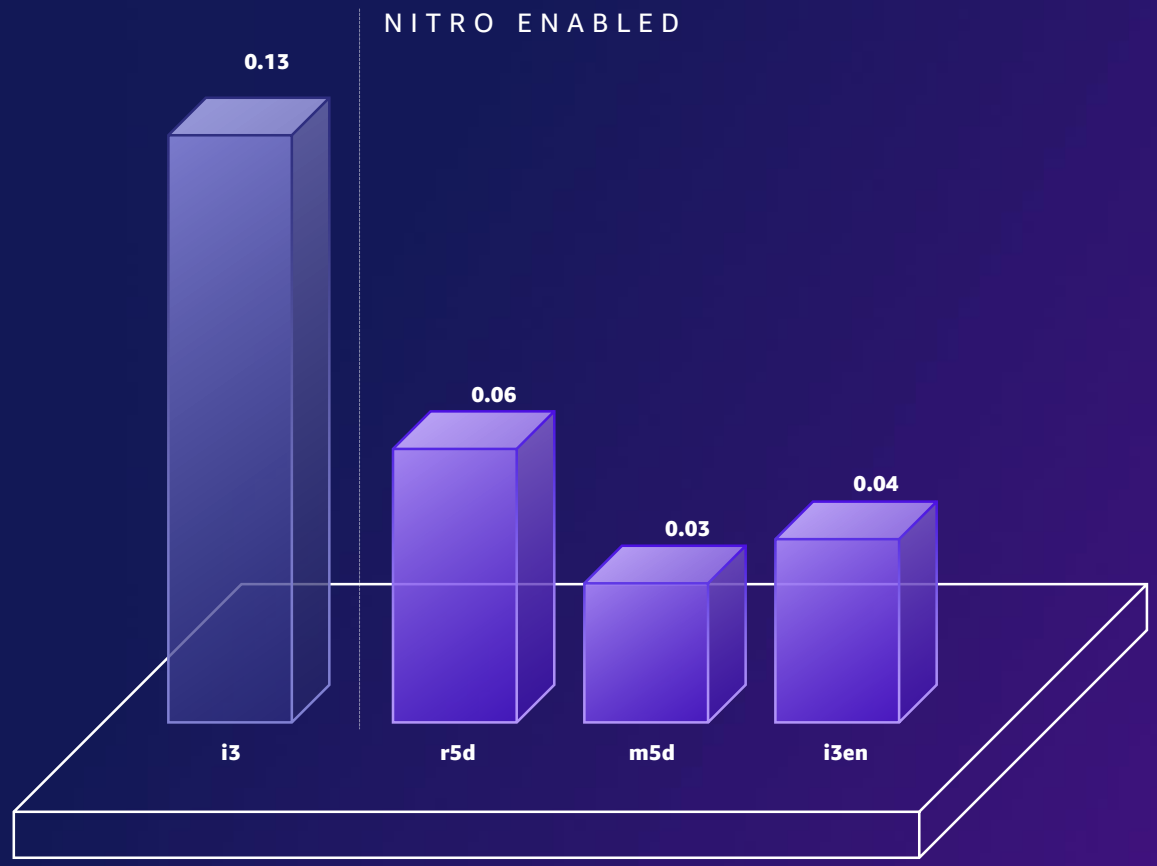
MYSQL SYSBENCH

Nitro System storage performance

UP TO 4X IMPROVEMENT IN INSTANCE LATENCIES



AVERAGE LATENCY (P50)



TAIL LATENCY (P99)

AWS Nitro SSD

NEW!

HIGH-PERFORMANCE, LOW-LATENCY SSD CUSTOM DESIGNED BY AWS

Lower latencies

Tightly integrated with the AWS Nitro System to provide 60% lower I/O latency and 4x lower jitter

Improved reliability

Faster firmware updates to improve reliability without any downtime to the instance

Nitro security

All data stored on the disks is encrypted at rest with AES-256 ephemeral keys

The AWS Nitro System enables . . .

