Overview of the AWS Nitro System

Building Trust Through Secure Cloud Infrastructure

Matt Wilson
Vice President / Distinguished Engineer, Amazon

Confidential Compute Summit

Agenda

01 **Introduction**
Who are you, what do you do?

02 **Principles of Engineering Trustworthy Secure Systems**

03 **Overview of the AWS Nitro System**
A system built using trustworthy secure system principles

04 **Continuous investments and delivery**
A solid foundation that supports new types of workloads

05 **AWS Leadership**
Independent validation and transparency

06 **Looking Ahead**
The future of confidential computing

Key Themes

- Engineering Trustworthy Secure Systems requires an *multidisciplinary integrative approach*
- *Trust* and *Trustworthiness* are foundational concepts
- Confidential Computing fundamentally requires *trust*
- What is the role of the engineer in establishing and maintaining *justified trustworthiness?*

01

Introduction

RA1

Who are you, what do you do?

I am an Engineer

I am a Systems Engineer

I am a Socio-technical Systems Engineer

I am a Socio-technical Systems Engineer

Open Source

Complex dynamics of communities, social norms, concerns about sustainability and supply chain risks

Software Engineering

How teams work effectively, safely, adaptively. AI is changing this more every day

Trustworthy Secure Systems

How do we build some of our most critical systems so that *trustworthiness is justified?*

02

Principles for Engineering Trustworthy Secure Systems

The Objective

To design and deliver an engineered system that reliably delivers its intended function, while ensuring that only the intended behaviors and outcomes occur, both with the system and within the system.

Principles for Trustworthy Secure Design

Anomaly Detection	Least Privilege
Clear Abstractions	Least Sharing
Commensurate Protection	Loss Margins
Commensurate Response	Mediated Access
Commensurate Rigor	Minimal Trusted Elements
Commensurate Trustworthiness	Minimize Detectability
Compositional Trustworthiness	Protective Defaults
Continuous Protection	Protective Failure
Defense in Depth	Protective Recovery
Distributed Privilege	Reduced Complexity
Diversity (Dynamicity)	Redundancy
Domain Separation	Self-Reliant Trustworthiness
Hierarchical Protection	Structured Decomposition and Composition
Least Functionality	Substantiated Trustworthiness
Least Persistence	Trustworthy System Control

03

Overview of the AWS Nitro System

A system built using trustworthy secure system engineering principles

The Nitro System: Purpose-Built to be Trustworthy

Nitro System Components

1

Nitro Cards

Custom hardware that offloads and isolates I/O, storage, and networking. Physical separation from host CPU.

2

Nitro Hypervisor

Minimal, purpose-built hypervisor. No shell, no SSH, no interactive access. Drastically reduced attack surface.

3

Nitro Security Chip

Hardware root of trust. Protects against unauthorized firmware modifications and physical attacks.

No Operator Access, By Design

There is no mechanism for any system or person to:

- Log in to EC2 Nitro hosts
- Access the memory of EC2 instances
- Access customer data on local encrypted storage or remote EBS volumes

Confidentiality is enforced across hardware platforms and AI accelerators by design

Enforcement Layers

Hardware

Nitro Cards physically separate host from customer workload path

Software

No SSH, no shell, no interactive debugging interface exists

Contractual

Operator access restrictions are codified in AWS Service Terms

Auditable

All administrative APIs are authenticated and logged

The part where Cory trusts Amazon

“I have spent a decade as a professional thorn in this company's side. I have a financial incentive, a personal brand, and frankly a temperament that all point toward not trusting AWS with so much as my lunch order. But credit where it's due: **whatever else they get wrong, Amazon takes security and data privacy deadly seriously.** […] I've seen what AWS does when security competes with other pressures. The list of companies I'd let build a map this detailed of my business is damn short, and most of the names on it are not the ones building these products.”