Performance

Better performance across CPU, networking, and storage

Security

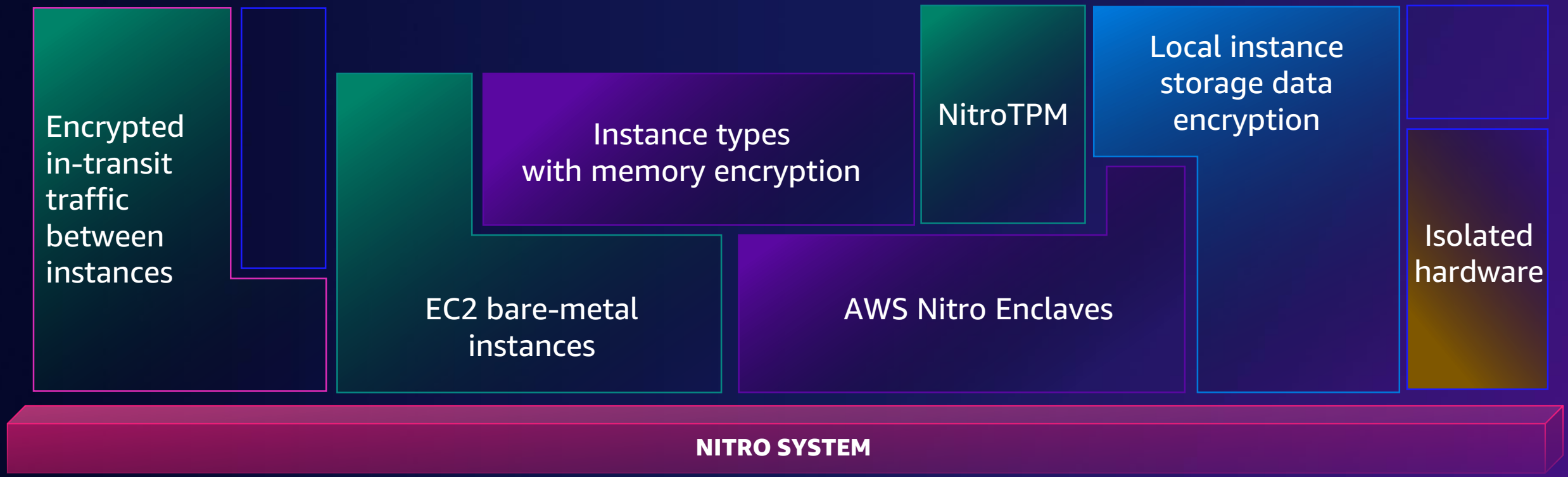
Enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware

Innovation

Building blocks can be assembled in many different ways, giving us the flexibility to design and rapidly deliver Amazon EC2 instances

Nitro System security

NITRO IS THE FOUNDATION FOR INNOVATIONS IN CONFIDENTIALITY AND PRIVACY



AWS Nitro System security

Designed from Day 1 to provide strong isolation between AWS and the customer

AWS Nitro Cards are physically separate from the hardware running customer instances

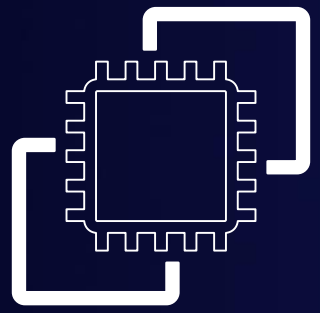
Dedicated CPU, memory, and hardware security chip

Virtual instances are fully isolated from one another and from the Nitro Hypervisor

Instances don’t share CPU cores or L1/L2 caches

Memory encryption w/Graviton2/3 and Intel Ice Lake

Nitro security – Confidential compute



AWS Nitro System

All interactions with the AWS Nitro System are through narrow, authorized, and authenticated APIs

There is no mechanism for any system or person to log in to the underlying Amazon EC2 host (no operational access)

There is no interactive access (no SSH, no general-purpose access of any kind)

Debugging features can’t disclose customer data

Nitro Systems run in an isolated network

VPC encryption

VPC encryption provides always-on, line-rate encryption between supported EC2 instance types

Works across VPC peering and between different AWS customers

VPC-encrypted traffic is anonymized and privacy-preserving

Accelerating Nitro firmware updates

We keep our systems updated with regular software updates

Instances keep running during Nitro updates

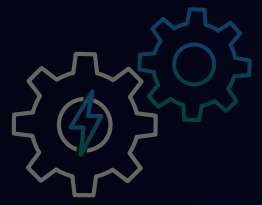
Some customers' workloads are sensitive to performance pause during updates

We introduced a smart management of state during updates

85% reduction in pause time

Sub-second pauses for C/M/R instances

The AWS Nitro System enables . . .



Performance

Better performance across CPU, networking, and storage

Security

Enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware

Innovation

Building blocks can be assembled in many different ways, giving us the flexibility to design and rapidly deliver Amazon EC2 instances

Broadest and deepest platform choice

Categories

General purpose + burstable

Compute-optimized

Memory-optimized

Storage-optimized

Accelerated computing

Graphics intensive

Capabilities

Choice of processor
(AWS, Intel, AMD, M1)

Fast processors
(up to 4.5 GHz)

High memory footprint
(up to 24 TiB)

Instance storage
(HDD and NVMe)

Accelerated computing
(GPUs, FPGA, ASIC)

Networking
(up to 800 Gbps)

Bare metal

Size
(<1vCPU to 448 vCPU)

Options

Amazon EBS

Amazon Elastic Inference

Windows, Linux,
UNIX, macOS

More than

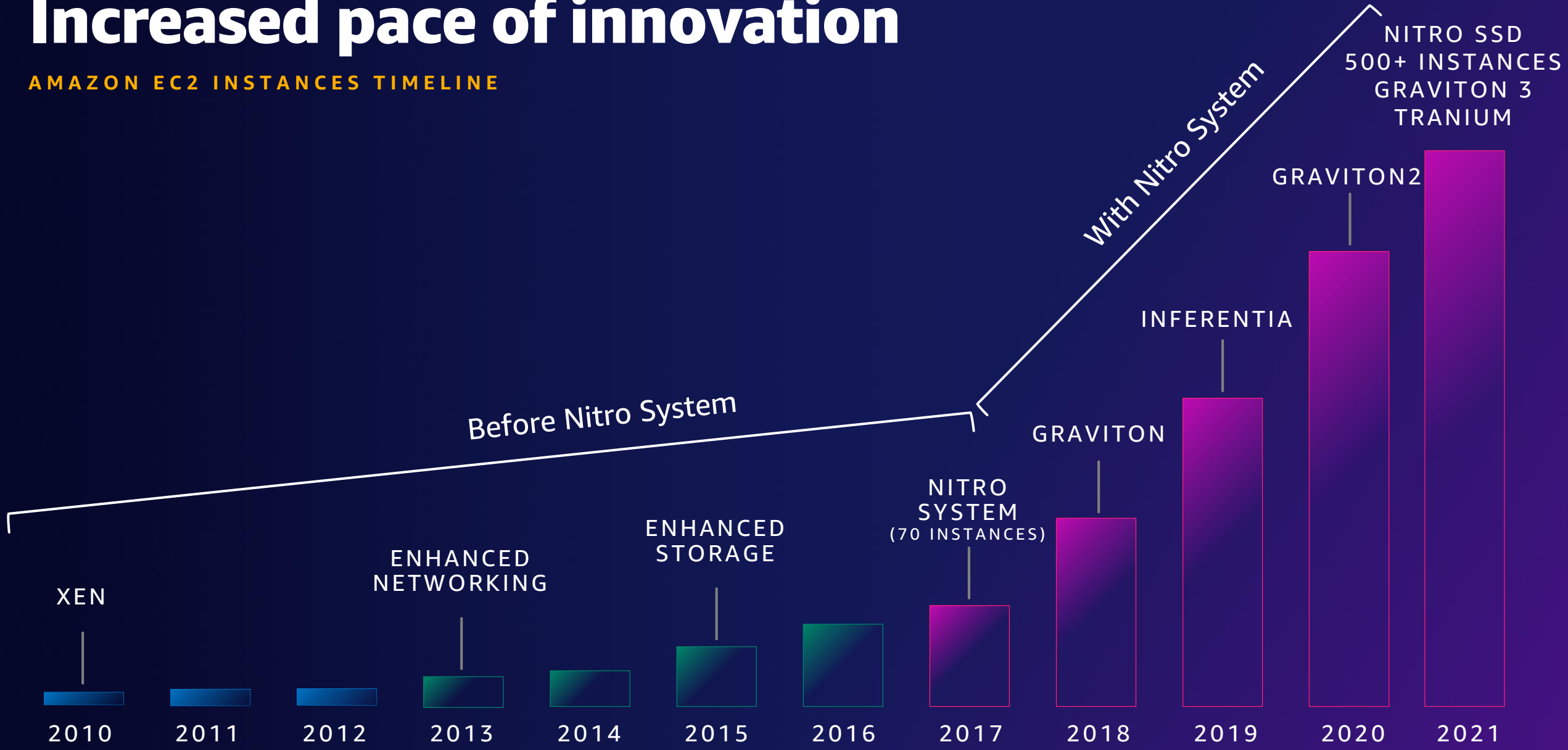
500

instance types

for virtually every