– Cory Quinn

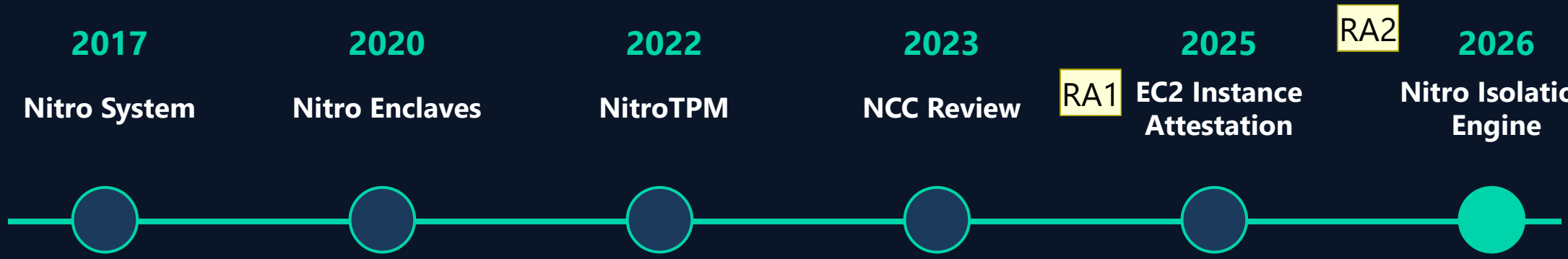
LJ1

04

Raising the Security Bar

Industry firsts, independent validation, and increased transparency

Continuous Delivery



Each milestone builds on the last. From hardware isolation to mathematical proof of correctness, AWS continuously raises the bar for what customers can trust.

Independent Validation of Our Claims

Claims without assurance is “veneer security”

Nitro Isolation Engine
Whitepaper 2026

Full technical deep-dive into the architecture enforcing hardware and software isolation across all AWS workloads. Open for public review.

NCC Group Review
2023

Independent architecture review by leading cybersecurity firm affirmed all Nitro System security claims.

Security Design Whitepaper
2022

Complete public documentation of Nitro System security architecture and design principles.

AWS Service Terms
Contractual Commitment

Operator access restrictions codified in service terms. Legally binding, not just technical documentation.

The Nitro Isolation Engine: Provable Security

Formal verification delivers mathematical proof of isolation — not just testing

What We Claim

- **Memory safety**
  No null pointer dereference, no use-after-free
- **No runtime errors**
  No reachable panics, such as unwrap on None or Err values
- **Functional correctness**
  No logical errors in isolation enforcement
- **Confidentiality & integrity**
  No unauthorized information flow between VMs

How We Prove It

- **Rust ownership model**
  Formal reasoning about memory safety at the language level
- **330,000 lines of proof**
  Machine-checked mathematical proof in Isabelle/HOL
- **Compositional verification**
  Each module proven independently, then composed
- **Provable VM isolation**
  Comparable in rigor to the landmark seL4 project

Same Rigor, Broader Impact

Firecracker — We applied the same security-first approach to Firecracker, powering AWS Lambda and AWS Fargate

Nitro Enclaves: Isolated Compute for Sensitive Workloads

What It Does

Creates isolated compute environments within an EC2 instance to further protect highly sensitive data:

- Personally identifiable information (PII)
- Healthcare and financial data
- Intellectual property
- Multi-party computation

Key Capabilities:

- Cryptographic attestation
- KMS integration
- No persistent storage, no SSH

Attestation

Attestation allows you to verify that only authorized code is running before releasing sensitive material to the enclave.

Extending Confidential Computing to AI Workloads

AI introduces new privacy concerns that demand provable isolation

AI Challenges

- Models process sensitive data at unprecedented scale
- Training data may contain sensitive information
- Inference must happen without exposing inputs or model weights to operators
- Attestable AMIs provide cryptographic proof of what’s running

06

Looking Ahead

The future of trust in cloud computing

Where Do You Start?

What are you protecting?

Sensitive data in use: PII, financial records, healthcare data, proprietary models, intellectual property

Who are you protecting it from?

Insiders, cloud operators, co-tenants, or even your own administrators

How AWS helps

Hardware isolation, cryptographic attestation, and zero operator access by design

Get started with AWS: aws.amazon.com/confidential-computing

Thank You

Matt Wilson
Vice President / Distinguished Engineer, Amazon

Confidential Compute Summit

Security is not a feature. It is the foundation.