workload and
business need

Increased pace of innovation

AMAZON EC2 INSTANCES TIMELINE



aws

Broadest choice of processors and architectures

RIGHT COMPUTE FOR THE WORKLOAD

Intel Xeon Scalable processors

AMD EPYC processors

AWS Graviton processors

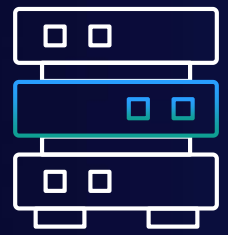
MAC mini (Intel / M1)

Is there more we could do to ensure that customers are able to use their selected instance without the risk of deprecation?

So we announced

Long-term support for previous generation instances

Support for Xen-based EC2 instances on the Nitro System

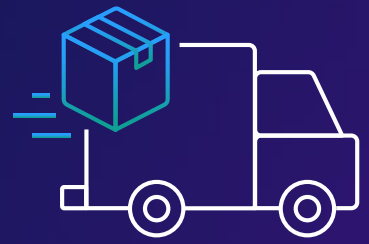


Extended lifetime

Run your workloads on the instances they were built on for years to come

Nitro benefits

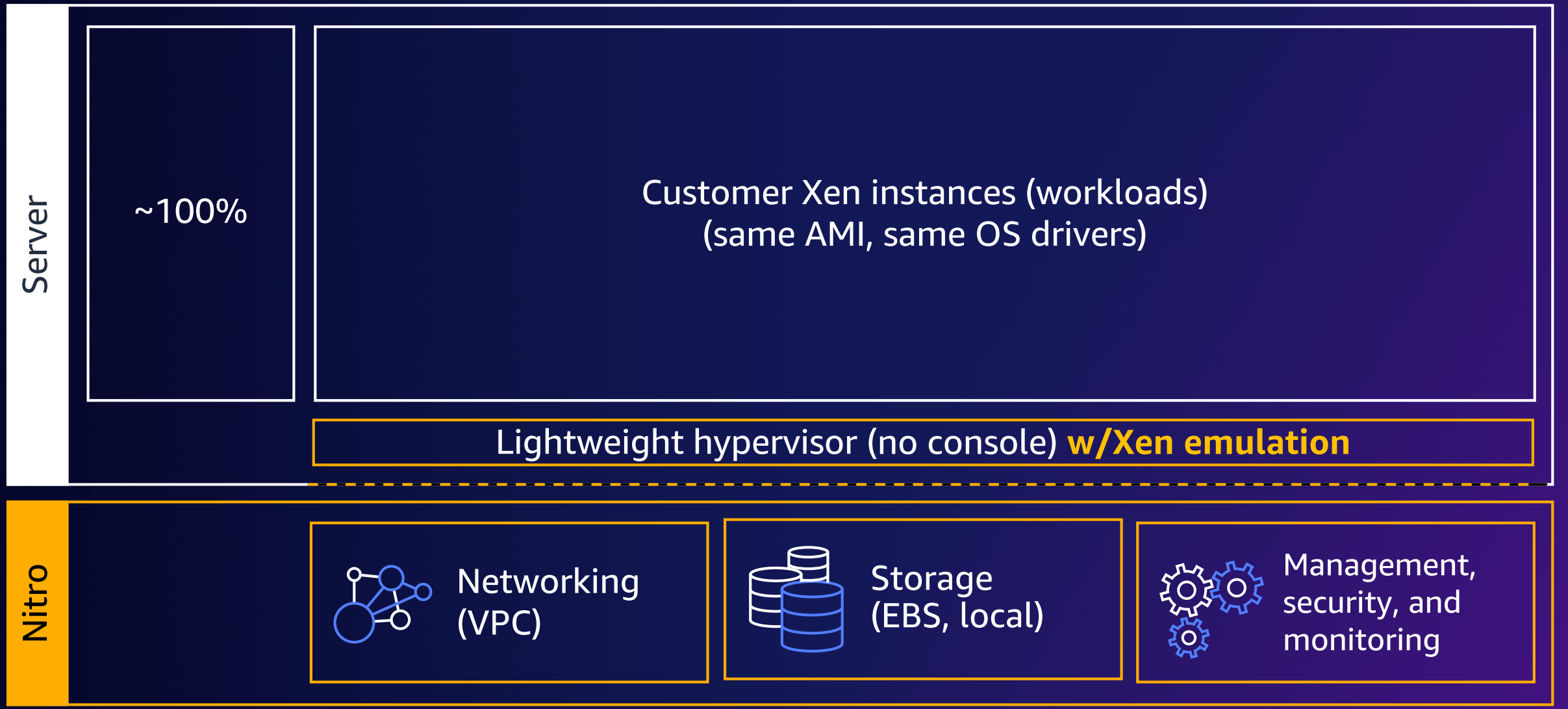
Brings the enhanced security of the AWS Nitro System to older instances and refreshed hardware for fewer maintenance events



Seamless migration

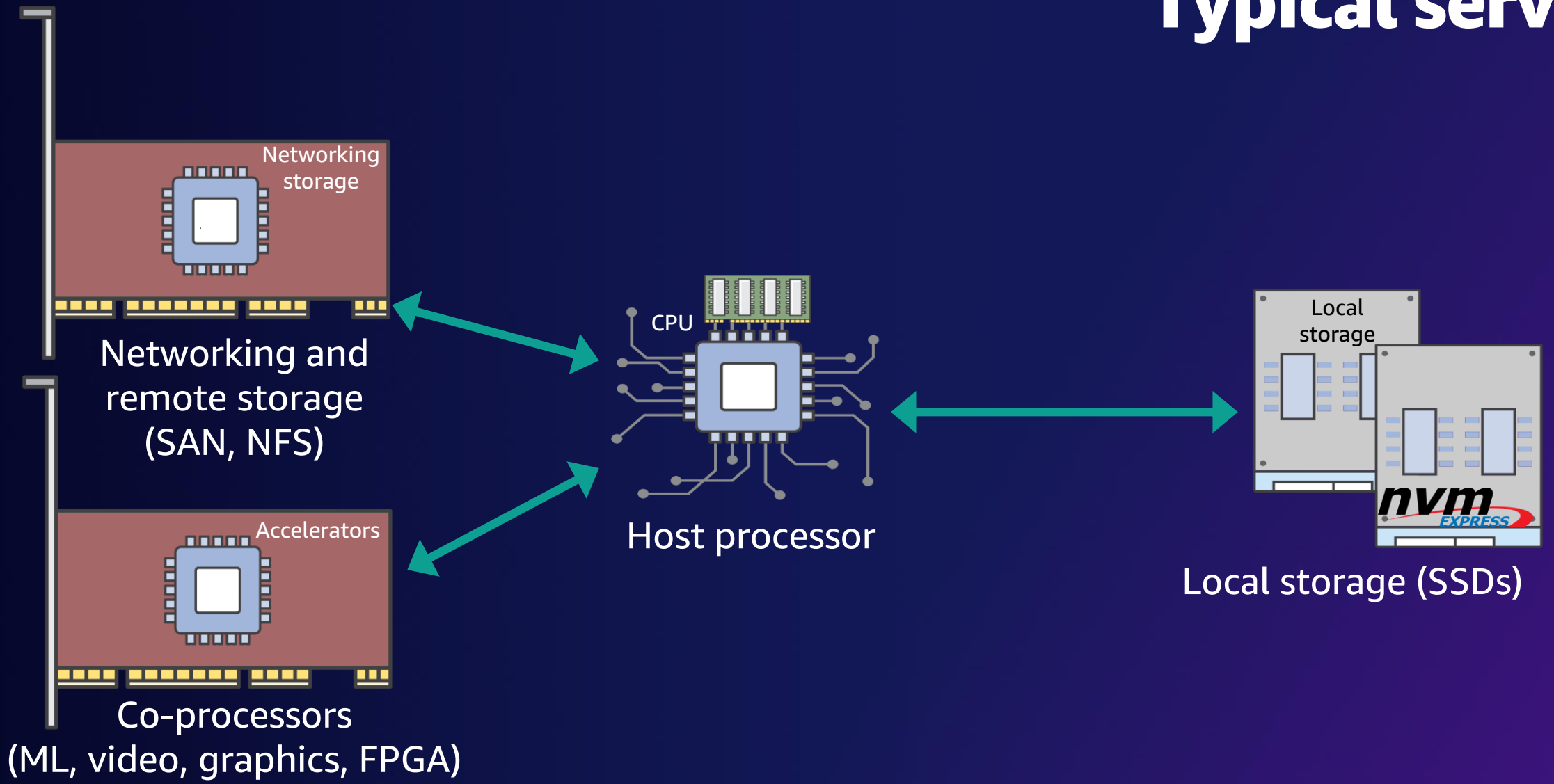
Seamless transition to the AWS Nitro System, with instance specifications, AMIs, and workflows remaining the same

Today: The AWS Nitro architecture

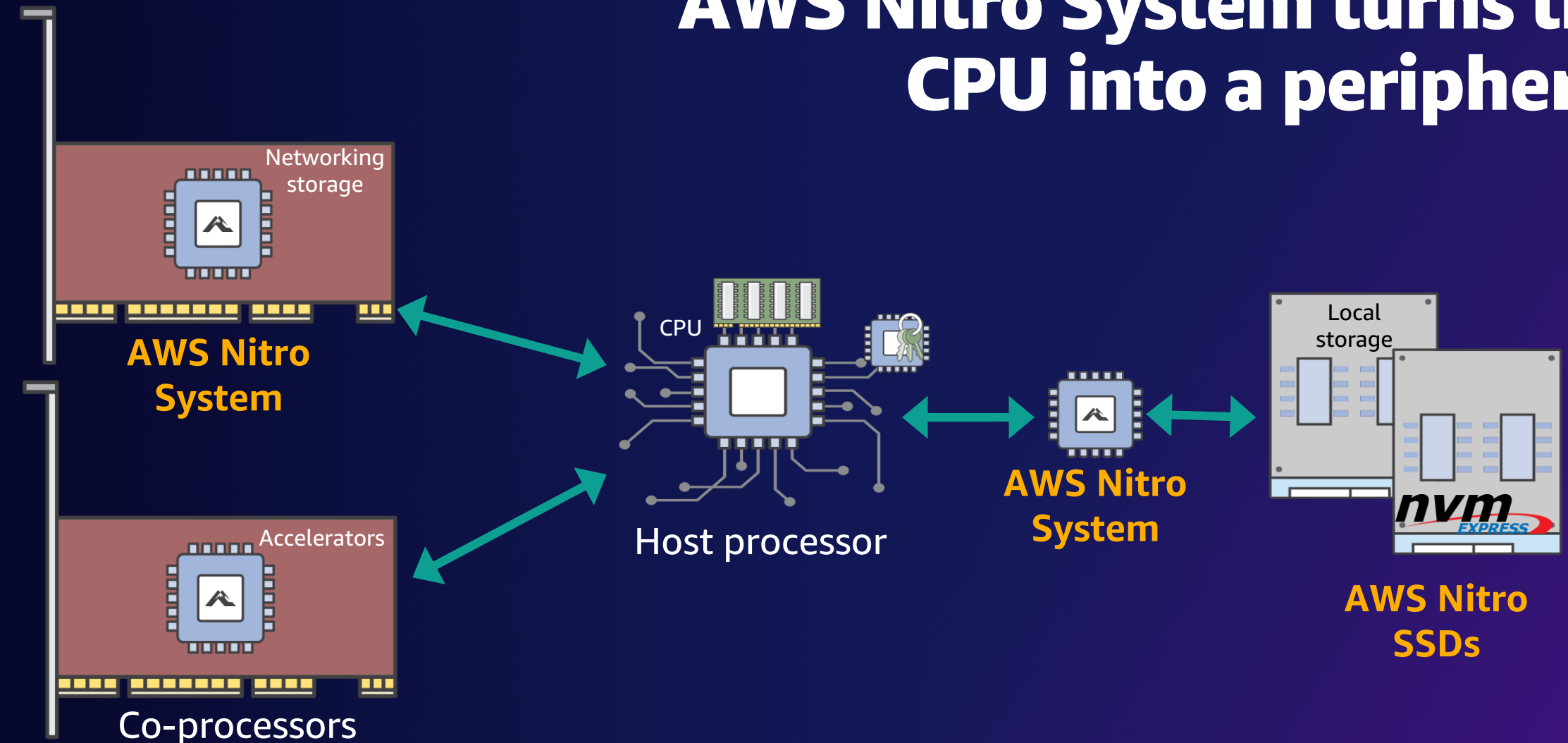


Summary

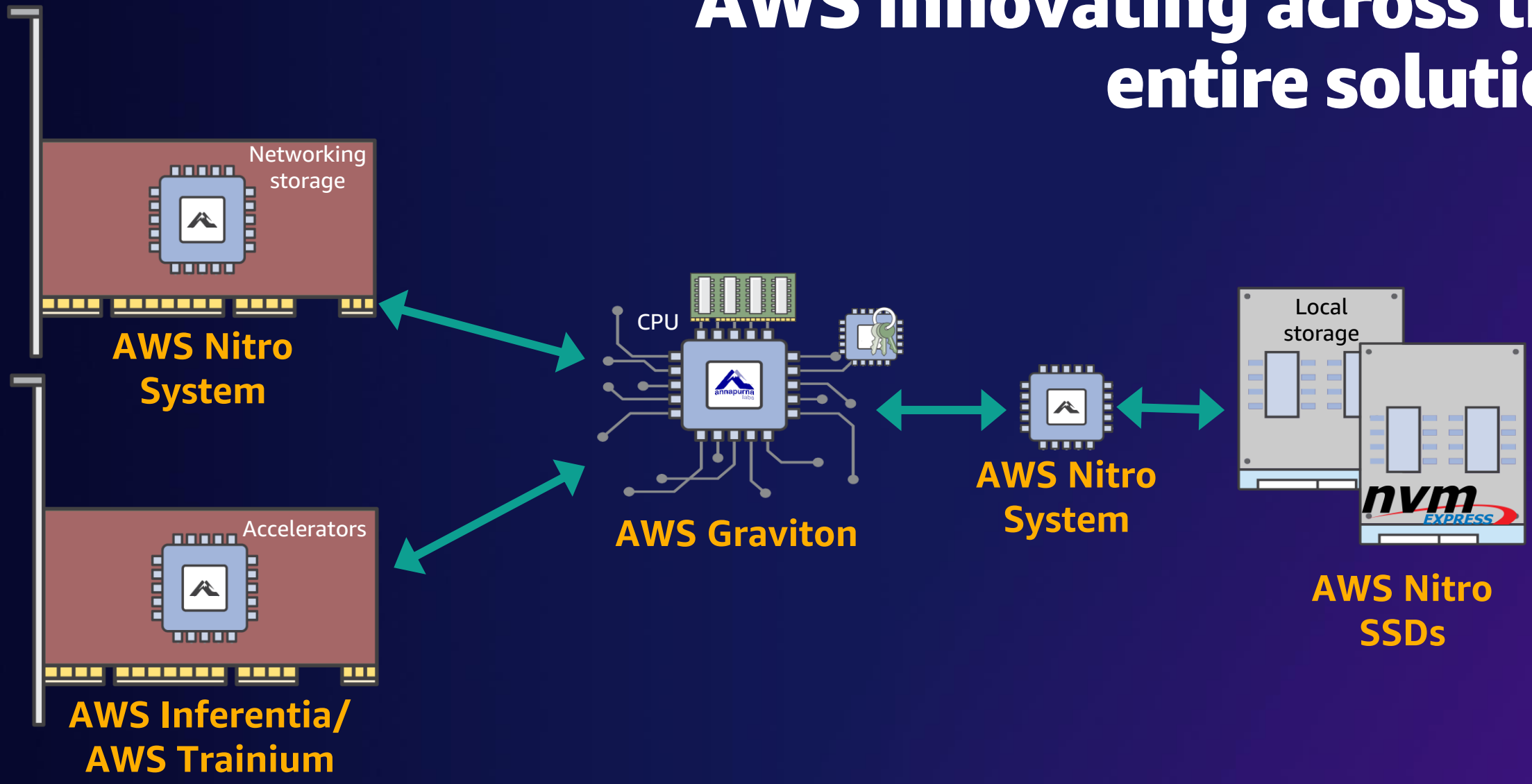
Typical server



AWS Nitro System turns the CPU into a peripheral



AWS innovating across the entire solution



Building on 15 years of silicon innovation

The AWS Nitro System architecture

Offering the best security, performance, and innovation in the cloud

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

aws

Thank you!

Brian Mycroft

bmycroft@amazon.com

Please complete the session survey in the mobile app

Android

iOS